Low Resource Availability and the Small- to Medium-sized Retail Enterprise's Ability to Implement an Information Security Strategy

Mary Ceil Holland, DBA| Columbia Southern University, Orange Beach, Alabama, USA

Jodine Marie Burchell, PhD | Columbia Southern University, Orange Beach, Alabama, USA
https://orcid.org/0000-0003-4927-5489

Contact: jodine.burchell@columbiasouthern.edu

Abstract

Improperly protecting businesses from cyber-attacks can result in unnecessary expenses, hardships, increasing threats, and vulnerabilities that foster data exposure and loss. This pragmatic qualitative inquiry study was designed to explore the influence of lower resource availability on Small-to Medium-sized Retail Enterprise' (SMEs) ability to implement information security strategies in the retail industry in the Northeastern region of the United States. This study explored the perceptions and experiences of 38 participants holding positions as CEOs, CIOs, ISSOs, Security Managers, and other information security professionals employed by an SME with 250 or fewer employees in the retail industry. Narratives provided insight into the research questions: (a) how does resource availability influence SMEs' ability to implement an information security strategy to protect networks and systems from vulnerabilities? (b) how do SMEs in the retail industry develop and implement an information security strategy to maintain business operations? Thematic analysis grouped similar statements and repetitions that identified patterns, themes, and subthemes. National Institute of Standards and Technology (NIST) Special Publication documents were also analyzed. The results suggest that the retail industry has several information security strategies consistent with limited resources. A holistic approach to developing and implementing an information security strategy with limited resources is achievable. The current research can help retailers strategically use cost-effective tools and controls to develop, implement, or enhance their information security strategy to improve business objectives and financial performance. Enhanced cybersecurity strategies within organizations may lead to more significant opportunities, competition, and performance in the retail industry.

Keywords: Information Security Strategy, Information Security Management, Security Plan, Cybersecurity, Cybersecurity Strategy, SMEs, Small Business, Sociotechnical Theory, Sociotechnical Design, Joint Optimization

Introduction/Background

In a complex, competitive, and dynamic business environment, small and medium enterprises (SMEs) may not be equally able to implement an effective information security strategy. Advancements in technology introduce new challenges to protect networks from human threats and vulnerabilities, such as the potential for being hacked and loss or alteration of customer data, employee data, and company proprietary information. SMEs with limited financial resources and experienced information technology personnel find it challenging to mitigate risks posed by cyberattacks (Chen, 2016). Without such talent and skills to stay abreast of threats that could stifle profits, the ultimate cost of an unprotected network or infrastructure because of a data breach or even a hack is the potential for going out of business (Bhattacharya, 2011; Chen, 2016; Clapper & Richmond, 2016; Keller et al., 2005). Numerous companies make a wide variety of cybersecurity products available to small businesses. Still, the lack of scaled-down or customizable tools, limited budgets, and technical knowledge outweigh spending on tools in which knowledge is limited (Watad et al., 2018). Some small businesses may understand the need for cybersecurity, but many fail to take adequate measures to protect against a cyberattack (Raghaven et al., 2017).

Additionally, long-term income loss, damage to the company brand, and customer trust could lead to changing competitors (Raghaven et al., 2017). Because of limited resources, some SMEs may use fewer preventive measures than larger organizations, such as backing up data regularly, developing a password policy, encrypting privacy and proprietary data, and adopting employee cybersecurity training (Keller et al., 2005; Raghaven et al., 2017). Protecting and defending assets against malicious threats from compromising confidentiality, integrity, and availability could determine future operations' longevity (Hall et al., 2011; Sleznick & LaMacchia, 2018). The immersion and interaction of technology, human, and organizational attributes contribute to preserving and securing information assets and resources (Zaini et al., 2018). The risks and vulnerabilities tie into the sociotechnical systems, whereas human and technology factors are vital elements. Sociotechnical Systems theory (STS) demonstrates that technology alone is not enough to thwart vulnerabilities (Hall et al., 2011). However, when coupled with the human element, SMEs may stand a better chance of survival.

Summary of the Literature

Information technology is ever evolving and existing, or new threats can target any industry or company. Large and small organizations from financial, retail, political parties, and credit card companies have been victims of information and cybersecurity attacks (Miller & Engemann, 2015). Resources such as people, technology, processes, and limited budgets prevent SMEs from building a robust information security framework. Lacking financial funds affect performance technology upgrades, asset acquisition, new market development, capacity expansion, and diversification (Kumar & Rao, 2015). Insufficient information technology knowledge and resources to hire employees may place small businesses at risk of compromising information technology systems and business data (Berry & Berry, 2018). Implementing information security tools is not consistent across all small businesses. Some of the most significant challenges include limited resources for the cost of information security, lacking knowledge and awareness of information security issues, and information security tools

designed for SME budgets. The following are some relevant topics related to this study found in the literature.

Sociotechnical Systems Theory (STS)

STS provided the theoretical framework and lens for this study. Within STS, the social and technical aspects work together to resolve problems and bring about change. STS was relied upon heavily during the 1950s (Trist, 1981). More specifically, newer work designs, organizational restructuring, and employee roles were more defined in several industries: mining, automobile, textiles, chemical plants, power stations, medical, and large national retail chain stores (Trist, 1981). Further, STS has been used in various engineering, manufacturing, and technology disciplines, including problems stemming from technology's socio or human and technical elements. STS portrays how technical and social elements fit together in the workplace smoothly as possible, as in joint optimization where people and technology coexist rather than place people into the technical element (Trist, 1981). Coles-Kemp and Hansen (2017) contended that real-world everyday cybersecurity problems were an emergent result of human activity and separating social and technical elements would not be astute. In the current research, STS is used as a lens to explore how information security strategy in SMEs in the retail industry in the Northeast protects information systems from threats and vulnerabilities that may appear because of limited resources. Coupling the socio, human, and technical elements of technology narrows the gap to help SMEs make better-informed decisions to develop and implement an appropriate strategy.

Leaders and Information Security

According to Uffen et al. (2012), executives' behavior and decision-making could lead to potential information security risks and directly impact information systems and management's cybersecurity level. Senior executives and lower-level managers share the responsibility to protect company assets by managing the information security program (Soomro et al., 2016). Transactional and transformation leadership styles impact employees' adherence to cybersecurity policy (Humaidi & Balakrishnan, 2015; Singh, 2015). Soomro et al. (2016) examined management's support in information security and suggested examining cybersecurity holistically. A cross-departmental leadership approach that includes human resources management, information security policy development and execution, information security awareness, and training is vital to maximizing resources and efforts to decrease cybersecurity issues (Soomro et al., 2016).

