2018

Reducing Internal Theft and Loss in Small Businesses

Eric L. Luster
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Eric L. Luster

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jaime Jo Klein, Committee Chairperson, Doctor of Business Administration Faculty

Dr. John Hannon, Committee Member, Doctor of Business Administration Faculty

Dr. Krista Laursen, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Reducing Internal Theft and Loss in Small Businesses

by

Eric L. Luster

MBA, Western International University, 2007

BS, Wayland Baptist University, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2018

Abstract

Every year, several documented data breaches happen in the United States, resulting in the exposure of millions of electronic records. The purpose of this single-case study was to explore strategies some information technology managers used to monitor employees and reduce internal theft and loss. The population for this study consisted of 5 information technology managers who work within the field of technology in the southwestern region of the United States. Participants were selected using purposeful sampling. The conceptual framework for this study included elements from information and communication boundary theories. Data were collected from semistructured interviews, company standard operating procedures, and policy memorandums, which provided detailed information about technology managers' experiences with data security. The collected data were transcribed, member checked, and triangulated to validate credibility and trustworthiness. Two themes emerged from data analysis: the development of policies, procedures, and standards on internal theft and loss, and the use of technology-driven systems to monitor employees and control theft and loss. Technology-based interventions allow leaders within an organization to protect the integrity of systems and networks while monitoring employee actions and behaviors. Study findings could be used by leaders of business organizations to identify and respond to theft and fraud in the workplace. Business leaders may also be able to use study findings to develop employee monitoring programs that help to prevent the loss of both organizational and customers' data, enhancing public trust as a potential implication for positive social change.

Reducing Internal Theft and Loss in Small Businesses

by

Eric L. Luster

MBA, Western International University, 2007

BS, Wayland Baptist University, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2018

Dedication

I dedicate this academic achievement to the Lord who has continued to bless me throughout life. I entered the journey, praying that I would have support and still be able to provide support to my family. To my sons, Cire Luster and Evan Luster, and to my daughter, Gracie Luster, always follow your heart and dream big! Never let the word "no" close the door or prevent you from obtaining a "yes" in life. You are my motivation to continue striving for excellence, and I thank you! To the family and friends whom I have lost along the way, Edith Henderson ("Grandma"), Edward Lee Harrison, Don Klassen, and Jim "Jam" Searles, this is dedicated to you. To Dr. Harold and Becky Coles, Arthur and Joetta Downs, Winston and Tamarah Wallace and my mother Gerlynn Luster; this is for you. To my twin brother Edward Luster, I appreciate the support from day one of our life. Last, but not least, I dedicate this work to my beloved wife, LaCheris Luster. You have endured and stuck with me through "thick and thin." You have put up with the isolation spans and deprivations and still found a way to provide encouragement. I am forever thankful for all the support from all my family and friends who have encouraged, guided, and supported the effort.

Acknowledgments

The completion of this study would not have been possible without the generous and unwavering support of my doctoral committee. Special thanks to all my peers, mentors, advisors, colleagues, my chair, Dr. Jaime Klein, committee members Dr. John Hannon, Dr. Tara Kachgal, Dr. Krista Laursen and Dr. Kim Critchlow for mentoring me and offering guidance when I needed it the most. I would like to thank Dr. Sethuraman "Panch" Panchanathan, Dr. Troy McDaniel, Dr. Morris Goldberg and Dr. Albert McHenry for providing early support throughout the doctoral journey. In addition, I would like to the mentors that I had the opportunity to work with while serving in the United States Army. Special thanks to Lt. Col. Brent Skinner and GySgt Othello Taylor (RET) who provided leadership, encouragement, and motivation.

Table of Contents

List of Tables iv

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 3

Nature of the Study 3

Research Question 4

Interview Questions 4

Conceptual Framework 5

Assumptions, Limitations, and Delimitations 7

Assumptions 7

Limitations 7

Delimitations 7

Significance of the Study 8

Value to Business 8

Contributions to Business 8

Implications for Social Change 9

A Review of the Professional Academic Literature 9

Information Boundary Theory 12

Supporting Theories 14

Contrasting Theories 16

Employee Theft.. 20

Success Factors for Identifying Fraud 23

Leadership in Fraud Prevention... 24

Addressing Cybersecurity to Mitigate Theft and Fraud 31

Transition 37

Section 2: The Project..38

Purpose Statement..38

Role of the Researcher..39

Participants...40

Research Method and Design 41

Research Method 41

Research Design.. 42

Population and Sampling 43

Ethical Research..44

Data Collection Instruments 45

Data Collection Technique 47

Data Organization Technique 48

Data Analysis...49

Reliability and Validity..49

Transition and Summary..51

Section 3: Application to Professional Practice and Implications for Change 52

Introduction...52

Presentation of the Findings..........52

Theme 1: Development of Policies, Procedures, and Standards on Internal Theft and Loss.......... 55

Theme 2: Use of Technology-Driven Systems to Monitor Employees and Control Theft and Loss 61

Applications to Professional Practice 65

Implications for Social Change..........65

Recommendations for Action 66

Recommendations for Further Research..........66

Reflections 67

Conclusion 68

References..........69

Appendix: Interview Questions 84

List of Tables

Table 1. Theme 1: Development of Policies, Procedures, and Standards on Internal Theft and Loss 54

Table 2. Theme 2: Use of Technology-Driven Systems to Monitor Employees and Control Theft and Loss 61

Section 1: Foundation of the Study

Organizations maintain technology assets that are at risk from a myriad of operational threats. The threats often arise from both internal and external sources. In a small business, information technology (IT) managers and business owners often make assumptions about an organization's security posture lack validity, which often leads to further exposure to theft and loss within the organization (Hess & Cottrell, 2016). Furthermore, business owners have a need to accurately identify, monitor, and report theft and loss due to internal data breaches (Fernandes, 2014). Other researchers have estimated that 92% of all business organizations in the United States (U.S.) use technology to monitor and track employee digital interactions (Chiemela, 2014). Section 1 of this study includes the (a) background of the problem, (b) problem statement, (c) purpose statement, (d) research methodology and design, (e) research question, (f) conceptual framework, and (g) literature review.

Background of the Problem

The threat of a data breach within an organization can come from either external or internal sources. The issue of theft at work often results in loss and mistrust for some businesses. In U.S. small businesses, leaders often fail to stay in business because of the lack of proper methods for handling the issue of theft and loss because of cybersecurity issues (Bhattacharya, 2015). The failure to report data breaches often arises from the noncommitment of managers and even personal feelings that hinder the desire to find solutions to cybersecurity-related problems.

The research literature clearly indicates that employee theft is a key factor in the growth or collapse of a small business (Boersma, 2016). Whether a small business grows or collapses is dependent on the approach that management uses to address the issue of theft (Boersma, 2016; Goh & Kong, 2016; Dunne, 2014). The amount of loss experienced by small businesses in the United States because of employee theft stood at an estimated 5% of annual revenues in a 2012 study (Boersma, 2016; Dunne, 2014).

Small business theft and fraud point to management challenges related to the lack of appropriate measures to safeguard the management of finances (Karadsheh & Alhawari, 2014). In ordinary business operations, dishonesty and lack of integrity from the employees in the organization can result in the embezzlement of funds through the manipulation of organizational systems. To prevent such losses, 80% of large U.S. corporations use technology to conduct remote monitoring of employees, according to Moussa's (2015) research findings. In order for employees to accept monitoring and surveillance as just, however, workers must understand the value of the information collected to the mission of the organization (Martin, & Murphy, 2017). To achieve this, managers require strategies for implementing monitoring at work, while leveraging the latest technologies for monitoring assets.

Problem Statement

Internal theft and loss occur at higher rates in U.S. businesses than other countries because of data breaches (Wikina, 2014). U.S. businesses leaders spend nearly $400 billion annually to reduce improper employee actions including time mischarging, theft, and computer crimes (Moussa, 2015). The general business problem is that employee theft and internal loss negatively affect organizational profitability and sustainability. The specific business problem is that some IT managers in small businesses lack strategies to monitor employees and reduce internal theft and loss.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies some IT managers in small businesses use to monitor employees and reduce internal theft and loss. The target population included five IT managers in a single small business in the southwestern region of the United States that successfully monitors employees using technology to reduced internal theft and loss. The implications for positive social change include identifying strategies business owners can use to protect the organization and prevent data breaches to protect community members from exposure of personal information. In addition, identifying strategies for monitoring employees could provide best practices for enhancing public trust along with compliance techniques that prevent loss of data.

Nature of the Study

I used the qualitative research method for the study. Researchers use a qualitative method to gather in-depth data, discover the meaning of the unknown, and reconstruct participants' stories on a conceptual level (Yin, 2014). In contrast, researchers conducting quantitative research seek to determine relationships or differences among multiple variables and test hypotheses (Marshall & Rossman, 2016). Because my focus was not on testing a hypothesis, I concluded that the quantitative method and the mixed method, which includes the quantitative method, were inappropriate for this study.

I used a single case-study design to address the specific business problem. I considered but ultimately decided against using an ethnographic or phenomenological design. Researchers using ethnographic designs focus on shared experiences and interactions within a particular culture (Murthy, 2013; Zilber, 2014). The ethnographic design was not appropriate for the current study. Furthermore, researchers using the phenomenological design explore the meanings of the experience to the participants involved in the subject phenomenon (Corley, 2015; Moustakas, 1994). The intent of the study was to explore strategies some IT managers in small businesses use to monitor employees and reduce internal theft and loss, and therefore, the case-study design was appropriate. A case study design was more appropriate than other designs such as ethnography because the focus of the study was on developing monitoring strategies based on participants' responses instead of assessing the individual experiences of participants. In some situations, a case-study design is more appropriate than grounded theory and narrative designs, because of the need to conduct the study over a shorter observation period (Zivkovic, 2012).

Research Question

The research question for this study was, What strategies do information technology managers in small businesses use to successfully monitor employees, and reduce internal theft and loss?

Interview Questions

1. What strategies have you implemented to prevent and reduce internal theft and loss in the organization?

2. What strategies have you used to monitor employees?
3. What barriers did you encounter in implementing the strategies?
4. How have you leveraged technology to innovate in the company?
5. How did you overcome the barriers to implementing the strategies?
6. How have you addressed the need for secure data storage throughout the organization while maintaining data integrity?
7. How has your organization trained employees regarding data security?
8. How have you responded to information security violations?
9. What is the net result of your response?
10. What additional information would like to add to support the study?

Conceptual Framework

The conceptual framework for this study was the information boundary theory (IBT). Stanton (2003) developed the information boundary theory to explain how monitoring and surveillance technologies on employees' privacy affect an organization. Stanton described how information boundary theory applies to monitoring of employee communications and performance employees in the work environment. The framework may help leaders develop effective monitoring strategies for their organization. The IBT contains industry and academically acceptable criteria, which have led to the establishment of the framework as a best practice when it comes to monitoring employees in the work environment (Belanger & Xu, 2015). As employers seek to develop and enhance their company's security posture, the IBT theory is supportive of this effort and aligned with this research project.

Operational Definitions

Data breach: The term data breach refers to unauthorized access or disclosure of information that leads to the loss or manipulation of sensitive personal identifiable information. Data breach events can happen internally or externally and affect an individual or an organization (Wikina, 2014).

Data exchange: Data exchange is a term used to describe information transactions between organizations or employees. Data exchange includes the transmittal of authorized and unauthorized electronic data transmission (Vest, 2010).

Electronic performance monitoring (EPM): EPM is a term used to describe systems intended to allow employers access to employees' online usage (Moussa, 2015).

Encryption: Encryption refers to the manipulation of data for storage or transmission that renders the data unreadable unless a valid security token decrypts the data (Knott & Steube, 2011).

Governance: Governance is the process of decisions and policies made to allow effective management within an organization. Management relies on information technology systems to implement and monitor governance compliance (Khatri & Brown, 2010).

Internal theft: Internal theft describes the act of stealing, using, or misusing organizations' assets without proper permissions. The term asset is important because it describes more than physical or monetary items. In many organizations, high-value items include digital assets (Fernandes, 2014).

Loss: Loss occurs when economic harm or damage is sustained by an organization. The damage can result in a reduction of value or capital for an organization (Fernandes, 2014).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions refer to issues accepted as true or fact without evidence (Houghton, Casey, Shaw, & Murphy, 2013). First, I assumed that the participant responses were truthful regarding information theft and loss within their organization. Second, I assumed that the archival records of the target company were accurate. Third, I assumed that the participants were knowledgeable of corrective actions taken during potential data breaches.

Limitations

Limitations are potential weaknesses in the study, which were out of the researcher's control (Coffie, 2013). The first limitation was that the participants might not disclose or provide information relating to the monitoring programs within their organization. The second limitation was that the employees might treat program documentation as proprietary and fail to disclose the information. The third limitation was the lack of proper disclosure of security incidents leading to corrective action.