SME Information Security

SMEs comprise a large part of the U. S. and world economy. Due to the inherent susceptibility to information security attacks, some SMEs consider cybersecurity as an issue only for large enterprises and fail to employ sound cybersecurity practices. Those organizations that have measures do not quite understand the exact information security practices they use (Hayes & Bodhani, 2013). Some SMEs partner with large enterprises, and the large enterprise fail to provide cybersecurity assistance. SMEs with limited IT resources and little investments in cybersecurity have become soft targets for cybercriminals (Sleznick & LaMacchia, 2018). Cybercriminals can infiltrate large enterprises that often use SMEs because of that weakness (Hayes & Bodhani, 2013). Assessing the infrastructure and focusing

on components such as information security policies, procedures, internal employee, network, and external cybersecurity threats would propel organizations in the right direction toward protecting assets.

Organizational Security Infrastructure

Organizations experienced an imbalance in information security infrastructures. Organizations with reliable information security infrastructure and countermeasures to combat risks and vulnerabilities to information systems, assets, and business data prevail over organizations without a plan (Hettiarachchi & Wickramasinghe, 2016). Hettiarachchi and Wickramasinghe (2016) found that organizations encountered various vulnerabilities and threats to increase organizations information security levels. Due to industry diversity, organizations experienced varying risks. For example, national defense and healthcare posed a higher risk than education (Hettiarachchi & Wickramasinghe, 2016). Information security infrastructures should consist of viable cybersecurity policies that address vulnerabilities, threat control, and countermeasures to mitigate possible risks and safeguard future vulnerabilities (Hettiarachchi & Wickramasinghe, 2016).

Information Security Strategy

Information security strategy is an essential element in information security. Previous research show SMEs experience significant challenges regarding information security standards (Alshboul & Streff, 2015; Chen, 2016; González et al., 2013). Using the STS approach, Werlinger et al. (2009) developed a comprehensive list of social, organizational, and technological challenges to understand factors that affect adopting cybersecurity practices. Alshboul and Streff (2015) examined the National Institute of Standards and Technology (NIST) 7621 Special Publication for an information security model to create a new framework to assess and manage risks. Beebe and Rao (2009) used formal, informal, and technical controls to examine the intricacies of information security, security systems, and deterrent strategies. Seeholzer (2012) explored previous researchers' eight information security roles (competitor, power relationship, reorganization, public image, umbrella, objectives and priorities, and continual change) to determine the effect on information security strategy, information systems strategy, and business strategy. Seeholzer (2012) concluded that role selection was critical to information security strategy implementation. Ahmad et al. (2014) research found that prevention and technical controls were organizations' primary strategies to address cybersecurity issues. Also, utilizing multiple strategies to ensure adequate information security measures and maintaining policies could address potential cybersecurity issues (Ahmad et al., 2014). González et al. explored information security policy and linked business and technological strategies to ascertain what affected information security policy implementation and its role in business value.

Information Security Policies

Failing to protect the organization's infrastructure results in business and intellectual property losses that could add unwanted costs to the industry. IT security managers must identify the risk and have a mitigation strategy to thwart such losses. For example, Hallova et al. (2019) examined the causes of information security-related incidents' impact on business practices and creating and improving policies to protect sensitive data. The results revealed that the security of information systems depended upon

compliance with security policy and business safety standards, and the human factor affects the security of information and communication technology at all levels.

Information Security Culture

SMEs have various perceptions, beliefs, and attitudes toward information security. Engaging employees to value a cybersecurity culture that protects data, knowledge, and information is essential. For example, Paulson and Coulson (2011) studied business information systems' impact on information security and organizational security culture. To improve processes and decision-making, organizations needed to understand the psychology surrounding information security and the business information tools' capability to implement a culture where employees embraced information security (Paulson & Coulson, 2011). Organizational information security culture is multi-faceted and includes employees, processes, and systems. Greig et al. (2015) assessed information security culture, knowledge levels, and information security policy awareness and behavior in a retail store. They found that employees engaged in inappropriate information security practices and behaviors. Despite poor security practices, Greig et al. found that the organization employed a coping environment where employees fulfilled business objectives without complying with information security policy, which increased the potential for cybersecurity threats. Greig et al. ascertained that designing systems and processes to support employees, cybersecurity education, awareness, and routinely assessing the security infrastructure is vital to an appropriate information security culture.

Information Security Risk Management

Information security risk management explores and utilizes psychosocial models and behavior science to create a defense mechanism to improve risks and design a plan for managing acceptable risk levels that could allow managers to operate effectively to compete with competitors. Because of the dynamic changes in cyber threats, Putte and Verhelst (2013) noted that management and information technology professionals experienced challenges in establishing exacting countermeasures to mitigate risks. Putte and Verhelst (2013) held that a successful risk analysis required business continuity managers to look both up and downstream to locate and isolate root causes of cybersecurity threats and vulnerabilities to determine the impact during and after an incident. This general risk approach limited losses to information technology systems, critical business data, and processes that ultimately decrease financial losses (Putte & Verhelst, 2013).

Administrative internal control and accountability can be helpful in information security governance. For example, Mishra and Dhillon (2006) surmised that more significant cybersecurity threats existed in information technology systems when employees' goals were misaligned. Mishra and Dhillon subscribed to an integrated approach to cybersecurity and proposed that information system governance encompassed informal, formal, and technical levels. To maximize effective security measures, managers established and governed certain functions or activities within each level. These levels maintained a controlled environment that minimized risks that pertained to information systems and organizational processes. Organizations that effectively managed the informal structure and considered behaviors, individual values, and norms created a better cybersecurity environment and internal controls protecting business processes. Berry and Berry (2018) surveyed small businesses' approaches to risk management

and cybersecurity threats and found that SMEs severely lacked information security techniques and countermeasures to protect information security assets. The top three risks included access to the business by others, the internet, and cybersecurity, all related to information technology. These risks can potentially lead to becoming a victim of future cybercrime (Berry & Berry, 2018).

Methods

Based on support from the background and literature review, the researcher explored how scarce resources influence SMEs' ability to implement an information security strategy to protect business data and other assets from risks, threats, and vulnerabilities. A qualitative, pragmatic inquiry design was used to help with collecting, synthesizing, and interpreting data to explore this phenomenon in the retail industry in the Northeastern region of the United States. The pragmatic qualitative inquiry design was selected to help discover commonalities within participants' experiences and explore underlying factors that influenced information security strategy implementation despite limited resources. A thematic data analysis aided in the identification of codes, patterns, and themes.

Research Questions

> RQ1: How does resource availability influence SMEs' ability to implement an information security strategy to protect networks and systems from vulnerabilities?
>
> RQ2: How do SMEs in the retail industry develop and implement an information security strategy to maintain business operations?

Data Collection

Questionnaire Data. Data were collected using a questionnaire and SurveyMonkey, an online survey tool, to help locate IT SME leaders that possessed some level of experience in information security and were working in the SME retail industry. Participants were identified by the position held and the duties and responsibilities performed in the retail sales industry. A plethora of predefined responses from the literature was used, and an option for 'Other' was also provided so that participants could add their thoughts. The questionnaire was launched in the Northeastern region of the United States. Because the questionnaire was administered via Survey Monkey, eligible participants selected a location, date, and time conducive to their schedule and completed the questionnaire in 10 minutes or less. After the questionnaire, data were downloaded onto a Microsoft spreadsheet and scrubbed for incomplete responses. The result was 38 usable responses.

Document Review. NIST Special Publications (SP) were used to aid in data triangulation. Any organization can use SPs, regardless of the industry, resources, or size. NIST provides guidelines for organizations' various information security needs based on information from evolving threats. Thus, several SPs were reviewed and used that complimented the subtopics generated from data analysis. For example, NIST SP 7621 Revision 1 discussed information security fundamentals for small businesses. SP 800-100 serves as an information security guide for managers. Other topics include cybersecurity training, templates for strategies and plans, risk management, protecting wireless networks, information

systems, organizational monitoring, bringing your own devices (BYOD), and many other tools and technologies that can help meet or exceed business objectives.

Data Analysis

The authors extracted and downloaded responses from SurveyMonkey into a Microsoft Excel spreadsheet and assigned participant pseudonyms that represented individual responses. Next, repetitive reviews were included, and a Microsoft Word document was created that contained the responses to assist in developing or using predefined themes and subthemes from the responses. A comprehensive literature review, participants' responses, and the theoretical foundation revealed the SME retail industry strategies with limited resources to protect networks from risks and vulnerabilities. A thematic analysis addressed the research questions: How does resource availability influence SMEs' ability to implement a cybersecurity strategy to protect networks and systems from vulnerabilities? How do SMEs in the retail sales industry develop and implement an information security strategy to maintain business operations?
The authors grouped similar statements and repetitions that identified patterns and main themes. Several subthemes such as cybersecurity controls and training, knowledge and skills, information security involvement, and contingency planning coincided with participants' responses and manifested throughout the thematic analysis process.

Six major themes were prevalent for the two research questions and will be discussed in more detail below:

Theme 1: Low resource availability negatively affects implementing an information security strategy.
Theme 2: Low resources lead to many challenges in developing and implementing an information security strategy.
Theme 3: Challenges must be handled despite lower resource availability.
Theme 4: Network and systems protection relies on readily available tools and internal resources.
Theme 5: Assessing the effectiveness of the strategy relies on a continuous effort.
Theme 6: Keeping a wish list of goals for information security strategies is prudent.

Results

The target population consisted of varying levels of information technology personnel and SME owners employed in the retail industry in the Northeastern region of the United States. Participants were members of SurveyMonkey, an online data service platform that provides customized survey development and service to paid subscribers. A sample of 330 responded to the questionnaire. After reviewing to ensure the questionnaire was fully completed, 38 responses were usable. Table 1 depicts a concise description of the participants.

Table 1

Sample Description (N=38)

Demographic	Category	Response	Percentage
Gender	Male	18	47.37
	Female	20	56.63
Age	18-29	9	23.68
	30-39	13	34.21
	40-49	10	26.32
	50-59	4	10.53
	60-69	1	2.63
	70+	1	2.63
Position	CEO	7	18.42
	CIO	2	5.26
	ISSO	1	2.63
	Security Manager	9	23.68
	IT professional	10	26.32
	Security Professional	7	18.42

The themes generated from the data addressed the research questions. For Research Question 1, how does resource availability influence SMEs' ability to implement an information security strategy to protect networks and systems from vulnerabilities? There are three themes found (Table 2).

Table 2

Main Themes for Research Question 1

Theme	Number of Participants (n=38)	Number of Documents
Low resource availability negatively influences implementing an IS strategy	31 (81.58%)	2
Low resources lead to many challenges in developing and implementing an IS strategy	35 (92.11%)	6
Challenges must be handled despite lower resource availability	36 (94.74%)	0

Theme 1: Low resource availability negatively affects implementing an information security strategy

A thematic analysis of the collected data revealed that limited resources impacted information security strategy implementation. The cost of safeguarding information and systems is unavoidable. Nieles et al. (2017) alluded that cost and resources are necessary to implement information security plans, policies, or strategies, with the highest costs being resources and personnel. Some participants responded that cybersecurity controls and training suffered. In contrast, others indicated that too little investment was spent on cybersecurity controls and not being able to afford security training. Information security controls protect the organizations' infrastructure and minimize risks and vulnerabilities to physical property, information, computer systems, or other assets. Many participants experienced some form of resource limitations to provide the necessary protection and the cost associated with employee cybersecurity training.

The appropriate technology is not acquired. Many participants' organizations allowed BYOD. BYOD has benefits/challenges such as working from anywhere and cost-savings for employers but also poses significant information security risks such as data theft, loss of devices, and malware. Despite the risks and vulnerabilities, several participants' organizations depended upon public WiFi for business operations. Maimon et al. (2017) ascertained that public WiFi introduced risks such as unencrypted, non-authentication, and malware distribution capability, jeopardizing users' security, and privacy. Some participants noted that implementing an information security strategy required too many resources. Protecting IT is both a business requirement and a business expense. Miniscule resources created challenges for two participants' organizations to identify and secure intrusion detection systems (IDS) or other visibility tools to protect hardware and software from harmful activity. Realistically, operating an IDS requires highly skilled professionals, and SMEs with limited budgets may not be able to hire an expensive specialist and possibly abandon the effort to employ IDS altogether.