Delimitations

Research delimitations are the factors a researcher uses to determine the scope of a study and explain its restrictions to readers (Yin, 2014). I conducted research with IT managers in an organization in southwestern region of the United States, who have successfully deployed strategies for reducing internal theft and loss. In conducting the study, I sought to explore how IT managers incorporate strategies to address information security concerns to prevent internal data breaches. I only included IT managers who have knowledge of the implementation of strategies to reduce internal theft and loss.

Significance of the Study

Some small business leaders lack the knowledge to implement monitoring strategies using innovative tools within their organization. The findings from the study could contribute useful knowledge for small business leaders who need to address internal theft or loss within their organization. The knowledge arising from the study may also provide guidance to employees who are often concerned about the effectiveness of information security.

Value to Business

Business leaders recognize that monitoring employees is essential to measure effective performance and to ensure security across the organization (Chiemela, 2014). Business leaders implementing the results of this study may be able to identify strategies that take advantage of common best practices while leveraging the latest technologies for monitoring assets. Furthermore, by applying newly developed technologies, small business leaders may find it possible to implement effective strategies regarding data management for their organizations.

Contributions to Business

Small business owners need to accurately identify, monitor, and report theft and loss due to internal data breaches (Fernandes, 2014). Moussa (2015) published research that illustrates a distinction between internal and external threats. Some IT managers make assumptions whereas business owners can lack validity, which often leads to further exposure to theft and loss within the organization (Hess & Cottrell, 2016). Findings from this research could lead to knowledge that may mitigate the risk involved with data security for organizations.

Implications for Social Change

Wikina (2014) stated that data breaches could lead to the release of personal identifiable information of customers on the Internet. The release of personal information could directly affect the communities within the service area of the organization. Accurate monitoring and reporting is essential to ensure that public trust and data security is a top priority, which will result in social change. Past, current, and future stakeholders may receive additional protection when successful strategies regarding data security are implemented (Brunswicker, & Vanhaverbeke, 2015). The strategies identified in this study could include insights that small business leaders can use to monitor employees, enhance public trust, and identify compliance techniques that prevent loss of both organization and customers' data.

A Review of the Professional Academic Literature

The issue of theft at work often results in loss and mistrust for some businesses. Small businesses leaders are failing to stay in business because of the lack of proper methods for handling the issue of theft and loss because of cybersecurity (Bhattacharya, 2015). The issue arises from the noncommitment of managers to address security issues, coupled with personal feelings that hinder the desire to find solutions to the problems.

There is extensive research regarding the issue of information security (Kennedy, 2015; Kuypers, Maillart, & Paté-Cornell, 2016). However, an established and agreed-upon process for incorporating technical safeguards does not exist. One theme in the existing literature is how to mitigate theft and loss in small businesses (Romanosky, Telang, & Acquisti, 2011). Due to the lack of consensus, there is a lack of research on why organizational leaders are unable to mitigate the problem, however. The purpose of this qualitative single-case study was to explore strategies some IT managers in U.S. small businesses use to monitor employees and reduce internal theft and loss.

I used several databases and search engines to locate scholarly journal articles published in the past five years (2014-2018) that were associated with the business problem for this study. ProQuest Psychology and Sociology journals, JSTOR: Journal Storage, Google Scholar, and the Directory of Open Access Journals were some of the resources I used to locate research related to theft, loss, misappropriated assets, and fraud in small businesses. The search terms I used to locate relevant and recent literature included the following: *information boundary*, *information boundary theory*, *theft*, *small business loss, small business theft*, and *small business fraud*. The key terms are the foundation for finding research related to the problem and research questions in this study. More than 85% of the sources that I used in the literature review consisted of peer-reviewed articles published since 2013.

The information boundary theory focuses on the elements of information sharing by the employees in a given organization (Stanton, 2003). When employees feel that the act of sharing crucial information about the state of security systems for controlling financial loss has a direct effect on their working relations at work, they engage in an information boundary closure (Romanosky et al., 2011). In contrast, when employees are confident about the outcome of sharing the security systems information, they offer valuable information on the strengthening of loopholes (Romanosky et at., 2011). This aspect is referred to an information boundary opening. Theft refers to an illegal activity that involves the fraudulent operations of financial and management systems in an organization that results in loss of funds (Rezaee, 2002). Certainly, controlling the factor of theft through instituting fundamental security strategies that consist of sealing the gaps in the financial management systems in a given entity should reduce incidences of financial losses (Badrul, Williams, & Lundqvist, 2016). Categorically, small business theft and fraud illustrate the management challenges related to the lack of appropriate measures in the management of finances. In ordinary business operations, the element of dishonesty and lack of integrity among the employees in the organization results in the embezzlement of funds through manipulation of systems (Vousinas, 2015).

Most of the literature reviewed was published from 2014-2018. I included seminal research on the conceptual framework of the study, dating back to 2002. A limitation of the literature review was the breadth of literature. Some articles used in the literature review included larger organizations as the study population. The overall goal of the literature review was to provide a procedural flow providing information regarding compliance and information security gaps.

In the first section of this review, I describe the strategies I used to search published research for studies associated with the problem. I describe the conceptual framework in the second section, which is information boundary theory. The third section of this literature review expounds upon employee theft. The fourth section describes cybersecurity in relation to theft and loss. The fifth section explains the implications of theft for small businesses. The final section of this literature review is a summary and conclusion.

Information Boundary Theory

Employee concerns about privacy, employer needs to monitor employee activity, and the ability of technology to gather robust information in the workplace have made the issue of boundaries a significant problem in contemporary organizations. The collection of information by management may contribute to a new understanding of the ways that employees are engaging in employee theft or contributing to resource loss (Stanton, 2003; Stanton & Stam, 2002). In addition, the collection of this information could provide insight related to the perceptions of employees regarding personal boundaries in the workplace. Employees engage in either boundary openings, where the employee will share information with an audience, or boundary closing, where the employee will shut down dialogue without the sharing of information with an audience (Stanton, 2003). The boundaries of employees are dynamic in nature, and employees may open or close these boundaries in order to regulate relationships in the workplace and with their employer (Stanton, 2003). In addition, employees will select what information and with whom they will share this information to protect themselves as well as maintain comfortable boundaries within the organization (Badrul et al., 2016).

Boundary opening and closure may have implications for the ability of management to collect information on employees. Workers with something to hide or may perceive that it is in their best interest to conceal information with closed boundaries. Furthermore, workplaces where data collection and monitoring is strong could also encourage employees to be more selective about boundary opening. These implications are problems related to the phenomenon of information boundary theory, which continue to plaque employers in the area information security.

Seminal work on information boundary theory began in the early 2000s by Stanton. Information boundary theory is a phenomenon created by employer surveillance and data collection on the activities of employees (Stanton, 2003). According to Stanton (2003), when the employer collects data and surveils the employee, the employee may feel a breach in his or her workplace privacy; hence, when management breaches an expected boundary of the employee, the employee may react negatively. The surveillance and data collection could cause an issue for employees; but, the elements consist of information boundary theory add an additional level of discovery for the employer. Another component of the theory is its description of the implications that collection of employee data would have on employee concerns over privacy and security as well as the ability of management to secure the workplace from theft and the misappropriation of assets (Stanton & Stam, 2002; Stanton, 2003). Employee concerns are realized when theories, such as IBT are deployed.

Supporting Theories

Information boundary theory stems from the synthesis of three different theories of interpersonal and organizational communication. Those theories are communications boundary theory, organizational justice theory, and expectancy-value theory (Stanton, 2003). Specifically, using information boundary theory will describe the relationship between security and privacy strategy in the organization to the likelihood of employee theft within a particular period (Holland, Cooper, & Hecker, 2015). Scholars have used information boundary theory as the theoretical framework in workplace privacy research studies (Kokolakis, 2017). Smith and Brunner (2017), Rupp et al. (2017) and Gelens et al. (2013) used interpersonal and organizational communication theories in their workplace privacy studies. Using interpersonal and organizational communication theories as a theoretical backdrop, Smith and Brunner (2017) explored decisions that employees make to manage private disclosures at work.

Smith and Brunner (2017) found that communication boundary theory was suitable for exploring the management of private information. Smith and Brunner (2017) also found that there are catalysts criteria that motivate people to reveal or conceal information while at work. From the research, Smith and Brunner (2017) took a sample of 103 full-time employees from various organizations and across industries to identify how employees handle private disclosures in the workplace. In the aforementioned study, communication privacy management theory was used to understand the management of private information.

Other scholars used organizational justice theory when examining information security issues in the workplace (Gelens et al., 2013; Rupp et al., 2017; Rupp et al., 2017). In their study, Rupp et al. (2017) used organizational justice theory to assess workplace fairness. Rupp et al. (2017) explored and measured the constraints that employees face. According to Wigfield, Tonks, and Klauda (2009), an expectancy-value theory is associated with the perception of the value of engaging in specific behaviours that provide personal gain. The belief in the perceived outcomes from maintaining boundaries determines the behavioural intentions of having open or closed boundaries of employees (Zakaria et al., 2003). These concepts map to workplace privacy concerns with the assumption that any organizational communications could ultimately have a negative impact. In summary, the frameworks are to aid researchers in identifying reactions and thoughts in regard to “boundary opening” and “boundary closure.”

Fundamentally, exploring the challenges of the information boundary theory stems from an examination of the perceptions of the employees towards the boundaries in the workplace. When the employees feel that the matter of sharing crucial information on the theft in the workplace could affect their working relations, there is a likelihood of boundary closure (Holland, Cooper, & Hecker, 2015). Typically, in the workplace, employees are usually resistant to changes in their working environment (Stanton, 2003). Moreover, accusations of fraud and theft could increase this resistance (Watkins, Coopman, Hart, & Walker, 2007). Essentially, the reaction of the organization’s management team towards safety concerns regarding fraud from the employees could be detrimental towards the wellbeing of the working relations among the employees.

Contrasting Theories

Other theories, such as neo-institutional theory is found in the literature and describe how internal and external forces influence management strategies in an organization (Suddaby, 2015). Using neo-institutional theory, the leadership team benchmarks their organization against other organizations in the industry and depend on societal factors to develop the organization’s structure. The neo-institutional theory view is absent from traditional views such as economics, which means that the organizations’ bottom-line is not taken into account (Macfarlane, Barton-Sweeney, Woodard, & Greenhalgh, 2013). Organizations experience macro-level changes in institutional structures, which happen over time. Based on the current landscape of information security, the security posture of an organization must change rapidly and appropriate buy-in from employees is required.

The measures established by the management office are restrictive and demanding from the employees’ perspective (Wells, 2017). Therefore, for shielding themselves from such stringent security regulations, the employees opt for an information boundary closure. The problem arises from a failure to disclose fundamental information about the weaknesses in the theft management systems. Once there is a breach of the theft system, a small business could begin to lose funds (Stanton & Stam, 2002). Hence, the information boundary closure portends an unfavourable scenario to the sustainability as well as the daily operations of the small business.

According to information boundary theory, employees will open or close boundaries based on their relationship with an audience (Stanton, 2003). Stanton (2013) determined that relationships established by workers could also depict the way they use the information as well as the level of sharing of knowledge with a specific audience. For employees, information boundaries are important because the information shared may lead to positive outcomes such as a raise or a promotion or a negative outcome such as disciplinary action or termination of employment (Stanton & Stam, 2002). Stanton and Stam (2002) noted that boundary opening and closure are gain and loss focused, where an employee will open boundaries if they feel opening up will help achieve a goal or mitigate losses. In addition, an employee will close boundaries if they believe they can solidify again or prevent loss by closing off a boundary (Stanton & Stam, 2002). Furthermore, trust, group-value, and the instrumental nature of information are factors that contribute to the boundary opening or closure decision making of the employee (Ong, 2016). The sharing of information from employees stems solely from the perceived good or bad outcome from providing entail.

The intrinsic need of humans to manage the balance between intimacy and autonomy in relationships outlines the basis for communications boundary (Stanton & Stam, 2002). Through intimacy, people are able to build relationships and form trust with one another. Furthermore, workers are also able to form trust within organizations when they feel comfortable enough to share information with agents of the business (Ong, 2016). Workers also seek autonomy where they are able to separate themselves from others. Stanton (2003) noted that there is tension between the concepts of intimacy and autonomy when people seek both in relationships. Hence, employees must manage the nature of their communications boundaries with leaders and other workers within the organization.

Leaders in the workplace engaging in monitoring and surveillance of employees can become a threat to the autonomy of the workers (Zakaria, Stanton, & Stam, 2003). Once the surveillance begins, the employee may close their boundaries as a way of controlling relationships developed within the workplace (Stanton & Stam, 2002). As a means of decreasing theft and employee knowledge sharing, small business leaders openly acknowledge the use of surveillance (Romanosky, Telang, & Acquisti, 2011). In essence, the matter of surveillance contributes immensely to the security factor, thus reducing the incidence of theft by the employees. Essentially, privacy has a direct impact on the employees' perspective of theft and the results of sharing their knowledge of any occurrences.

Control relates to the concept of organizational justice. The employee seeks to negotiate the nature of their boundaries in the organization; however, organization protocol and the design of workplace security determine the nature of how it is that employees will be monitored (Zakaria et al., 2003). The employee is not able to negotiate this with agents within the organization, therefore, the worker's reaction to monitoring and surveillance will be a way in which the employee seeks organizational justice (Romanosky, Telang, & Acquisti, 2011). Furthermore, employees will seek organizational justice through fair and equal treatment with other members of the organization and the nature of this membership and group status will contribute to their perceptions of whether treatment is fair in the organization (Martin, Borah, & Palmatier, 2017). In order for employees to accept monitoring and surveillance as just, workers must understand the value of the information collected to the mission of the organization (Martin & Murphy, 2017). The key is not to have a perception of unfairness by the subordinates based on the data collected.

Employees choose to give information based on value. According to Wigfield, Tonks, and Klauda (2009), an expectancy-value theory is associated with the perception of the value of engaging in specific behaviours that provide personal gain. The belief in the perceived outcomes from maintaining boundaries determines the behavioural intentions of having open or closed boundaries of employees (Zakaria et al., 2003). Being a part of the system while earning funds and being in the good graces of leadership is an example of how workers use expectancy theory (Wigfield et al., 2009). Hence, the appropriate management approach should allow for a mutually beneficial technique that the employees could embrace in the information sharing exercise.

Stanton (2003) concluded that there are four key elements of information boundary theory. are the elements (1) a minimum boundary where requests for information from supervisors are not scrutinized, (2) boundary opening and closure are governed by organizational justice considerations, (3) boundary opening is governed by instrumental motivations and that trust, and (4) mistrust facilitates decision-making related to if information should be shared (Stanton, 2003). Stanton (2003) noted that because of these elements, the implications for employees on how business leaders conduct and understand monitoring and surveillance through the context of how sharing information will be a benefit or detriment to the employee.

Employee information can be valuable in organizations as the communication can contribute to the improvement of business processes and stronger management of resources. Information technology supports effective monitoring and surveillance of employees in organizations while the collection of this information is valuable (Stanton & Stam, 2002). Yet, encouraging employees to expand their boundaries can be a challenge for management. Conversely, Goh and Kong (2016) noted that workplace surveillance and the expansion of information boundaries could increase the ability of management to improve theft and loss prevention efforts. There is a paucity of research on the topic of workplace surveillance and loss prevention (Goh & Kong, 2016). With this paucity, small business leaders could begin to develop strategies that could expand the boundaries of information, improve theft mitigation, increase loss prevention efforts, and maintain company profits (Wells, 2017). Understanding information boundary theory in the scope of loss prevention can be a key to understanding how to prevent theft and the implications that loss prevention efforts may have on employee performance.

Employee Theft

Indeed, researchers in the field of business and management have provided research regarding the concern of employee theft substantially. From the analysis, there is a clear indication that the challenge of employee theft is a key factor for the growth or collapse of a small business (Boersma, 2016). Furthermore, this growth or collapse is dependent on the approach in which the management is going to use in addressing the issue of theft (Boersma, 2016; Goh & Kong, 2016; Dunne, 2014). The amount of loss experienced by small businesses in the United States because of employee theft stood at $3 billion (Boersma, 2016; Dunne, 2014).

Fundamentally, this figure aids in explaining the gravity of the challenge in the matter of the operations of a small business (Dunne, 2014). In general, about 5% of revenue from small business entities is lost because of employee theft channels annually (Kennedy, 2015; Kennedy, 2016a). Therefore, the problem of employee theft is an immense threat to the sustainability levels of small businesses. For further analysis of the topic, it is imperative to examine the effect of employee theft to the overall management of the business outside the impact of the direct financial loss (Kennedy, 2015; Kennedy, 2016a; Kennedy, 2016b; Kennedy & Benson, 2016).

Benson and Kennedy (2016) delved into the impact of the incidents of employee theft on the general management of small businesses. In addition, researchers questioned the management approaches adopted by business executives after experiencing financial losses in the business (Benson & Kennedy, 2016). Furthermore, employee theft influences the management of business organization in a negative way because of the reduction the level of employee trust by the management (Kennedy, 2015) The working relations between the employees and the managers are affected hence reducing the level of productivity in the business because of employee theft (Benson, 2016). Finding solutions to theft could aid with the overall flow of employee and management relationships in small businesses.

Employee theft in small businesses contributes immensely to counter productivity. The fundamental concern within the problem of employee theft is that employees for personal gain (Kennedy, 2015) embezzle the finances of a business. Therefore, the business can no longer sustain operations since the financial loopholes have a profound impact on the cash flow management in the entity. The analysis made by Kennedy (2015) indicated that employee theft has received little attention from business managers. Shockingly, this reality is ignorant of the adverse effect that employee theft has on the financial health of a small business. Furthermore, Kennedy (2015) maintained that there are particular reasons why management ignores employees in the operations of the business. Majorly, the aspect of the impact that the disclosure on theft will have on the reputation and overall image of the entity is one of the key reasons. At the same time, the tense relations between the employees and management have a critical contribution to the element of open disclosure. Thus, the factor of underreporting thrives in these business scenarios.

Kennedy (2016a) advised that business managers should establish comprehensive investigatory measures to ensure the controlling of employee theft to minimal levels. Markedly, proactive business measures could implement a check on the likelihood and control of the incidences of employee theft in the ordinary operations of the business (Kennedy, 2015; Kennedy, 2016a; Kennedy, 2016b). The overall benefit is mutually advantageous in the sense of boosting the financial health of the business. In addition, enhancing the business prospects and the confidence levels of the managers towards the employees are heightened.

Success Factors for Identifying Fraud

Small business owners face the possibility of becoming the victims of fraud. Fraud can pose a significant problem in small businesses. Hess and Cottrell (2016) acknowledge that fraud could cause limitations within administrative support resources in small and growing business to the point where internal control over theft and loss is difficult. According to Hess and Cottrell (2016), small businesses owners have a high chance of becoming victims of fraud and management must do their due diligence in order to protect the organization from employee fraud. In addition, Boersma (2016) noted issues such as rapid growth, a lack of administrative support resources, and financial strain make it difficult for managers to prevent and detect fraud. The small business manager must engage in strategies that contribute to the mitigation of fraud in the organization. There is a significant amount of difficulty in finding enough evidence to prove theft; therefore, in cases where there is fraud, the small business owner and members of management should be thorough in how they investigate the potential of fraud in the organization (Boersma, 2016).

While managers and employees may feel it is difficult to confront fraud it is necessary to confront deception because theft could impact the profitability of an organization. Dunne (2014) noted that 5% of revenue is lost based on fraud. Losing any percentage of finances is detrimental to the health and sustainability of an organization and threatens the ability of a firm to continue.

For this reason, small business owners must be engaged in strategies that could aid in identifying areas of potential fraud and loss. Dunne (2014) noted that because small business owners may only have a few employees and a limited amount of resources, these leaders might not use strategies such as the use of an internal auditor. Ownership and management must perform internal checks to ensure that fraud is not taking place in the business. Dunne (2014) noted that while pressure, opportunity, and rationalization must be present for fraud to occur, there are ways to mitigate fraud by limiting one of those elements. Opportunities to commit fraud can be limited in an organization by engaging in activities that reduce dependency on the employee in one role where they may commit fraud by segregating tasks, engaging in reconciliations of accounts, analysis, and making employees take routine vacations. Eliminating opportunity is important; however, organizational leaders should also reduce the potential that an employee may rationalize engaging in theft by reducing organizational factors that would contribute to theft. In the same view, Hess and Cottrell (2016) examined the matter of security risk presented by financial risk. Therefore, there is a need for small business owners to mitigate risk against fraud through instituting stringent management measures relating to the activities of the staff members within the entity (Hess & Cottrell, 2016). Understandably, it is evident that a collaborative safety management approach is appropriate for the prevention of theft. In addition, due diligence is extremely important as the new approaches are deployed.

Leadership in Fraud Prevention

Employees expressed that the most influential reason for performing employee theft was that other workers did the same things. Although workers steal, these employees know that they are committing crimes although they understood their wrong deeds. Rezaee (2002) concluded that employee theft is a problem for Generation Z and that immersing students in ethical coursework to develop an ethical foundation for their approach to the workplace should be helpful. Developing a foundation for leaders and employees that understand ethics could be the best way to deal with this fraud. When the young generation leaders have the foundation, these leaders could influence other generations. It is easier to affect new leadership and employees rather than trying to change an already established culture.

Employee theft is not just about taking resources for enrichment; employee theft has some social implications. Stealing can be a part of the culture of an organization and become expected of people (Goh & Kong, 2016; Kennedy, 2016b; Kennedy & Benson, 2016). This may also be associated with equity theory where employees seek an equitable exchange in the same fashion as their coworkers and see theft as the most expeditious way to achieve it (Adams et al., 2006). There is, therefore, an engraved system of looting and theft that these employees would develop the moment they get an opportunity to work. Some individuals may get it the workforce not intending to steal; however, once they get into a culture of theft, these people are unable to resist stealing. Overall, employee theft can be confounding to management regarding how to address deception because it may be confusing as to why the fraud occurs.

Research on the implications of employee theft on management is vibrant. Key findings are evidence that employee theft is an issue that managers may try to ignore (Kennedy 2016a; Kennedy 2016b); however, when forced to address the problem it can have implications regarding how management addresses the leadership of the staff

(Kennedy, 2016). Theft is one of the most significant crimes that a small business leader will need to deal with, and because of that, ownership will typically seek to make changes that will contribute to avoiding future theft in the organization (Kennedy, 2017). Furthermore, in response to theft, a small business owner will construct their answer based on how they perceive the severity, what they believe could be done about the issue.

An important aspect that has risen from research is that employee theft non-reporting and the rationalizations that employees have for not reporting theft. Kennedy (2016) noted the ways that employee theft harms a business, placing emphasis on how employee theft will have an impact on financial, emotional, and organizational elements of the business. Theft is, therefore, one of the most underreported crimes in small business. Management and ownership will typically be confounded regarding how to handle theft, especially in cases where the thief is a trusted employee. In addition, theft begins with a trivial amount; however, over time, theft will continue to increase.

When people have already developed the character of a thief, they would often engage in even more elaborate methods of fraud at work. For instance, the US Chamber of Commerce estimated that 75% of the employees engage in thefts and only fifty percent of these are reported (Krishnakumar, Hopkins & Robinson, 2017). The effect of theft is that it leads to failure of the business. Furthermore, about one of the three companies that fail is caused by theft of fraud. The effect of these issues leads to loss to the government and even business. In general, the US Department of Commerce mentioned that dishonesty costs business about 50 billion annually (Dion, 2008). In terms of non-reporting, the key reasons for not reporting are associated with personality factors and previous involvement with the criminal justice system. In an ideal sense, employee theft could continue to remain underreported because business leaders will avoid having to deal with the time and problems associated with a theft experience, and those employees who become thieves lose their job without anyone disclosing the crime to law enforcement (Dion, 2008).

There are many reasons that cause dishonest behaviour in small businesses. Jaakson, Vadi, Baumane-Vitolina, and Sumilo (2017) investigated organizational factors related to dishonest behaviour in retail. Business leaders believe that they would be leaking sensitive information if they were to discuss being victims of theft (Jaakson et al.,2017). Of the 781 employees and 6 organizations investigated, Jaakson et al. (2017) determined dishonest behaviour would more likely happen in urban areas and in firms that were larger. In small businesses, employees were more likely to steal based on a feeling of injustice in the business. Furthermore, there is evidence of factors unique to small business owners, which are not present with larger firms and that when employees in smaller firms receive poor treatment, the feeling is more personal, and the employee may use the poor treatment as a reason to engage in theft (Jaakson et al., 2017). In addition, Dahmen, & Rodríguez, (2014) determined that the lack of professionalism among the leadership within the small business leads to employee theft. Most small businesses are headed by family members that have little or no knowledge of what leadership is. Since they have little knowledge, they often end up mismanaging and mistreating their subordinates. Furthermore, they do not handle issues in the way that can show professionalism and this often leads to the employees being discounted in their workplace.

Personal issues also top the factors that influence employees into engaging in theft. Moorthy, Seetharaman, Jaffar, and Foong (2015) investigated the behaviour of employees in retail organizations regarding employee theft. Moorthy et al. (2015) investigated the organizational and individual factors that contribute to employees engaging in theft behaviour. The researchers determined that both organizational and individual elements will influence the theft behaviour of employees and that the nature of internal control systems will moderate the relationship between workplace theft and an employee’s intention to steal. This survey-based research contributes key knowledge regarding if employees who wish to steal will steal. When there are strong systems in place, employees who would like to steal from the organization are less likely to engage in theft (Moorthy et al., (2015). Internal controls could essentially be a way of theft prevention because employees are aware that parameters exist; therefore, employees will avoid doing things that may trigger the system to draw attention to them. The researchers noted that one of the keys to good internal control is having a system in place where co-workers can report employees are engaging in theft. Yet, whistleblowing is difficult to encourage because employees and managers typically are not comfortable with reporting on co-workers, particularly because of the potential implications of doing so with other staff.