The ability to gain expertise/knowledge is limited. Limited resources impact the ability to gain expert knowledge to develop an information security strategy that prohibits expending funds on formal external training such as conferences, certifications, or other security-related courses. Scarce resources, including a lack of experienced personnel, increase risks and add to the ongoing cybersecurity problem. Surprisingly, one-half of participants revealed that limited resources hampered opportunities to improve the experience and stifled their ability to gain the necessary skills required to develop and implement an information security strategy. Moreover, several participants indicated that limited resources impacted their ability to retain high-skilled employees. Evolving technology and retaining information technology personnel are crucial to business success. Some small businesses find it challenging to retain highly-skilled IT employees because of the demand for increased salaries or other compensation. Therefore, when departing the organization, those employees with system knowledge or specialized work skills are difficult to replace. Because of the lack of financial resources to hire or retain knowledgeable employees, SMEs open the doors to unwanted cybersecurity activity that could compromise networks, systems, and data breaches. Almost one-third of the participants asserted a lack of information to help SMEs develop and implement an information security strategy. Previous research indicated that cost is a significant factor when organizations use the money on security controls and tools where knowledge is

limited and the capability to obtain resources to increase opportunities to get additional training is constrained (Chen, 2016; Keller et al., 2005; Raghaven et al., 2017; & Watad et al., 2018).

Theme 2: Low resources lead to many challenges in developing and implementing an information security strategy

Participants' most significant challenges stemmed from leadership's low proficiency and knowledge, ranging from basic information security concepts, strategy development and implementation, leaders who don't understand the risk, and difficulty prioritizing assets. The results of data analysis revealed that these challenges were attributed to a lack of management know-how, the capacity of information security involvement for profitability, business operations disruptions, and the ability to protect data and assets. Based on resources, information security may not be a top priority. Without understanding risk, leaders are challenged to invest in the right technology, people, and processes to grow the business.

Management lacks skills/nonexistent of an information security toolbox for management. With the non-existence of a toolbox for management to use as a guide to develop and implement an information security strategy, many participants disclosed that their greatest challenges stemmed from leadership's lack of knowledge. Some participants indicated that leaders did not understand the risks of not having a strategy. From a holistic business approach including financial, technology, assets, and physical security, senior leaders and management are responsible for determining acceptable levels of risks to ensure systems and processes protect information and assets that prevent CIA breaches (Nieles et al., 2017; Putte & Verhelst, 2013; Uffen et al., 2012). As the senior-most leader in organizations CIOs require skills to identify, understand and address risk factors associated with technology, operations, and information at the organizational level. CIOs should keep senior executives apprised of the successes and challenges of the overall information security architecture. Without understanding risk, leaders are challenged to invest in the right technology, people, and processes to grow the business, impacting external stakeholders. Additionally, how leaders conduct business and the overall organizational culture impact their approach to information security.

Several participants indicated that leaders had difficulty prioritizing assets. Identifying and prioritizing assets is one of the first steps in creating an inventory of the organization's assets (Cawthra et al., 2020). Simple basic measures can protect assets and business data and information such as files and databases, and customer information from adverse events. Many participants divulged leaders lacking the knowledge to develop an information security strategy/plan was a challenge in their organization. Insufficient knowledge is synonymous and ties in with the low resources thwarting opportunities to obtain the necessary skills to help implement an information security strategy, as indicated by participants. Numerous participants divulged leaders experienced adversities with understanding the concept of information security. Without the necessary skillset, it is difficult for leaders to provide direction and govern the information security architecture to thwart unwanted cybersecurity incidents. Realizing the responsibilities of management is indicative that senior leaders lacked skills, experienced challenges, and need the direction and guidance that an information security toolkit can provide.

Uncertain level of involvement in information security for business profitability. Of the participants, 5 of 7 CEOs were unsure of their participation in information security to make a profit. Businesses expect to make a profit or close the gap on competitors using readily available information

maintained on hand. For example, loyal customers may purchase goods or services, and valuable customers, attract new customers. Supplier, manufacturer, or even distributor lists are helpful information for business performance. Therefore, information should be afforded some measure of protection to prevent the risk of being compromised. Some participants reported their organizations had trouble understanding minimal information security guidelines for small businesses. A few others experienced an ongoing battle with identifying risks and vulnerabilities. Young et al. (2011) argued that complete risk control was impossible because of the nature of the risks. However, risks were reduced as investments in information security increased. A couple of participants had problems estimating the cost of information security. Young et al. implied information security protection incurred both direct and indirect costs. Compromising information can be extremely costly but investing in cybersecurity is less expensive even if using some of the most basic and available security protections (Gordon et al., 2018; Young et al., 2011). Keeping pace with evolving technology, including hardware and software, requires skilled employees to manage networks and systems to thwart potential vulnerabilities. Some participants posited that their organizations had difficulty keeping pace with evolving technology, whereas others experienced problems assigning responsibility to update security software and hardware. Overall, numerous participants were indeterminate of their involvement with information security for profitability.

The inability to provide for future emergencies/contingency planning. Information systems should operate with minimal interruption. In emergencies or other disruptions to servers or networks, recovering as quickly as possible is the ideal goal. Swanson et al. (2010) asserted that business continuity planning (BCP) is essential to information security. Organizations should have a backup plan to keep the business ongoing during turbulent times to maintain critical business processes and customer service. Some participants surmised that low resources were a problem that impacted their ability to provide for future emergencies. Surprisingly, almost one-third of participants, including CEOs, lacked a contingency or BCP, making it extremely difficult to continue operations should a disaster occur. One of the most straightforward strategies for disaster recovery is creating an information systems backup policy and ensuring that designated employees regularly back up all information systems as specified in the policy (Swanson et al., 2010).

Inability to adequately protect business data and assets. A couple of participants' organizations found it difficult to secure resources to assist with cybersecurity. Similarly, another group had problems limiting employees' access to data and information. Yet, others experienced challenges in securing wireless access points and networks. Financial, human, and technology resources are required to operate a business, regardless of the industry. SME owners and IT personnel should understand that internal and external systems, processes, and security risks can negatively and positively impact business operations (Zaini et al., 2018). Limited resources, lacking knowledge, and little security investment opens the door for potential cybercriminals and other attacks. The most basic information security strategy can positively impact financial performance.