There is also an important aspect of the influence of internal controls and resources management. Internal control seems to be an important aspect that affects the employees and leads them to commit theft in a small organization. Sankoloba and Swami (2014) investigated the role of internal controls in small businesses in Botswana. The researchers performed a qualitative case study, gathering data from 52 respondents. According to Sankoloba and Swami, internal controls play a significant role in the management of small business resources because this factor lessens the ability for workers to steal. For this reason, a significant expense of small business owners should be to become trained on implementing internal control standards. Furthermore, knowing that internal controls are just the start, small business owners need the resources to place internal control specialist in their businesses (Brunswicker, & Vanhaverbeke, 2015). For that reason, they will generally need to maximize internal control through their own investigative work. To mitigate loss and employee theft, ownership should seek to train managers and themselves on internal control standards.

There is quite a big challenge that employees face when dealing with an issue of theft. The problem is even magnified with the challenge that comes with reporting these issues. Boersma (2016) gives an analysis of the challenge that arises from the issue of reporting theft. One of the issues is that the colleagues and even managers at the workplace often find it hard to report their colleague’s wrongdoing. Furthermore, they often decide to the keep these issues within themselves and thus increasing the cases of thefts (Shaheen et al., 2014). Since the challenge is within the employers, the owners of small businesses only notice theft when there are financial issues.

The other challenge is that when one becomes the whistleblower then they have the burden of providing the evidence out of the theft. If a whistleblower would fail to provide credible evidence of how the issues took place, then they are forced to face issues such as victimization and mistrust. There is also the challenge as mentioned by Boersma (2016) on the issue of reporting theft with an organization. Some people are never ready for the responsibility of reporting any cases of theft in the organization. The challenge is also more prevalent in the lack of structures used to report potential violations. There are common cases where the managers ignore the calls that are made by employees about theft (Liu, Liao, & Wei, 2015). Since there are not any clear methods of handling the issues, quite often the theft would often go unreported. There is also the mention of the personal relationship with the leadership. Many of the people that are reported might have a personal relationship with management and thus the cases would not be handled (MacGregor & Stuebs, 2014). The decisions of management are often clouded by personal relationships, thus affecting the objectivity of solving the issue.

There is quite a serious issue when it comes to the impact that theft has on employees and leaders. This issue stems from the fact that the theft does not only involve people taking the funds from the organization but in some cases just people misusing the funds in the organization for personal gain.

Emotional intelligence is one key issue that is often affected by employee theft. Kennedy and Benson (2016) argued that managers are often faced with a serious challenge when trying to handle the issue of theft within the organization. Their reactions are often affected by experiences (Bibi et al., 2013). There might be cases where the employees are not involved in the theft, but since the managers have the perception that everyone is involved in stealing, leaders begin treating all workers with suspicion (De

Clercq, Bouckenooghe & Matsyborska, 2014). The manager would often find it hard to handle the issue and thus productivity would go down. From the view of Kennedy and Benson (2016) managers should learn some aspects of emotional intelligence as a means of learning how to handle their feelings while in the workplace. Having emotional intelligence is the one-way leaders can effectively handle the issues of employee theft.

In addition, another issue arises from the commitment of the employees to report cases of theft. Isenring, Mugellini, and Killias (2016) investigated the willingness of employees and management to report employee theft to the police. The researchers performed a survey-based investigation of employee theft in small businesses in Switzerland. Not all theft is reported and there are factors such as the type of business, severity of theft, fear of damage to reputation, and trust in the police were key factors in whether theft would be reported or not (Isenring et al., 2016).

Addressing Cybersecurity to Mitigate Theft and Fraud

Cybersecurity is a key issue for small and medium-sized businesses. Valli, Martinus, and Johnstone (2014) investigated cybersecurity awareness in small Australian businesses to understand management perceptions of cybersecurity. The researchers sought to understand the outcomes of cybersecurity events in terms of how a penetration occurred and how the firm responded. Resilience and resistance were key problems in organizations, resulting in penetration and in many instances, loss of intellectual property and cyber theft (Valli et al., 2014).

For small businesses cyberattacks, specifically, data theft will have a significant impact on share prices and the creation of systematic risk in organizations. Hinz, Nofer, Schiereck nd Trillig (2014) investigated the impact that data theft has on share prices in the consumer electronics industry. The share prices will decrease significantly in firms where there has been a cyber attack resulting in the theft of data (Hinz et al., 2014). The loss of share prices could have negative effects on a small business. This is evidence that the theft of intellectual property does have real implications regarding the value of the firm.

Bhattacharya (2015) investigated the evolution of problems related to cybersecurity in small businesses. Although cybercrime is a problem for large organizations, it is a key problem for small businesses. Because of the role that small businesses play in the economy, it is important to understand the nature of the security threats that those firms face, namely cybersecurity (Broadhurst et al., 2014). Understanding security threats are important because of the benefits that come from both production and the development of intellectual property. Furthermore, losing production because of cybercrime could impact the sales of a business.

Small businesses leaders generate 2.4 times more innovation than executives within large businesses; therefore, small business owners must be investigated based on the implications on the economy and potential economic growth. Bhattacharya (2015) noted that cybersecurity has been a problem for decades, but as consumers begin to demand online solutions for retail commerce, cybersecurity issues have increased for organizations. In the current form, cybersecurity is a threat because of the problems related to the ease of penetration, especially as organizational leaders will typically not have a subject matter expert to protect the organization. In addition, when management does not understand controls as well as the staff it is possible for staff to steal from the firm without detection (Scott, 2015).

As a means of staying open, small business owners should compose a guide for responding to cybersecurity theft problems. Developing an internal control and anti-fraud program for small businesses where there is fraud risk assessment, control activities, and the documentation of information could aid with decreasing or ending cybersecurity (Dawson, Dawson, Eltayeb, & Omar, 2016). The framework for an antifraud plan for the business depends on management engaging in periodic investigations and understanding the work processes of the business (Vousinas, 2015). Managers who have the task of investigating internal controls of the firm should be able to evaluate how employees are conforming to designed business processes and analyze their work to determine if there is potential fraud happening in the organization (Vousinas, 2015). Therefore, if leaders use the internal controls properly, they could detect fraud and stop cybersecurity threats.

Dawson et al. (2016) also identified the need for fraud and fraud reporting policies on organizations. These policies are key to mitigating the threat of theft and fraud. The researcher concluded that from the implementation of a robust anti-fraud and theft framework it is possible to significantly mitigate internal threats of fraud, theft, and loss in the organization. This is supported by Paulsen (2016) who indicated that through cybersecurity, it is possible for small business leaders to be more flexible and adapt to changes. Through this adaptation, it is possible for small business leaders to address issues related to theft and fraud quicker than large organizations (Paulsen, 2016). The key for this to happen is for small business leaders to have a well-defined plan in place to implement small business security standards.

Small business leaders must engage in behaviours that contribute to limiting exposure to fraud, theft, and loss. Ensuring the security of work processes and the information system is one key measure by which leaders may ensure safety. Paulsen and Toth (2016) investigated small business information security to determine how it is that small business leaders could protect their systems from internal and external theft and fraud threats. Small businesses can be prime targets for theft and fraud by people inside and outside the organization (Paulsen & Toth, 2016). This is because small businesses will not have the funds available to invest in robust security and internal control (Kuypers, et al., 2016). While the firm may have valuable assets and intellectual property, the leaders must protect those items, otherwise, the assets and intellectual property may be damaged or stolen by cyber intruders or people in the organization.

Paulsen and Toth (2016) noted that small business owners are in a difficult position in terms of fraud and theft. Not only can fraud and theft have immediate costs, but also there are long-term costs. One of the long-term effects of fraud is the closure of the business (Paulsen & Toth, 2016). In addition, there are other effects such as the loss of finance and court cases. A business that is not able to handle the issue of theft would definitely suffer detrimental effects. New technologies are making this problem more significant because customers are relying on cloud-based solutions and small businesses must assimilate into the current demand of the customer or become less competitive.

The lack of knowledge on the use of cloud computing seems to also be an aspect that is fueling the issue of theft in small businesses. The challenge is not only the lack of knowledge but also the resource and finances to be able to tap into the use of technology. Karadsheh and Alhawari (2014) noted that small business owners are now having difficulty utilizing cloud-computing technologies. This is a problem for entrepreneurs because cloud-computing technologies are a significant element for consumers engaging with businesses and make purchases. There are multiple internal risks and security issues that management may face when implementing cloud-computing technologies. Those internal risks include: Without appropriate security policy in place, organizations may have increased difficulty regarding selling to the consumer and protecting private information (Willison & Warkentin, 2013). The key could be to find solutions that will not require fundamental changes to the infrastructure of an organization.

There is a lot of security when organizations opt to use cloud computing in the daily transactions. Clients in the 21st Century prefer a business run online. In addition, they also prefer if communications and information about the business can be found in online platforms. Paulsen and Toth (2016) and Karadsheh and Alhawari (2014) determined the security of transactions and the business, in general, is possible through the utilization of policies related to cloud computing security. The authors recommended there be a disparate division of labour where employees receive different tasks within a process so that some employees are not able to commit fraud without detection.

There is much more gain for any organization that decides to use cloud computing. One of the positive impacts is that cloud computing helps to secure data.

Vousinas (2015) argued that one of the causes of fraud in the organization is that many of the employees have access to the data within the organization and thus they can easily manipulate information to suit their own personal gains. It is common to find the employee trying to hide details about their participation in theft. It often takes years for the companies to realize that such theft even happened. The lack of protection for data and information thus makes the organization prone to theft of various proportions. Even after detecting theft, management would often have not means to stop them (Willison, Warkentin, & Johnston, 2016). The situation would even lead to bigger proportions as the employees seek new ways to steal from the organization. The results are often the collapse of the business. There is no doubt that cloud computing, though could not be the absolute solution, can be one of the ways to deal with the issue.

Transition

Section 1 of this study contains a discussion on strategies some information technology managers in small businesses use to monitor employees and reduce internal theft and loss. The section begins with the foundation of the study, the background of the problem, the problem, and purpose statements, nature of the study, the research question along with the interview questions, conceptual framework, operational definitions, assumptions, limitations, delimitations, and significance of the study. In Section 1, I reviewed the academic and professional literature of the conceptual framework. The themes collectively present an in-depth coverage of the research topic. The literature review includes a discussion on the themes of security violation response, compliance programs, reduction of internal theft and loss, data breaches, data governance and policy, auditing, remote monitoring, and reporting.

Further descriptions and explanations of the study are in Section 2 and include information on the participants of the study, research method, research design, research process, description of the case, and the interview questions. Section 3 includes the presentation and analysis of the findings. Included in the analysis is how the findings support the conceptual framework of the study and the data collected in the literature review. Section 3 concludes with recommendations for future research, recommendations for action, and implications of positive social change.

Section 2: The Project

Section 2 includes a detailed explanation of the research process. Using a qualitative single case study, I explored strategies some IT managers in small businesses use to monitor employees and reduce internal theft and loss. The research involved data collection through personal interviews and analysis using academic accepted research procedures. The findings of the study may contribute to positive change in business practices within the small business community. In addition, in Section 2, I emphasize my role as the researcher, describe the target participants, and provide a detailed description of the research method and design selected for this study.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies some information technology managers in small businesses use to successfully monitor employees, and reduce internal theft and loss. The target population included five information technology managers in a small business in the southwestern region of the United States that successfully monitors employees, and reduces internal theft and loss. The implications for positive social change include identifying strategies business owners can use to protect the organization, prevent data breaches to protect community members from exposure of personal information. In addition, identifying strategies for monitoring employees could provide best practices for enhancing public trust, while identifying compliance techniques that prevent loss of data.

Role of the Researcher

In this qualitative case study, my role as the researcher involved collecting, organizing, analyzing, and interpreting the data. I recruited participants, scheduled and conducted interviews, collected other data, and performed data analysis. In a case study, the researcher must build a solid foundation with the interviewee by asking good questions, exhibiting good listening skills, and properly documenting the interview (Yin, 2014). In this study, I followed ethical guidelines for protecting the research participants. The ethical guidelines included respect, beneficence, justice, informed consent, risks and benefits assessment. The method used for the selection of subjects for the research aided in avoiding bias for the research (U.S. Department of Health and Human Services, 1979; Yin, 2014).

I have over 20 years of professional experience in computer network engineering, computer network security, business development, project management, and executive operations. I selected an organization in which I am not employed to participate in the study. I had no relationship with the participants and was not involved with them in any personal capacity at the time of the study. Therefore, I believe that participants were not at risk for retaliatory actions based upon their responses. My previous experience with computer network security increased the potential for bias in the study. However, maintaining ethical considerations for data collection and analysis should eliminate the potential for bias (Yin, 2014). To prevent bias with the selected participants, the prerequisites for participating in the study was that the participant had to be an employee of the Corporation under study. In addition, participant’s must be 18 years old or older, work in engineering and/ or IT, and have managerial experience.