Theme 3: Challenges must be handled despite lower resource availability

Nearly all participants mentioned that information security challenges in the organizations should be addressed appropriately despite limited sources. When inquired about how their organizations handle

challenges, data analysis implies that organizations used various activities as a type of information security strategy. The majority indicated that establishing clearly defined security roles and responsibilities of IT personnel eliminated conflicts of interest or no one employee had access to all internal control keys. Defining roles and responsibilities for specific tasks held organizations and employees accountable and increased efficiency. As a result of scarce resources, employees in small organizations may fill several roles. Nieles et al. noted that small companies had the same leverage as large companies in roles and responsibility separation and securing information because separating roles did not rest merely on company size. Many participants continuously observed security and reviewed policy compliance and suggested reviewing and updating policies annually and informing employees when changes occurred in the organization and technology. Previous researchers also addressed security policy and plans challenges (Beebe & Rao, 2010; Colwill, 2010; Gordon et al., 2016, 2018; Hallova et al., 2019; Soomro et al., 2016). To handle key challenges, some participants reviewed their security posture. Examining the overall status of information assurance resources and capabilities ensures alignment that affords the best defense and provides opportunities to make changes when necessary. Several participants indicated that valuing and promoting information security as a core business practice was a challenge that required addressing despite limited resources. Connecting and aligning information security protocols to business objectives to include the human element is vital to organizational performance. Security processes, procedures, and technology are investments and should integrate into overall business objectives. These processes create a dynamic security program, and repositioning the organization, including people, processes, and technology, toward risk management helps to reduce internal and external threats.

For Research Question 2, how do SMEs in the retail sales industry develop and implement an information security strategy to maintain business operations? There are three themes found (Table 3).

Table 3

Themes for Research Question 2

Theme	Number of Participants (n=38)	Number of Documents
Network and systems protection relies on readily available tools and internal resources	35 (92.11%)	9
Assessing the effectiveness of the strategy relies on a continuous effort	35 (92.11%)	6
Keeping a wish list of goals for security strategies are prudent	37 (97.37%)	3

Theme 1: Network and systems protection relies on readily available tools and internal resources

Because of the interconnectedness and the ability to share information using the internet, protecting sensitive and valuable data such as customer information, financial data, or even login information to systems and protected files can be challenging. As such, networks and systems require protection against threats and losses. The transport layer security (TLS) protects data during electronic dissemination across the internet and provides CIA protection of data between two communicating applications (McKay & Cooper, 2019). This research did not address the TLS but instead focused on participants' strategies to protect their networks and systems from cyber vulnerabilities.

Planning, engagement, and governance control. Information security governance influences policy development oversight and continuous monitoring activities (Bowen et al., 2006). When inquired about their organizations' strategies to protect networks and systems from cyber vulnerabilities, organizations used varying strategies, while several used more than one strategy. Nearly one-half of participants' organizations subscribed to a holistic approach by balancing human and technical controls. Technical and non-technical multidimensional factors require a holistic approach to information security protection (Sadok & Welch, 2019; Soomro et al., 2016; Uffen et al., 2012). Many participants enforced their organization's security policy. Both socio and technical aspects of STS are crucial in an information security policy, and information security policy awareness reduces incidents and threats (González et al., 2013; Greig et al., 2015; Humaidi & Balarkrishnan, 2015). The information security equation often overlooks the human element. For example, very few participants indicated that their organizations offered cybersecurity education training regularly. According to Bowen et al. (2006) and Soomro et al., information security awareness and training can help improve the security posture, intensify vigilance, and decrease security issues. Thus, leaders should integrate security education training and awareness into business objectives.

Viable internal human resources. IT personnel enables the workforce to communicate, obtain data, process information, and manage information systems and other assets such as intellectual property, customers, and sensitive data that the organization depends on for business operations. Technical knowledge, skills, and experiences are needed to protect information and assets. Numerous participants indicated their organizations used viable internal human resources by striving for knowledgeable IT staff with technical expertise as a part of their strategy to protect networks and systems from cyber threats and vulnerabilities. Because of the complexities of evolving technology, cybersecurity work has changed, and organizations find it challenging to resolve issues designing and building complex systems. Therefore, some organizations use varying self-created methods to attempt to solve problems. Participants in this study indicated the positions held in their organizations; however, the researcher did not examine participants' knowledge, skills, or experience. Organizations can build a dynamic cybersecurity workforce by describing work in the form of tasks and what is required to perform that work through knowledge and skills. Surprisingly, only two participants indicated that only privileged users manage systems and networks as an information security strategy. Privilege users have trusted IT account holders who perform systems management, maintenance, access, and control tasks that ordinary users or other IT employees are not authorized to act (Pillitteri et al., 2020; Waltermire et al., 2018). Regardless, organizations should maintain a privileged management policy and monitor, audit, control, and manage privileged account usage.

Identification and deployment of tools and technologies to authenticate controls and track access. Using technology and tools to identify and track users to authenticate unauthorized access to data, resources, and assets decreases risks and vulnerabilities. Participants utilized various strategies to maintain the security and integrity of data, information systems, and networks. Some participants used continuous monitoring and auditing as a part of the risk management process encompassing the security architecture and programs to help leaders make risk tolerance cybersecurity decisions regarding threats and vulnerabilities. A few participants used multi-factor authentication to alleviate the risks of unauthorized access to information. Other participants depended upon automatic updates to software and patches. Ensuring software and patches are updated swiftly increases security measures against threats and vulnerabilities (Souppaya & Scarfone, 2013). Internal tools and resources such as monitoring, security training, and privileged user access to manage systems and networks to decrease the potential threats and increase business objectives are significant components of developing and implementing an information security strategy.

Theme 2: Assessing the effectiveness of the strategy relies on a continuous effort

Assessing the effectiveness of information security strategy can provide insight into how the organization values information security and help management make better-informed decisions to compete. The inquiry into how participants assess the effectiveness of information security strategy in their organizations centered around a continuous and concerted effort to review and evaluate processes, procedures, security posture status, security threat landscape, and customer value. Several participants indicated that their organization uses abundant processes or procedures to assess the effectiveness of their information security strategy.