Before data collection, an established and well thought out interview protocol that supports proper qualitative research should be established (Jacob & Furgerson, 2012). Using interviews as the primary data collection method aids the research because interviews allow the participants to share their experiences (Yin, 2014). Conducting in-person interviews allow researchers to observe the participants while collecting the data leading to more in-depth data collection (Yin, 2014).

Participants

The participants for the study were IT managers who manage, develop, implement, or maintain compliance programs and are members of a small IT firm located in the southwestern region of the United States. Leaders of the participating firm were willing to participate and allow access to interview participants. A set of inclusion or exclusion criteria is important in order to establish boundaries of the sample (Brown, 2013; Maskara, 2014). I obtained the interview participants through purposeful sampling. Previous researchers have used purposeful sampling to select individuals who have in-depth knowledge about the selected research topic (Palinkas et al., 2015). The selected study participants were not my work peers, associates, or family members.

First, I contacted the executive team of the participating organization to identify likely interview participants. Second, I provided letters of consent to each participant. Last, I provided a letter of cooperation for review and signature of an executive in the organization. Participants had the option of removing themselves from the study at any time (Comi, Bischof, & Eppler, 2014; Maskara, 2014; Yin, 2014). Data collected for this study did not identify the participating organizations or interview participants, which protected their anonymity.

Research Method and Design

The methodology and design of a study are vital to its success. I selected a qualitative single-case study design to explore and better understand best practices and methodologies deployed by organizations concerning information security. The objective of this qualitative research approach was to identify strategies that small businesses use to successfully monitor employees and reduce internal theft and loss.

Research Method

Researchers use one of three common research methods: qualitative, quantitative, and mixed methods (Turner, Kane, & Jackson, 2015). In this study, I used a qualitative research method. Researchers use qualitative research methods to explore and attempt to understand a phenomenon through the experiences of the research participants (Doody, & Noonan, 2013). Qualitative researchers attempt to understand contemporary issues in real-world settings (Barratt, Choi, & Li, 2011). I intended to explore the knowledge of IT managers; therefore, the qualitative method aligned well with the purpose of the study.

In contrast, quantitative researchers seek to determine relationships or differences among multiple variables and to testing hypotheses (Marshall & Rossman, 2016). The absence of a hypothesis in the study illustrates that the quantitative method and the mixed methods, which include the quantitative method, were not suited for this study (Bansal & Corley, 2012). The quantitative research method lacked compatibility due to the required resources and the absence of existing data to analyze. Therefore, quantitative and mixed method research was not appropriate for this study (Venkatesh et al., 2013; Yoshikawa et al., 2013).

Research Design

I used a single case-study design for the research. There are several designs available for DBA qualitative studies, including the (a) case study design, (b) phenomenological design, (c) ethnographic design, (d) narrative design, and (e) grounded theory design. The foundational research question for my single case study was, as follows: What strategies do information technology managers in small businesses use to successfully monitor employees and reduce internal theft and loss? Use of a single case-study design allowed me to focus on specific organizations’ processes while obtaining different types of data for addressing the purpose of the study (see Yin, 2014).

Before choosing to use a single case-study design, I examined other qualitative designs, such as the phenomenological design, ethnographic design, narrative design, and grounded theory design. I determined that a phenomenological design was not suitable, because the purpose of this study was not to explore the lived experiences of participants. In ethnographic design, the researcher studies cultural groups in a natural setting over a period of time (Mannay & Morgan, 2015). Ethnography was not suitable for the study, because I did not seek to study a specific cultural group for an extended period. The focus of the study was to understand approaches used to develop monitoring strategies instead of the individual experiences. Narrative researchers study the life of one or more individuals, giving an account of an event chronologically (Yin, 2014). The narrative design was not appropriate for the study. Last, the goal of grounded theory is to establish a new theory built on existing knowledge (Urquhart & Fernández, 2013). My study purpose did not entail the creation of new theories. Therefore, grounded theory was not an appropriate research design for this study.

Population and Sampling

The population of the study consisted of five IT managers within the participating IT firm in the southwestern region of the United States. To achieve the appropriate sampling, I used purposeful selection. Purposeful selection of interview participants allows researchers to capture communication-based on experiences and opinions in support of research (Palinkas et al., 2015). Purposeful sampling was the appropriate technique that met the needs of the study. Previous researchers used the approach to focus on selecting participants that experiences align and serve as rich sources of information (Palinkas et al., 2015). In addition, this form of sampling is absent of randomization but ensures participants selection meet the specific study criteria (Robinson, 2014). The criterion for the study includes having management experience, knowledge of theft monitoring systems, and success in implementing monitoring strategies to minimize fraud and theft.

In qualitative research, data saturation is the point in which the data contains no new concepts or themes (Fusch & Ness, 2015). Data saturation determines the sample size used in a study (O'Reilly & Parker, 2012; Walker, 2012). The limit of the sample size depends on the point of data saturation, which indicates there are no new data and themes that emerge from the study (Ando, Cousins, & Young, 2014). The interviews for my study included five IT managers depending on the ability to reach data saturation.

For the study, I ensured that the interview environment was comfortable for the participants. The interviews took place at quiet and relaxed location for each participant. Furthermore, I sought agreeance from each participant for the time and location of the one-on-one interview, face-to-face or via telephone. Higher quality collection results exist when participants feel comfortable (Ando et al., 2014; Cleary, Horsfall, & Hayter 2014; Trier-Bieniek, 2012).

I conducted follow-up interviews with two of the five participants of the study. The follow-up interviews were based on the output of the initial interview with participants. The purpose of the follow-up interviews was to correct the record based on feedback from member checking. I made all necessary corrections.

Ethical Research

I received Institutional Review Board (IRB) permission to interview participants prior to the collection of data for this study. The Walden University IRB reviewed my application for research, which included descriptions of methods used to protect the safety of the participants. Participants in the study received fair and ethical treatment throughout the study. In addition, participants who indicated interest in participating in the study received a copy of the consent form via e-mail. The consent form had a description of the invitation to participate and an introduction and the purpose of the study. The consent form included a disclaimer that no incentives or reimbursements are available for participating in the study. In the event of no response from the e-mail, the participant received a telephone call to confirm their participation interest.

The consent process required the participant to respond to the invitation e-mail and indicate their level of interest. Interested parties received a consent form for the study. The consent form ensured that participants were aware that participation in the study was voluntary. In addition, participants were able to withdraw prior to the start of the interview or at any time during the interview. Participants' identity remained confidential and the participants will have no need to identify themselves in the interview. The interview recordings and the interview data remained in a confidential, secure environment for a period of five years after completion of the research. The data remained in on a secure hard drive and a copy of the files will reside in the cloud service provided by Dropbox.

Dropbox is a cloud-based online repository that allows users to create backup copies of documents and files. Dropbox users can securely, store and retrieve copies of files from any location by logging in and downloading files. The hard drive backup and Dropbox website all require passwords to access data with plans to expunge them after five years.

Data Collection Instruments

The primary data collection method for the study was one-on-one interviews. Based on current research, interviewing is an appropriate approach to use for qualitative case studies (Comi et al., 2014; Maskara, 2014; Yin, 2014). During the interviews, I used voice recording and hand-written notes to capture the pertinent information from the interviews. I asked the participants' open-ended interview questions (see the appendix), which allowed for additional insight and a thorough exploration of the research questions. The process of member checking after the interview process provided reliability and validity during the data collection process. The process of member checking provided confirmation that recorded and transcribed sessions are credible and dependable (Marshall & Rossman, 2016; McCusker & Gunaydin, 2015). I conducted two follow up interviews after the member checking.

The information contained in the literature review provided a foundation for the interview questions and provides support for the study. During the interviews, all participants received the same interview questions in the same order. The concepts for exploration in the study were the themes identified in the literature review. Several elements in the literature review included security violation response, compliance programs, reduction of internal theft and loss, data breaches, data governance and policy, auditing, remote monitoring, and reporting. The present study did not include measurements of concepts or calculation of scores. The participants answered interview questions that addressed how the participants implemented compliance programs to reduce the risk of internal fraud and data breaches. Using open-ended interviews for the study had the advantage of capturing realistic data from experts in the industry.

Furthermore, using a well-developed interview protocol was vital to discussing the interview questions with each participant. For example, interviewing information technology leaders with experience in information security yielded valuable insights into reducing data theft and loss. In addition to the interview data, I included data from the company-established documentation.

Data Collection Technique

The purpose of this qualitative single case study was to explore strategies some information technology managers in small businesses use to monitor employees and reduce internal theft and loss. Using a digital recorder and handwritten notes, I conducted interviews with each research participant. All one-on-one interviews took place in a private area at the company worksite to encourage privacy and confidentiality. I digitally transcribed the interview using the TranscribeMe software. The process for data collection followed the Walden University IRB requirements.

I stored all digital information in a password-protected and encrypted storage system (Maskara, 2014; Spengler, 2015; Wilkinson, 2012). Encrypting and storing the data in a secure location prevented unauthorized access to the data. All digital and physical data captured during the study was stored in physical folders and locked in a secure location (Jacob & Furgerson, 2012). Walden IRB requires the destruction of all data for this study after 5 years of CAO approval. I will destroy the files after 5 years.

I provided each study participant with consent forms for the study. Upon receipt of the required consent forms, I provided each participant with a confirmation e-mail. A reminder e-mail was sent one day in advance of the interview appointment. The one-on-one interviews will consist of open-ended questions with the duration lasting 30 to 60 minutes (Maskara, 2014; Spengler, 2015; Wilkinson, 2012). The interviews were recorded using my laptop computer and additional notes recorded on a physical notepad.

I coded the interview responses based on common themes to identify emerging themes within the data. Coding is a technique used to organize and categorize information gathered from interviews (Rowlands, Waddell, & Mckenna, 2015). Member checking was used to address the issue of incorrect interpretation and inaccuracy of interview data is important (Yin, 2014). In addition, secondary data sources were used as part of the data collection process. The secondary data source consisted of documentation and will come from the organization under study (Maskara, 2014; Spengler, 2015; Wilkinson, 2012).

Data Organization Technique

I used the cloud-based storage system called Dropbox to capture digital files and folders containing data from the study. One folder contained the interviews and a separate folder houses the documentation of the secondary data sources. All audio files of the interviews are stored in a separate folder. In addition, a standard naming convention was adopted for all digital files captured during the study. For example, files pertaining to the first and second participant were labelled, Company1-Participant 1- Interview, Company1-Participant 2 - Interview, etc. The transcribed files for each audio recording of the interview is stored in a separate folder using the same naming convention. A separate Microsoft Word file was created for each interview participants and use the same naming convention for each interview as Participant 1, Participant 2. All hard copies of documentation were converted to an electronic format and will be maintained for five years, followed by deletion. The hard copy sources followed the process of conversion to electronic format through scanning, then destruction.

Data Analysis

I used the study to answer the following research question: What strategies do information technology managers in small businesses use to successfully monitor employees and reduce internal theft and loss? Data analysis followed the inductive strategy of (a) compiling the data, (b) disassembling the data into codes, (c) reassembling the data into themes, (d) interpreting the meaning of the data by applying critical thinking, and (e) concluding the data (Brown, 2013; Thomas, 2015; Yin, 2014). After interviewing all participants and gathering all the data, I analyzed the data.

The most appropriate data analysis technique is to collect data from interviews and a secondary data source; which consisted of documentation that came from the organization under study (Ando et al., 2014; Cleary, Horsfall, & Hayter 2014; Trier-Bieniek, 2012). I used data triangulation to support the validity of the interviews during the study. Data triangulation strengthens data validation by leveraging two or more sources for verification (Yin, 2014). During the data analysis phase, I listened to the recorded interviews and reviewed the documentation provided by the participating organization. I used the NVivo 12 software to sort, code, and organize the data obtained from my research. I then imported, sorted, coded, and organized the data, and transcribed the audio recording of the interviews using a service called TranscribeMe. The final write-up of my study included the conclusion of the data.

Reliability and Validity

Reliability is a concern in qualitative research, especially case studies (Zivkovic, 2012). Methods to enhance reliability include using multiple sources of data, check transcripts for possible errors and use formalized software to analyze interview data (Barratt et al., 2011; Baysal, Holmes, & Godfrey, 2013). An additional method for increasing reliability is the process known as member checking, which is a process of building trust between a researcher and a participant by allowing the member to check the interpretation of the responses prior to inclusion in the final report (Carlson, 2010). Carlson (2010) provided five methods of avoiding traps in member checking: (a) prior determination of the member checking procedures, (b) prior determination of the extent of the transcripts needed, (c) prior determination of the precision of language needed for the final report, (d) informing participants of the member checking procedures, and (e) prior determination of the use of narratives.

Validity is the demonstrated accuracy of the results and determines a study's applicability and replicability of findings (Calipinar & Soysal, 2012). To address the validity of the study, I used known research processes that will allow future researchers to determine my conclusions' validity, and determine the study's potential for application for other populations. The processes selected for the study are standard in qualitative case studies and will lead to confirmability within the study. Achieving data saturation for this study is based on the selection and fit of the interview participants. Participant alignment with the research ensures that there will be enough data to analyze and present (Sutanto, Palme, Chuan-Hoo, & Chee Wei, 2013).