Employee compliance and process evaluation. Some participants' organizations examined and audited data logs. In the retail industry where charge cards are offered, the Payment Card Industry Data Security Standard (PCI DSS) mandates those organizations that "store, process or transmit cardholder data" for credit cards to "track all access to network resources and cardholder data" (Kent & Souppaya, 2006, p. 2-8). Many indicated their ability to review and change security policies as needed. For example, organizations should review at least annually and update as soon changes to processes or procedures and technology occur (Paulsen & Toth, 2016). Some organizations offer continuous cybersecurity training which is vital to protecting business information and resources. Several monitored and evaluated employees, processes, and technology for compliance. Ensuring policies and procedures are current and align with employees and technology to fulfill business objectives is the embodiment of an information security strategy.

Strength of the security posture. Cyber threats to systems and information could be internal or external, whether accidental or willful. The strength of an organization's security posture comprises information, networks, systems, and resources such as people, hardware, software, policies, and capabilities to protect and respond as conditions change. Several participants assessed their security strategy based on the ability to identify, remediate, and manage risk. Conducting a risk assessment helps determine vulnerabilities and reveal uncommon risks that jeopardize business performance and resilience. A few participants reviewed the CIA triad to protect their data. Reviewing information to provide the CIA is vital to safeguarding information, tangible and intangible assets, and the

organization's reputation. Ransomware, malicious codes, insider threats, and data breaches can halt profitability when the appropriate cybersecurity protections are not in place (Nieles et al., 2017). Various participants assessed their strategy on the organization's ability to maintain data privacy and protect consumer information. Customer and other private information should be protected through measures, including operational safeguards, privacy-specific safeguards, and security controls. Not preserving data integrity leads to attacks such as deletion, modification, or unauthorized insertion of corporate information such as emails, employee financial records, and customer data (Cawthra et al., 2020; McCallister et al., 2010).

Security threat landscape. A few participants assessed the effectiveness by the number of incidents received and resolved. Organizations might measure the number of incidents handled to the amount of work that the incident response team performed rather than the quality of the team unless consideration was given to the quality of the team's work. A significant number of participants assessed their effectiveness capacity to keep abreast of evolving cyber threats and vulnerabilities. Interestingly, intrusion and malware detection methods have been ineffective in defending against advanced persistent threat (APT) tactics (Zou et al., 2020). The disguise and sophistication of APT make it difficult for organizations to notice. Of those instances noticed, the APT appears to be random and uncorrelated. However, the attack action in APT does leave traces behind that can only be audited or recorded by security sensors such as systems audit logs or firewall logs (Zou et al., 2020). In essence, participants realize threats and vulnerabilities and the appropriate countermeasures to minimize or lessen the degree of impact on the security infrastructure.

Focusing on customer service. One-half of the participants assessed the effectiveness of their information security strategy on the organization's ability to meet or exceed aggressive delivery timelines and customer demands. Meeting deadlines to satisfy consumer demands is a significant factor in the retail industry that may come with a price. Only two participants focused on customer needs to help maintain consumer retention and prevent stakeholder loss, which may be contrary to some scholars' beliefs. For example, according to Fleming (2021), many small businesses use technology and facility enhancements as creative ways to rethink customer service to meet business objectives while envisioning new business opportunities and increasing customers even amid the COVID-19 pandemic. Because of evolving technology and threats and vulnerabilities, information security strategies must be reviewed regardless of organizations' scope and methods. Assessing processes and procedures can identify areas for improvement.

Theme 3: Keeping a wish list of goals for security strategies is prudent

Poorly configured work systems and employees' security behaviors can provide an open door for employees and external hackers to break into networks. Protecting the information, people, and organizational reputation is paramount to business operations. An information security mindset can increase data protection and thwart potential threats and vulnerabilities from wreaking havoc on organizations. Participants responded to the type of information security strategy they desired to implement.

Resilience and sustainable information security architecture. The ability to anticipate, prepare, detect, respond, and adapt to essential changes and unexpected disruptions is necessary to survive and succeed. Safeguarding stakeholders' interests, ensuring employees comply with policies, and maintaining technology capabilities can help avoid unwanted activity. Participants desired various information security strategies, as garnered from data analysis, and based on organizations' needs. Some participants desired to leverage information security to achieve a competitive advantage. Some wanted to balance organizational needs and business capabilities. Others wanted to integrate the IS strategy into business and regular processes. Various participants yearned to achieve business and IT alignment. Multiple participants desired amendable security policies that aligned with business functions and processes. According to Patterson (2020), developing IT makes it nearly impossible to separate business and IT strategies. Integrating IT strategy into overall business strategy adds value to an organization. Communicating and collaborating between senior leaders and IT personnel is critical in designing, implementing, managing, and improving IT solutions and controls for IT architecture to meet, align and support business objectives.

Prevention. Many participants desired to protect networks and data from viruses, spyware, and malicious codes. The damage that threat events may cause to systems varies considerably. Unwanted activity may affect the CIA of information, while another may affect the system's availability. Plenty of participants wanted a strategy that could reduce the success rate of an attack. Various participants desired more leadership involvement. The assurance that information security is enforced and leadership-driven from the top-down could indicate that leadership is needed to forge compliant behavior. Effective information security arises if infused in the entire organization and is practiced by all employees and at every level (Guhr et al., 2019). Nearly one-half of participants' organizations wanted a trained staff to prevent, detect, and respond to risks and vulnerabilities. Responding to risks and vulnerabilities such as natural disasters, fire, medical emergencies, or even burglary could positively impact information security.

Security event management and its role in monitoring. Maintaining a real-time view of information security risks across an organization requires the involvement of the entire organization. Diverse participants desired an information security strategy to control and monitor internal and external threats and vulnerabilities effectively. According to Dempsey et al. (2011), an adequate information security continuous monitoring strategy addresses monitoring requirements and activities within the organization, mission/business process, and information systems tiers. Each tier has unique responsibilities in the monitoring process that reveal anomalies.

Comprehensive and all-encompassing solid security architecture. Businesses face new and challenging risks to safeguard information and resources. Protecting data, assets, and resources should be considered in all business activities, including external legislation, internal security policy, business functions, organizational structure, and the leaders' commitment to introduce and invest in an information management system for managing information security (Šikman et al., 2019). Only a few participants wanted an information security strategy supporting the CIA triad and protecting competitive advantage, reputation, and customer trust. Senior decision makers' commitment to obtaining the necessary tools, systems, hardware, software, and human resources to support the CIA triad of information and manage risk is of great value to stakeholders and the organization. Three participants wanted a strategy focused on detection, prevention, deterrence, response, and deception. Paulsen and

Toth (2016) surmised that safeguarding organizational information required limiting access to sensitive information, encrypting sensitive business data, and training employees. Additionally, regularly monitoring to ensure timely discovery of cybersecurity events and rapidly responding to degradation in information systems, security processes, and procedures help to reduce the impact on the security architecture.