This study included member-checking methods to enhance reliability, which met the intent of prior determination of member checking procedures. The consent form included information on how participants can receive a transcribed copy of the interview, which met the intent of informing participants about the member checking procedure employed for this study. The consent form included disclaimers that the final report would use selected portions of the transcripts and responses would receive editing to ensure proper grammar. These methods supported the guidelines related to transcripts.

Transition and Summary

The purpose of the study was to explore strategies some information technology managers in small businesses use to monitor employees and reduce internal theft and loss. The two sources of data for the study will be one-on-one, semi-structured interviews and corporate documentation (Brown, 2013; Maskara, 2014; Yin, 2014). The research problem was appropriate for a qualitative single case study design for data collection because I explored the knowledge of IT managers. Section 2 includes descriptions of the participant population, eligibility to participate in the study, consent procedures, data collection, data organization, and data analysis techniques. The data analysis consisted of searching for re-occurrences and themes to answer the central research question of the study (Lee, 2014; Thomas, 2015; Yin, 2014). In addition, the section covers the methods to enhance reliability and validity during the duration of the study. Section 3 includes the presentation of findings from the data collection and conclude with potential implications for social change and further areas of research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative single-case study was to explore strategies some IT managers in small businesses use to monitor employees and reduce internal theft and loss. Based on the formulated research question and the responses obtained from the study participants, I identified two major themes. The first theme was the development of policies, procedures, and standards on internal theft and loss. The second theme was the use of technology-driven systems to monitor employees and control theft and loss. In Section 3, I explore the research problem and discuss the study findings and their application to professional practice. The section includes implications for social change, recommendations for action and further research, reflections, and conclusions.

Presentation of the Findings

To achieve the objective of the study and answer the research question, I conducted one-on-one semistructured interviews with five IT managers in a small business in the southwestern region of the United States. The participants were small businesses owners who had managed to successfully monitor their employees and reduce internal theft and loss. Throughout the interview sessions, the focus was on determining the strategies that the business owners and managers used to protect the organization and prevent data breaches to protect community members from exposure of personal information. During the participant interviews, I used voice recording and handwritten notes to store and capture relevant and pertinent information from the participants. Every participant responded to the same series of open-ended questions and provided additional insights into the issue of data security. I ensured that the interviews were conducted in a private location within the company worksite for privacy and confidentiality reasons. Each participant was given a unique code that I used both in the data collection and the data analysis process to ensure that the identity of the participants was masked. The participants were identified by using the codes Participant 1, Participant 2, Participant 3, Participant 4, and Participant 5. The unique codes were used throughout the study. The interviews were digitally transcribed using the TranscribeMe software.

The next step after collecting the data was to code and analyze the interview responses based on common themes. The data analysis process followed the inductive strategy (Merriam, 2015). The process entailed (a) compiling the data, (b) disassembling the data into codes, (c) reassembling the data into themes, (d) interpreting the meaning of the data by applying critical thinking, and (e) drawing a conclusion based on the responses from the participants and previous literature. Every participant provided information and responses that related to the strategies they often adopted to monitor employees and prevent loss and theft. Thus, it was imperative to carefully and systematically examine the major themes in the responses. To explore the themes, I referred to previous studies and literature related to employee monitoring and the prevention of loss and theft in small business (see Hess & Cottrell, 2016) to help in analyzing the responses. My primary goal during data analysis was to make sense of the data collected during the interviews and use the information as the basis for answering the formulated research question.

At the end of data coding process and analysis, two primary themes emerged: (a) development of policies, procedures, and standards on internal theft and loss and (b) use of technology-driven systems to monitor employees and control theft and loss. The two themes reflected on the responses that the five participants provided and gave insight into the mechanisms and strategies that the small businesses in question adopted to reduce loss and theft.

Table 1 and 2 show the themes and keywords/phrases that were derived from the five interviews. The tables have two major sections. The first is the participant response column that gives the specific words and phrases that participants discussed in support of the theme in question. The second column shows the number of participants who mentioned the words and phrases related to the theme. Table 1 includes an overview of participant responses related to Theme 1.

Table 1

Theme 1: Development of Policies, Procedures, and Standards on Internal Theft and Loss

Words and phrases in participant responses	Number of participants
Standards	1
Operating procedures	3
Security standards/rules	5
Policies	2

Note. The first column includes the participant responses linked to the theme. The second column includes the number of manager participants who used each word or phrase when answering the interview questions.

Theme 1: Development of Policies, Procedures, and Standards on Internal Theft and Loss

During the interview, the managers agreed that the development and use of appropriate policies, procedures, and standards are critical to the prevention and control of internal theft and loss. The participants stated that the development of policies, procedures, and standards not only help in the identification of the threat of fraud and loss but also aids with developing mechanisms and ways of managing threats. Participant 1 noted, “the organization has developed clear operating standards and procedures that the IT and security team use to identify and deal with breaches.” While addressing fraud issues, Participant 1 stated that

> We have a security personnel on staff that they and then they make sure all our computers have the security on them that we need to safeguard it from getting anything. We have also we make sure everything’s locked up. Any paper type things that I have, I make sure that they’re under lock and key and lock the door.

Participant 1 further stated, “we had our security manager, IT manager, everyone kind of working together to create the proper processes.” Upon further questioning, Participant 1 noted “the creation of proper procedures helps managers and employees to deal with breaches of the safety and security of important data. Thus, procedures are critical to the success of the business in the competitive world.”

From the responses, it is evident that Participant 1 is aware that some employees may be tempted to steal from their employers or engage in fraud. Some of the issues that may drive employees into fraud and internal theft include financial need, greed, and pressure from colleagues (Boersma, 2016). Whatever the reason, organizations need policies and procedures that can successfully prevent and deter theft and fraud (Hess & Cottrell, 2016). Organizations take different steps to deter theft and fraud. In the case of the organization where Participant 1 works, the process of preventing theft and fraud entails creating a policy where a security manager works with other employees and individuals to secure the available resources per the company standard operating procedures. Participant 3 noted the application of the security policies in the workplace. The participant's statements were consistent with Willison and Warkentin's (2013) conclusion that, without appropriate security policy in place, organizations may have increased difficulty regarding selling to the consumer and protecting private information. I used additional interview questions to probe more on the topic of organizational policies.

Participant 3 stated that

> I guess it comes back to-- I've only been using the approved areas where they tell me [inaudible]. We have a confluence site for collaborating or emailing them with our email banner at the bottom. If every email we send, read the [inaudible] fine print. It could be some of this is proprietary. This could be confidential. Don't share this without asking me. Kind of a big deal [inaudible]. So that's how I try to do it. Like I said, don't put data-- I don't stick it on a thumb drive. I don't--

From the responses provided in this case, it seems that the employees know their employer has security and IT managers who work together to prevent fraud and theft.

The clear communication of the policies helps with deterring and preventing incidents within the organization.

Another issue that Participant 1 raised regarding antitheft policies and procedures related to security clearance include the following:

> We've had to do training especially, like I said, the guys that have security clearances, they have training that they're constantly doing. I not so much, so it's just myself. It's more what we do on the outside and just the one program we started so.

The above statement implies that the organization provides a specific group of people access to critical information and areas. The intention is to prevent and deter theft and fraud cases that may cost the organization a lot of money and damage the company reputation within the market. While addressing the threats, Participant 1 stated "they set up what they called a UDN, an Unclassified Data Network, that was independent and had its own higher security standards for protecting the data that was used in experiments that could become new products."

A careful analysis of the responses provided by Participant 1 revealed the organization has policies related to the process of reporting theft and fraud. During the interviews, Participant 1 said:

> Well, we've done a training class just recently actually to let them know to be aware of it can be anybody and you need to report what you see or hear that you think may be an issue. That's I think that's the only thing I can think of is that and I am not inside so I can't, I'm not sure all that they do in there.

This statement implies that the organization expects employees to report cases of theft and fraud. The immediate and prompt reporting of such cases allows organizations to take appropriate measures to prevent further losses. Participant 2 also alluded to the importance of security procedures in the prevention of internal theft and fraud. The respondent said:

> I've been a reviewer of-- when we created our standard operating procedures, and then when we were working to become [inaudible] compliant, we had our security manager, IT manager, everyone kind of working together to create the proper processes. I was more of a reviewer in that process, but also did provide some inputs on what could be the outcome if we had a data breach, and what type of data.

According to Participant 1, the security procedures and policies help the organization to protect classified data and vital company and trade secrets. Participant 5, on the other hand, discussed the significance of security standards when dealing with the access and storage of critical data. Participant 1 noted "there is always the risk of unauthorized individuals accessing information in the classified networks." Thus, it is imperative to develop procedures, standards, and policies that protect important company data. According to Participant 5, "however, the use of existing security standards and policies may be problematic especially when the organization deals with subcontractors and external stakeholders." In this regard, Participant 5 stated:

> Then if a subcontractor were working for another company, increasingly they don't want us to store their proprietary information on our systems. Even though

> we try to follow the same security rules and provide the same kind of infrastructure to protect our IT systems, increasingly they just don’t want the proprietary information stored on our systems.

Participant 5 strived to explain:

> Even though the organization has security standards and policies, challenges are bound to arise when dealing with external parties and stakeholders such as subcontractors. Even in such contexts, however, the organization strives to protect its systems by sticking to the laid down security policies and standards. Furthermore, it encourages employees to protect the integrity of the IT system and contribute towards the fraud and theft prevention efforts.

The theme of the significance of policies, procedures, and standards in preventing internal theft and loss is consistent with existing literature. Research showed that employee theft and internal fraud are costly to businesses (Moorthy, Nahariah, & Foong, 2015). A broad range of organizational, workplace, and individual factors tend to influence theft and fraud behaviours. Therefore, it is important for enterprises to develop internal control procedures and mechanism that can change worker behaviour and minimize theft and fraud. According to Moorthy et al. (2015), formal monitoring procedures and security policies and standards can deter employee theft and fraud. These interventions work by increasing the cost of stealing. When employees know that the organization is monitoring their activities and has procedures and policies for dealing with theft, they are less likely to engage in such behaviours (Moorthy et al., 2015). In other cases, however, some employees find ways of circumventing the existing controls and security policies to engage in theft and fraud (Kennedy, 2015). Thus, other workers must play their role by monitoring behavior of their colleagues and reporting any case of fraud and theft.

Previous studies have shown that managers and business leaders have a critical role to play in limiting the exposure of their organizations to loss, theft, and fraud (Dawson et al., 2016 & Moorthy et al., 2015). Paulsen and Toth (2016) noted that small businesses are a prime target for fraud and theft by individuals who are inside and outside the organization. When the cases of fraud and theft occur, the small business may lose a significant amount of resources. Furthermore, continued theft and fraud may damage the reputation of the organization and hinder the achievement of short term and long-term business goals. Thus, they must work hard and invest in appropriate procedures and policies that will prevent both internal and external theft and threats (Kuypers et al., 2016). Furthermore, organizational leaders should develop robust and appropriate standards that help with identifying the threats early enough and providing a framework for their management.

In this globalized and dynamic world, business leaders face a wide range of security threats such as cyber-attacks that may affect operations and success in the market (Moussa, 2015). In addition, these threats can lead to significant loss of important information and market share. Organizational leaders that fail to deal with threats are likely to lose their competitive edge in the market and achieve short-term and long-term business goals and objectives. Dawson et al. (2016) posited that small business owners have no choice but to develop antifraud and internal control programs and measures to monitor and manage such threats. Furthermore, organizational leaders need procedures and standards that can help in identifying, assessing, and documenting the threats. Vousinas (2015) stated the frameworks and policies that organizational leaders adapt to manage threats depends on the understanding of the work process, nature of the events, and the need to engage in periodic investigations. Irrespective of the threat in question, managers have a key role to play in developing the internal control mechanism and procedures while ensuring that employees conform all time. Furthermore, managers should constantly use existing procedures and controls to detect and prevent loss and fraud in the respective organizations.

Theme 2: Use of Technology-Driven Systems to Monitor Employees and Control Theft and Loss

The second major theme that was evident during the data analysis process was the use of technology-driven systems to monitor employees and control theft and loss. Those who participated in the study argued that the businesses face a wide range of threats that can adversely impact operations. Therefore, the organizational leaders require technology-based systems and solutions that can remotely monitor employees and identify threats. Furthermore, the systems are developed in such a way to prevent threats from creating a negative impact on the processes and operations of the business. Table 2 includes an overview of participant responses related to Theme 2.

Table 2

Theme 2: Use of Technology-Driven Systems to Monitor Employees and Control Theft and Loss

Words and phrases in participant responses	Number of participants
Network security	3
Software	3
Intrusion detection	1
Data integrity	4

Note. The first column includes the participant responses linked to the theme. The second column includes the number of manager participants who used each word or phrase when answering the interview questions.

Participant 3 made references to the existence of a system that secures communication between employees and other people who interact with the business. Participant 3 noted the following:

> I don’t know if I’ve implemented any strategies, and you said personal strategies. I don’t discuss any-- for emails, I only use the work email for work, and I only use the work-approved communication channels for [crosstalk]. So, there’s that piece. I don’t use personal devices for accessing any of the company data. I only use the company-provided resources. Yeah. And for the first part, I also-- any information or data I generate is going to the company system.

The above statements from the participantaffirms the existence of a secure communication platform and system that protects the organization from external and internal attacks. Furthermore, showing that the organization provides secure resources that are meant to mitigate external threats that may affect operations.

Similar sentiments were raised by Participant 2 and 5 during the interview. Participant 4 stated that:

> Probably the biggest thing as far as data security goes is we have intruder detection set up, and we also have firewalls installed that actually capture the data as it's going in and out of the network. So, because we're a small business, we use a lot of open-source as well.

The firewall that the respondent discussed is meant to prevent cyber-attacks and unwarranted access to the organization's IT system. Participant 5, on the other hand, discussed the existence of security devices in their organization. The participant stated "we had these little devices we would put on our belt. Digital pedometers that would monitor our steps." "The "little devices", in this case, are security tools that help the organization to monitor employees from time to time."

Participant 5 went on to discuss how they use technological solutions and measures to prevent fraud and theft when working with external parties and subcontractors. Participant 5 stated:

> And on the activities, that involve new R&D, all the emails that we send among team members using the corporate laptops must be further encrypted and digitally signed. And in a way, that's good for Company because, in those areas where the [Company] is most concerned about protecting the information, there's just no way we could do anything wrong if we follow those rules. And so that protects us.

The above statements indicate organizational leaders such as where Participant 5 works, believe in the use of technology-based systems and devices to monitor employees and prevent theft and loss in the place of work. Furthermore, the leaders within the organization demonstrate the role of technology-based tools in fraud and theft prevention in small organizations. These measures allow the organization to remotely monitor employees and guarantee the security of its resources and critical corporate data.

The use of technology-based tools to monitor employees and prevent theft and loss is a concept featured in previous studies. Researchers have noted that modern business leaders rely on advanced technologies that allow for identifying, analyzing, and responding to threats emanating from the cyberspace and other internal and external sources. Karadsheh and Alhawari (2014) determined small business leaders have tried to embrace technologies such as cloud computing with the goal of securing operations and data. The author, however, noted that such organizations face multiple challenges while trying to use technology. The commonly identified problems and risks include the lack of appropriate security policies, volume of private information to be protected, and the lack of an appropriate infrastructure within the enterprise (Dawson et al., 2016). These challenges, notwithstanding, technology provides an excellent avenue through which modern enterprises can secure systems and prevent loss and theft.

In other cases, researchers have argued that one of the main reasons why small business leaders face fraud and theft is employees are given access to critical organization data and secrets (Watkins, Coopman, Hart, & Walker, 2007). In such cases, the employees can access the information needed and manipulate the information to obtain goals (Willison et al., 2016). Other employees engage in fraudulent activities because they know how to hide details and information about the actions of the managers or owners of the enterprise. Therefore, the protection of information and data is something that organizations must work towards achieving in the modern world (Vousinas, 2015). Through innovative technologies such as cloud computing and other data security systems, a small business can prevent cases of theft and prevent employees from engaging in fraud.

Applications to Professional Practice

The study is relevant to the identification and understanding of the strategies that information technology managers in small businesses use to successfully monitor employees and reduce internal theft and loss. Information technology managers have a key role to play in securing the organization and ensuring that the systems are not prone to attack from both external and internal sources. Thus, these managers may find the above-identified strategies useful to their work. IT managers may develop and use the identified strategies to help deal with problems of theft and loss. In the long run, these initiatives will help the information technology managers to effectively help the organization to achieve short-term and long-term business goals.

Implications for Social Change

The results of the study may lead to positive social change within small businesses by providing compliance techniques that prevent loss of both organization and customers’ data. The participants consisted of five IT managers within the participating IT firm in the southwestern region of the United States. The responses provided by the participants’ indicated small businesses face several threats that lead to theft, fraud, and loss. Thus, there is a need to come up with better strategies for dealing with the problems.

By implementing or developing interventions that are in line with the above strategies, the managers will be able to deal with the problem of theft and loss within the organization. Furthermore, those who may be tempted to engage in theft may have to think twice about it because necessary measures have been put in place to mitigate the menace.

Recommendations for Action

The role of the information technology manager is to help with the security of business processes, systems, and resources. Therefore, it is imperative to consider the interventions and strategies that can help in securing the enterprise, monitoring employees, and preventing external attacks such as cyber threats. Based on the results of this study, there are two major recommendations that can help such managers carry out their duties effectively and secure the organization. First, developing and implementing security policies, standards, and procedures that are geared towards securing the enterprise and the system. All employees should be aware of such policies and procedures to contribute towards the goal of securing the small business. Secondly, managers should use technological advanced platforms and systems such as cloud computing to protect the systems and critical data. While making a choice on the right technology, attention should be given to factors such as cost, availability of resources, and the operation of the enterprise.

Recommendations for Further Research

The results of this study could provide critical insights that organizational leaders can use to secure systems and processes. Furthermore, the results of the study include vital tips that can help information technology managers succeed in their roles. Like any other study, this project has some limitations that can be addressed through further research. First, the use of face-to-face semistructured interviews, coupled with time constraints, limited the amount and volumes of data gathered and used to answer the formulated research question. Future studies can use more appropriate and effective methods such as questionnaires to gather detailed accounts of the strategies used to prevent loss and theft. Secondly, the small sample size in this study was a significant limitation that may have affected the validity and applicability of the findings. Future studies could use a larger sample size to improve the validity and reliability of the findings.

Reflections

The process of working on this project has been a challenging yet fulfilling journey. At the start, it appeared to be a huge task that would take a long time and energy to bring to completion. However, through commitment and passion, I have been able to successfully carry out the study. More importantly, I have managed to determine some of the major strategies that small business leaders use to prevent threat and loss. From the data collected during the face to face interview, I found that leaders of small organizations can use security procedures, standards, and policies and technology-based platforms to deal with the menace of theft and loss. These interventions can also help the organizations to monitor employees and ensure that they focus on helping the enterprise to achieve its goals and objectives.

By taking part in this project, I have been able to learn a lot about the operations of small businesses. First, I have appreciated the fact that such enterprises face a wide range of security challenges that may affect operations and compromise business growth and development. Secondly, I have learned that managers have a critical role to play in dealing with such threats. Finally, it is evident that there are reliable interventions and systems that the organizations can use to prevent theft and loss. Therefore, information technology managers should always review their environment in which they work and select the most appropriate method of mitigating the threats.

Conclusion

The purpose of this study was to identify and understand the strategies that information technology managers in small businesses use to successfully monitor employees, and reduce internal theft and loss. To achieve this goal, five participants were interviewed and the responses provided used as the basis for answering the research question. The data collected in the study indicated a wide range of avenues that organizations use to monitor employees and reduce internal theft and loss. A thematic analysis of the data revealed two major approaches that cut across the enterprises that were considered in this study. First, the organizational leaders can develop policies, procedures, and standards on internal theft and loss. Secondly, small businesses can use technology-driven systems to monitor employees and control theft and loss. The successful use of these interventions can help the organizations to monitor employees, reduce internal theft and loss, and achieve short-term and long-term business goals.

References

Adams, G. W., Campbell, D. R., Campbell, M., & Rose, M. P. (2006). Fraud prevention. *The CPA Journal, 76*(1), 56. Retrieved from https://www.cpajournal.com/

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology, 3*(4), 1-7. doi:10.2466/03.CP.3.4

Badrul, N. A., Williams, S. A., & Lundqvist, K. Ø. (2016). Online disclosure of employment information: Exploring Malaysian government employees' views in different contexts. *ACM SIGCAS Computers and Society, 45*(3), 38-44. doi:10.1145/2874239.2874245

Bansal, P., & Corley, K. (2012). Publishing in AMJ—Part 7: What's different about qualitative research? *Academy of Management Journal, 55*, 509-513. doi:10.5465/amj.2012.4003

Barratt, M., Choi, T. Y., & Li, M. (2011). Qualitative case studies in operations management: Trends, research outcomes, and future research implications. *Journal of Operations Management, 29*, 329-342. doi:10.1016/j.jom.2010.06.002

Baysal, O., Holmes, R., & Godfrey, M. W. (2013). Developer dashboards: The need for qualitative analytics. *IEEE Software, 30*(4), 46-52. doi:10.1109/MS.2013.66

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*, 573-578. doi:10.1111/isj.12092

Bhattacharya, D. (2015). Evolution of cybersecurity issues in small businesses. *Proceedings of the 4th Annual ACM Conference on Research in Information Technology*, 11. doi:10.1145/2808062.2808063

Bibi, Z., Karim, J., & ud Din, S. (2013). Workplace incivility and counterproductive work behavior: Moderating role of emotional intelligence. *Pakistan Journal of Psychological Research*, *28*, 317. Retrieved from http://www.pjprnip.edu.pk

Boersma, K. (2016). Reporting corporate theft: Breaking the taboo. *Organization*, *13*(1), 48. doi:10.1080/15416518.2016.1152065

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber-crime. *International Journal of Cyber Criminology*, *8*(1), 1-20. Retrieved from http://www.cybercrimejournal.com

Brown, M. E. (2013). *Data-driven decision making as a tool to improve software development productivity* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 1435602894)

Brunswicker, S., & Vanhaverbeke, W. (2015). Open innovation in small and medium-sized enterprises (SMEs): External knowledge sourcing strategies and internal organizational facilitators. *Journal of Small Business Management*, *53*, 1241-1263. doi:10.1111/jsbm.12120

Calipinar, H., & Soysal, M. (2012). E-Procurement: A case study about the health sector in Turkey. *International Journal of Business and Social Science, 3,* 232-244. Retrieved from http://www.ijbssnet.com/update/

Carlson, J. A. (2010). Avoiding traps in member checking, *The Qualitative Report*, *15*, 1102-1113. Retrieved from http://www.nova.edu/

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing*, *70*, 473-475. doi:10.1111/jan.12163

Coffie, M. R. (2013). The impact of social venture capital and social entrepreneurship on poverty reduction. Retrieved from ProQuest Dissertations and Theses database. (Order No. 3556987)

Comi, A., Bischof, N., & Eppler, M. J. (2014). Beyond projection: Using collaborative visualization to conduct qualitative interviews. *Qualitative Research in Organizations and Management: An International Journal*, *9*(2), 110–133. doi:10.1108/QROM-05-2012-1074

Corley, K. G. (2015). A commentary on “What grounded theory is…” Engaging a phenomenon from the perspective of those living it. *Organizational Research Methods*, *18*, 600-605. doi:10.1177/1094428115574747

Chiemela, I., (2014). Workplace e-monitoring and surveillance of employees: Indirect tool of information gathering. *International Journal of Science and Research, 3,* 2349-2353. Retrieved from http://www.ijsr.net

Dahmen, P., & Rodríguez, E. (2014). Financial literacy and the success of small businesses: An observation from a small business development center. *Numeracy*, *7*(1), 3. doi:10.5038/1936-4660.7.1.3

Dawson, M., Dawson, M., Eltayeb, M., & Omar, M. (2016). *Security Solutions for*

Hyperconnectivity and the Internet of Things. IGI Global

De Clercq, D., Bouckenooghe, D., Raja, U., & Matsyborska, G. (2014). Unpacking the goal congruence–organizational deviance relationship: The roles of work engagement and emotional intelligence. *Journal of Business Ethics*, *124*, 695-711. doi:10.1007/s10551-013-1902-0

Dion, M. (2008). Ethical leadership and crime prevention in the organizational setting. *Journal of Financial Crime*, *15*, 308-319. doi:10.1108/13590790810882892

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher, 20*(5), 28-32. doi:10.7748/nr2013.05.20.5.28.e327

Dunne, J. (2014). Small business occupational fraud. Lasalle University, Philadelphia, PA. Retrieved from http://digitalcommons.lasalle.edu/

Fernandes, L. M. (2014). Emerging security risks and threats to accounting information systems in the rapid changing environment: Implications to management and accountants. *ZENITH International Journal of Multidisciplinary Research, 4*(6), 64-72. Retrieved from http://www.indianjournals.com/

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20,* 1408-1416. Retrieved from http://tqr.nova.edu/

Gelens, J., Dries, N., Hofmans, J., & Pepermans, R. (2013). The role of perceived organizational justice in shaping the outcomes of talent management: A research agenda. *Human Resource Management Review*, *23*, 341-353. doi:10.1016/j.hrmr.2013.05.005

Goh, E., & Kong, S. (2016). Theft in the hotel workplace: Exploring frontline employees' perceptions towards hotel employee theft. *Tourism and Hospitality Research*, doi:10.1177/1467358416683770

Hess, M. F., & Cottrell, J. H. (2016). Fraud risk management: A small business perspective. *Business Horizons*, *59*(1), 13-18. doi:10.1016/j.bushor.2015.09.005

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2014). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52,* 337-347. doi:10.1016/j.im.2014.12.006

Holland, P. J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review, 44*, 161-175. doi:10.1108/PR-11-2013-0211

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigor in qualitative case-study research. *Nurse Researcher, 20*(4), 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Isenring, G. L., Mugellini, G., & Killias, M. (2016). The willingness to report employee offences to the police in the business sector. *European Journal of Criminology*, *13*, 372-392. doi:10.1177/1477370815623569

Jaakson, K., Vadi, M., Baumane-Vitolina, I., & Sumilo, E. (2017). Virtue in small business in small places: Organisational factors associated with employee dishonest behaviour in the retail sector. *Journal of Retailing and Consumer Services, 34*, 168-176. doi:10.1016/j.jretconser.2016.09.017

Jacob, S. A., & Furgerson, S. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *Qualitative*

Report, *17*, 1-10. Retrieved from http://www.nova.edu/ssss/QR/QR17/jacob

Karadsheh, L., & Alhawari, S. (2014). Applying security policies in small business utilizing cloud computing technologies. In *Cloud Computing Advancements in Design, Implementation, and Technologies* (pp. 112-124). IGI Global.