Summary

Despite limited resources, lacking knowledge was the most significant challenge reported by participants. However, information security strategy does exist in some form or fashion in the retail sales industry in the Northeastern region of the United States. Participants' SMEs should customize a security program to fit their unique needs. SMEs desire some sort of information security strategy. Because of lacking resources and not networking or sharing knowledge with competitors, scaled-down versions or ready-made policies, regulations, or publications that require minimum implementation effort to understand would be ideal.

Conversely, SMEs should make a concerted effort to review public service organizations or federal government websites and use the step-by-step ready-made templates to resolve potential internal and external cybersecurity threats and vulnerabilities. Pursuing knowledge and additional skills and understanding the swift change in information security vulnerabilities could lead to better information security strategy development and subsequent implementation. SME participants experienced challenges ranging from the inability to acquire necessary knowledge and skills, purchase software upgrades, relying on public wireless networks, and BYOD, all of which create risks to their organizations. Furthermore, despite limited resources and tools, SMEs were resourceful in tapping into readily available tools and internal resources to assess the effectiveness of their information security strategy, which resulted in an information security continuous monitoring program. In essence, taking a holistic approach to implementing an information security strategy with limited resources is achievable. Several external agencies, resources, and tools were presented throughout the current research that provided free instructional courses and templates for various policy documents to aid the SME retail industry in enhancing or expanding their information security strategy goals to remain profitable.

Summary of Findings and Conclusion

This pragmatic qualitative inquiry design aided in exploring how lower resource availability influences the SME retail industry in the Northeastern region of the United States' ability to implement an information security strategy to protect business data and other assets from risks, cybersecurity threats, and vulnerabilities. A thorough look at each of the research questions provides unique information.

Research Question 1

How does resource availability influence SMEs' ability to implement an information security strategy to protect networks and systems from vulnerabilities?

Revenue from the SME retail industry contributes to a significant part of the economy. Results imply that protecting the CIA of stakeholders and business information and assets from unauthorized disclosure, modification, use, or deletion has been an enormous challenge for the retail industry because of limited resources, knowledge, skills, and tools. There is a lack of direction and commitment to understanding information security at the senior leadership or management level. Additionally, a plethora of information security concerns exists in participants' organizations. Even with minute resources and employing a strategy commensurate with resources on hand, both the human and technology factors posed significant risks to stakeholders and consumers.

Participants' knowledge can be improved through technology and educational means, whether acquired via on-the-job training, online, or externally. Scarce resources and budgets lead to participants requiring information security guidance, solutions, and practical training, enabling organizations to enhance implemented cost-effective information security strategies to help decision-making and retain resiliency. Participants appear to meet business objectives regardless of the scarce resources, knowledge, and skillsets. The themes 1) low resource availability negatively affects implementing an IS strategy, 2) low resources lead to many challenges in developing and implementing an information security strategy, and 3) any challenges that must be handled despite lower resource availability are supported in the literature. The results point to specific capabilities, information sources, strategies, and decision styles aligned with current literature.

Research Question 2

How do SMEs in the retail industry develop and implement an information security strategy to maintain business operations?

The results reflect that many participants used multiple security strategies. Because leadership lacks the resources to hire IT experts and address the ideal strategies that participants' desired, the results of this study implied that some participants are not prepared and have little confidence in their ability to manage risk. SMEs need to find the value in risk assessment and grasp the consequences that exposing data could cause to their organizations and compromise the whole security posture. That lack of preparation also creates vulnerabilities. To remain resilient, management and senior leadership positions require understanding, anticipating, and guarding against risks. Grasping the concepts of information security is needed by both leadership and employees. IT skillsets are an absolute must to maintain systems, controls, and protect information. Addressing vulnerabilities is multi-faceted, and developing and implementing information security strategies should focus on systems, people, processes, and policies. All participants used technology, anticipated revenue growth, and desired holistic security strategies to achieve a competitive advantage. However, investing and implementing such strategies requires time and resources, which ends up in costs, and subsequently increases the profit margin for the retail sales industry. Risks, threats, and vulnerabilities threaten the existence of the retail sector. Lacking resources and varying vulnerabilities lead to outdated technology and the inability to protect data and assets. The themes 1) network and systems protection rely on available tools and internal resources, 2) assessing the strategy's effectiveness relies on a continuous effort, and 3) keeping a wish list of goals for security strategies is prudent is supported throughout the literature. Retailers are responsible for a significant amount of valuable data, and it is worth investing in more advanced protection. Having a plan or a strategy to secure data is crucial to the industry's livelihood. Overall, the findings suggest that

the SME retail industry knows that threats and vulnerabilities place their organizations at risk. SMEs can appropriate and orchestrate the means to respond to cybersecurity threats that negatively influence information security strategy implementation impacting organizational performance.

Theoretical implications

The theoretical framework for the study is the Sociotechnical Systems theory (STS, Trist, 1981). The theory suggests that activities and situations are influenced by socio (human) and technical (technology, resources, processes) elements. STS is an open system in which continuous change happens, whereas people and technology function together as a unit or a complex system to achieve the business' objectives. STS suggests that people, technology, and the environment directly influence the output of a product. A significant connection between this theory, people, the environment, and the technical factors that influence processes and procedures to implement an information security strategy is highlighted throughout the study. People, technology, and the external environment are connected and work together to generate an output (profit). STS is adaptable in decreasing evolving threats and other unpredictable developments to retain the CIA of information and assets. Given the increase in cyberattacks, retailers are vulnerable to various threats. Employees require the right tools to exceed business objectives. STS factors help manage risks and quickly adjust and adapt when conditions, changes, or disruptions occur. When the human element operates and interacts with the technical element, a new complex system proactively addresses challenges, improves customer experience, and increases competitive advantage. Integrating technical, the cybersecurity environment, and human factors as core business practices can produce a holistic information security strategy that thwarts threats and vulnerabilities that protect data and assets. A significant connection exists between the elements and SMEs'. Information security strategy implementation can either amplify or mitigate threats and vulnerabilities and provide a means to improve performance. The current study includes valuable information for the SME retail industry to determine the effectiveness of the security strategy and aid senior management and other decision-makers to ascertain low but cost-effective tools and controls that can best enhance and protect data and assets.