Kennedy, J. P. (2015). Functional redundancy as a response to employee theft within small businesses. *Security Journal*, *30*(1), 162-183. doi:10.1057/sj.2015.37

Kennedy, J. P. (2016a). Employee theft. *The Oxford Handbook of White-Collar Crime*, 409.

Kennedy, J. P. (2016b). Shedding light on employee theft's dark figure: A typology of employee theft nonreporting rationalizations. *Organization Management Journal*, *13*(1), 49-60. doi:10.1080/15416518.2015.1110513

Kennedy, J. P., & Benson, M. L. (2016). Emotional reactions to employee theft and the managerial dilemmas small business owners face. *Criminal Justice Review, 41*, 257-277. doi:10.1177/0734016816638899

Khatri, V., & Brown, C. (2010). Designing data governance. *Communications of the ACM, 53*(1), 148-152. doi:10.1145/1629175.1629210

Knott, C., & Steube, G. (2011). Encryption and portable data storage. *Journal of Service Science, 4*(1), 21-30. Retrieved from http://servsci.journal.informs.org/

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64,* 122-134. doi.org/10.1016/j.cose.2015.07.002

Krishnakumar, S., Hopkins, K., & Robinson, M. D. (2017). When feeling poorly at work does not mean acting poorly at work: The moderating role of work-related emotional intelligence. *Motivation and Emotion, 41*(1), 122-134. Retrieved from http://www.springer.com

Kumar, A., Bhatia, S., & Chiang, I. (2013). Deployment of an in-house designed training process in a quaternary care hospital. *Technology & Health Care, 21*, 469-478. doi:10.3233/THC-130750

Kuypers, M. A., Maillart, T., & Paté-Cornell, E. (2016). An empirical analysis of cyber security incidents at a large organization. *Department of Management Science and Engineering, Stanford University, School of Information,* UC Berkeley. Retrieved from http://fsi.stanford.edu/

Lee, Y. -A. (2014), Insight for writing a qualitative research paper. *Family and Consumer Sciences Research Journal*, *43*(1), 94–97. doi:10.1111/fcsr.12084

Liu, S. M., Liao, J. Q., & Wei, H. (2015). Authentic leadership and whistleblowing: Mediating roles of psychological safety and personal identification. *Journal of Business Ethics*, *131*(1), 107-119. doi:10.1007/s10551-014-2271-z

Macfarlane, F., Barton-Sweeney, C., Woodard, F., & Greenhalgh, T. (2013). Achieving and sustaining profound institutional change in healthcare: case study using neo-institutional theory. *Social Science & Medicine, 80*, 10-18. doi.org/10.1016/j.socscimed.2013.01.005

MacGregor, J., & Stuebs, M. (2014). Whistle while you work: Whistleblowing in the presence of competing incentives and pressures. *Accounting Perspectives, 13*(4), 309-324. doi:10.1111/1911-3838.12038

Mannay, D., & Morgan, M. (2015). Doing ethnography or applying a qualitative technique? Reflections from the ‘waiting field’. *Qualitative Research, 15*(2), 166-182. doi:10.1177/1468794113517391.

Marshall, C., & Rossman, G. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36-58. doi:10.1509/jm.15.0497

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155. doi:10.1007/ s11747-016-0495-4

Maskara, A. (2014). *A process framework for managing quality of service in private cloud* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3636194)

Merriam, S. B. (2015). Qualitative Research: Designing, Implementing, and Publishing a Study. *In Handbook of Research on Scholarly Publishing and Research Methods* (pp. 125-140). IGI Global.

Moorthy, M. K., Seetharaman, A., Jaffar, N., & Foong, Y. P. (2015). Employee perceptions of workplace theft behavior: A study among supermarket retail employees in Malaysia. *Ethics & Behavior, 25*(1), 61-85. doi:10.1080/10508422.2014.917416

Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in America. *SAGE Open*, *5*(2), 1–13. doi:10.1177/2158244015580168

Moustakas, C. (1994). *Phenomenological research methods.* Thousand Oaks, CA: Sage Publications Inc.

Murthy, D. (2013). Ethnographic research 2.0: The potentialities of emergent digital technologies for qualitative organizational research. *Journal of Organizational Ethnography, 2*(1), 23–36. doi:10.1108/JOE-01-2012-0008

Ong, J. T. B. (2016). Self-leadership coaching for employees during organisational change. Retrieved from http://www.epubs.scu.edu.au

O'Reilly, M., & Parker, N. (2012). "Unsatisfactory saturation": A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research, 13,* 190-197. doi:10.1177/1468794112446106

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health, 42*(5), 533–544. doi:10.1007/s10488-013-0528-y

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, *49*(8), 92-97. doi:10.1109/MC.2016.223

Paulsen, C., & Toth, P. (2016). Small business information security. U.S. Department of Commerce. doi:10.6028/NIST.IR.7621r1

Rennie, D. L. (2012). Qualitative research as methodical hermeneutics. *Psychological Methods, 17,* 385–398. doi:10.1037/a0029250

Rezaee, Z. (2002). *Financial statement fraud: Prevention and detection*. John Wiley & Sons.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*, 25-41. doi:10.1080/14780887.2013.801543

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2), 256-286. doi:10.1002/pam.20567

Rowlands, T., Waddell, N., & Mckenna, B. (2015). Are we there yet? A technique to determine theoretical saturation. *Journal of Computer Information Systems, 56*(1), 40-47. doi:10.1177/1049732311401424

Rupp, D. E., Shapiro, D. L., Folger, R., Skarlicki, D. P., & Shao, R. (2017). A critical analysis of the conceptualization and measurement of organizational justice: Is it time for reassessment?. *Academy of Management Annals, 11*(2), 919-959. doi:10.5465/annals.2014.0051

Sankoloba, T., & Swami, B. N. (2014). Impact of internal controls in managing resources of small business: Case study of Botswana. *Journal of Small Business and Entrepreneurship Development, 2*(2), 87-105. Retrieved from http://jsbednet.com/

Scott, M. E. (2015). *Strategies for retaining employees in the hospitality industry* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3738026)

Shaheen, S. A., Martin, E. W., Cohen, A. P., Chan, N. D., & Pogodzinski, M. (2014).

Public bikesharing in North America during a period of rapid expansion: Understanding business models, industry trends & user impacts. *MTI Report*, 12-29. Retrieved from http://transweb.sjsu.edu

Smith, S. A. & Brunner, S. R. (2017). To reveal or conceal: Using communication privacy management theory to understand disclosures in the workplace. *Management Communication Quarterly*, doi:10.1177/0893318917692896

Spengler, S. S. (2015). *Educators' perceptions of a 21st century digital literacy framework* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3701210)

Stanton, J. M. (2002). Information technology: A boundary management perspective. In S. Clarke, E. Coakes, G, Hunter and A. Wenn (Eds), *Sociotechnical and Human Cognition Elements of Information System.* (pp. 79-103). London, England: Idea Group.

Stanton, J. M., & Stam, K. R. (2002). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance & Society, 1*(2), 152-190. Retrieved from http://www.surveillance-and-society.org

Stanton, J. M. (2003). Information technology and privacy: A boundary management perspective. In Socio-technical and human cognition elements of information systems. *IGI Global*, 79-103. doi:10.4018/978-1-59140-104-9.ch005

Suddaby, R. (2015). Can institutional theory be critical? *Journal of Management Inquiry, 24*(1), 93-95. doi:10.1177/1056492614545304

Sutanto, J., Palme, E., Chuan-Hoo, T., & Chee Wei, P. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37,* 1141-A5. Retrieved from http://www.misq.org

Thomas, S. J. (2015). *Exploring strategies for retaining information technology professionals:* A case study (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3681815)

Trier-Bieniek, A. (2012). Framing the telephone interview as a participant-centered tool for qualitative research: A methodological discussion. *Qualitative Research, 12,* 630-644. doi:10.1177/1468794112439005

Troklus, D., & Warner, G. (2011). *Compliance 101.* (3rd ed.). Minneapolis, MN: Health Care Compliance Association.

Turner, P., Kane, R., & Jackson, C. (2015). Combining methods to research an emergency department: A case study. *British Journal of Healthcare Management, 21*(2), 81-85. doi:10.12968/bjhc.2015.21.2.81

Urquhart, C., & Fernández, W. (2013). Using grounded theory method in information systems: The researcher as blank slate and other myths. *Journal of Information Technology, 28,* 224–236. doi:10.1057/jit.2012.34

U.S. Department of Health and Human Services. (1979). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Valli, C., Martinus, I., & Johnstone, M. (2014, January). Small to medium enterprise cyber security awareness: An initial survey of Western Australian business. In

Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21–54. Retrieved from http://www.misq.org/

Vest, J. R. (2010). More than just a question of technology: Factors related to hospitals' adoption and implementation of health information exchange. International *Journal of Medical Informatics*, 79, 797-806. doi:10.1016/j.ijmedinf.2010.09.003

Vousinas, G. L. (2015). The critical role of internal audit in addressing bank fraud: A conceptual framework and critical review of the literature with future extensions. doi:10.2139/ssrn.2632911

Walker, J. L. (2012). Research column: The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing*, *22*(2), 37-41. Retrieved from http://www.cccn.ca/

Watkins Allen, M., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172-200. doi:10.1177/0893318907306033

Wells, J. T. (2017). Corporate fraud handbook: Prevention and detection. John Wiley & Sons, Hoboken, NJ, USA. doi:10.1002/9781119351962.ch1.

Wigfield, A., Tonks, S., & Klauda, S. L. (2009). Expectancy-value theory. *Handbook of Motivation at School*, 55-75.

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, *11*(Fall), 1h. Retrieved from http://perspectives.ahima.org/

Wilkinson, R. T. (2012). *Perceptions of supervisory relationship influences on cognitive complexity development during practicum supervision: A qualitative study* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3520492)

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, *37*(1). Retrieved from http://dl.acm.org

Willison, R., Warkentin, M., & Johnston, A. C. (2016). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*. doi:10.1111/isj.12129

Yin, R. K. (2014). *Case study research: Designs and methods* (5th ed.). Thousand Oaks, CA: Sage.

Yoshikawa, H., Weisner, T. S., Kalil, A., & Way, N. (2013). Mixing qualitative and quantitative research in developmental science: Uses and methodological choices. *Qualitative Psychology*, *1*(S), 3–18. doi:10.1037/2326-3598.1.S.3

Zakaria, N., Stanton, J., & Stam, K. (2003). Exploring security and privacy issues in hospital information system: An information boundary theory perspective. In *AMIA Annual Symposium Proceedings* (Vol. 2003, p. 1059). American Medical Informatics Association. Retrieved from https://www.ncbi.nlm.nih.gov

Zilber, T. B. (2014). Beyond a single organization: Challenges and opportunities in doing field level ethnography. *Journal of Organizational Ethnography, 3*(1), 96–113. doi:10.1108/JOE-11-2012-0043

Zivkovic, J. (2012). Strengths and weaknesses of business research methodologies: Two disparate case studies. *Business Studies Journal, 4*, 91-99. Retrieved from http://www.alliedacademies.org

Appendix: Interview Questions

Participant Number: ________

Interview Questions:

1. What strategies have you implemented to prevent and reduce internal theft and loss in the organization?
2. What strategies have you used to monitor employees?
3. What barriers did you encounter in implementing the strategies?
4. How have you leveraged technology to innovate in the company?
5. How did you overcome the barriers to implementing the strategies?
6. How have you addressed the need for secure data storage throughout the organization while maintaining data integrity?
7. How has your organization trained employees in regards to data security?
8. How have you responded to information security violations?
9. What is the net result of your response?
10. What additional information would like to add to support the study?