Implications for professional practice

The SME retail industry can use the results of this study to understand how employees perceive information security development and implementation. All participants were from the Northeastern part of the United States, had either worked in the SME retail industry over the past year, or were currently providing IT security support offered their perceptions based on personal experience. Security training is a necessary investment, but not a priority. The plethora of challenges experienced by participants can be resolved through security education and training from the senior leadership to the lowest level employees. Because of unavailable resources, some employees fill multiple roles outside the scope of their skillsets. Evolving technology and ensuing persistent threats and vulnerabilities have shown that IT support requires advanced tools, skills, and knowledge to leverage information security as a necessary asset of business operations. Leadership may venture out to federal and local business agencies for security information and advice and create an information toolkit for their organizations. Senior leadership knowledge and awareness are paramount to protecting data and maximizing profits to achieve a competitive advantage. The retail industry suffers greatly without the prerequisite security awareness

knowledge and skills to execute security controls that protect data and other critical business assets and manage risks.

A second implication is that written documentation, such as an information security policy, is necessary. Without guidance or security protocol, employees can unwittingly or inadvertently create threats and vulnerabilities to undocumented processes and procedures. For example, compromising customer and stakeholder data through point-of-sales transactions can become a problem. A written information security policy covering significant aspects of business objectives integrated with the overall information security infrastructure can create a well-trained staff that can detect, prevent, and responds to risks and vulnerabilities. Based on the results of this research for future implications, there are plenty of lessons to learn for individuals who desire to establish a non-eCommerce retail sales business. First, an awareness of the plethora of challenges forged by limited resources is critical to expected financial performance.

IT and information security should be considered core business practices during the planning phases. IT increases process speed and returns cost-saving benefits to the business. Adhering to PCI security compliance and controlling data and information during point-of-sales transactions are vital to achieving a competitive advantage in the industry sector. In essence, the findings may produce practical value for SME retail business leaders to understand the redisposition of resources in information security and allow leaders to focus on resources that improve value creation and overall performance.

Limitations

The main limitation of this study is that a pragmatic qualitative inquiry design was used to conduct the study. As such, findings are not extrapolated beyond the industry selected for the study. The study was also limited by the sample population that encompasses only the retail sector comprising SMEs with 250 employees. Participants were selected based on positions in the organization rather than specific experience levels, which were the only inclusion for this study. The researcher depended solely on the experience and knowledge of the study participants. Participants may have different levels of knowledge about resource allocation and information security strategy implementation. The questionnaire depended upon subscribers to SurveyMonkey. The data from a small sample of SME owners, IT professionals, information systems security officers, chief information security officers, chief information officers, information systems security managers, system administrators, security managers, and other business leaders do not reflect a large population of the United States but rather the Northeastern geographical area.

Recommendations for future research

The first recommendation for future research is to determine the SME retail industry's senior leadership involvement in information security. The amount of time SME retailing CEOs devote to information security to increase their knowledge and, subsequently, their effectiveness toward asset protection and risk management is critical to business existence. Meeting with CISOs and CIOs to obtain the organization's information security architecture status is a start. Still, the CEO's role as the senior-most leader is of a different caliber.

A second recommendation for future research is to determine how the SME retail industry provides security education training to the organization and assess program effectiveness. Continuous security training and relevant materials serve to remind employees across the entire organization. Cost-effective and accessible training materials are available on federal, state, and local business websites. Frequent email reminders and illustrative posters can demonstrate organizations' commitment to protecting data and assets. A vigilant workforce can help mitigate threats and vulnerabilities more effectively during early detection.

The third recommendation for future research is for the federal government to take a more proactive approach and offer additional resources and assistance, not just to retailers but also to other SME industries. Because of resource limitations, some SMEs may use or rely on older methods to protect information. However, advancing cybersecurity threats and vulnerabilities could easily infiltrate and infect networks with malicious malware. The federal government can require SMEs to validate their information security program based on a set of guidelines managed by the federal government. This initiative will also help larger businesses linked to SME businesses. In hindsight, the goal is for SMEs and the federal government to collaborate and work together to reduce cybersecurity threats and vulnerabilities and preserve SME existence because failure to do so places consumers and stakeholders at risk.

Conclusion

This pragmatic qualitative inquiry design was used to explore the influence of lower resources on the SME retail industry in the Northeastern region of the United States' ability to implement an information security strategy to protect business data and other assets from cybersecurity risks, threats, and vulnerabilities. The value of this study highlights the importance of how a holistic approach can be used when employing the socio (human) and technical (technology, procedures, processes) factors in the retail industry to develop and implement information security strategies effectively. Some invaluable free and up-to-date training resources, along with identified publications containing varying templates to construct written policy and other guidance, are emphasized in the study. Due to evolving technology, the SME retail industry needs to be informed about the latest threats, vulnerabilities, and the necessary resources and tools applied to information technology systems, procedures, and processes to implement a strategy that fits business objectives and enhances profitability. Very little research has explored how SMEs develop security strategies given limited resources. However, little research has been conducted specifically in the retail industry. Protecting stakeholders' interests and the overall financial performance is no easy feat, but in-depth solutions are required to minimize security risk.

Participants' ensuing accounts provided a broad understanding of their organizations' security strategy and a narrower focus on the distinct variations in individual experiences. Subsequently, analyzing the meaning of the phenomenon and integrating the descriptions of participant experiences garnered six dominant themes: 1) Low resource availability negatively affects implementing an IS strategy, 2) Low resources lead to many challenges in developing and implementing an information security strategy, 3) Challenges must be handled despite lower resource availability, 4) Network and systems protection rely on available tools and internal resources, 5) Assessing the strategy's effectiveness relies on a continuous

effort, and 6) Keeping a wish list of goals for security strategies is crucial. Despite limited resources, SME retailers need to know how to best utilize the resources on hand and leverage many external resources to integrate information security and business objectives in the most cost-effective manner that contributes to security strategy implementation.

Capturing the essence of the phenomena required inquiring how participants perceived their organizations' security strategy could only be analyzed within the context in which it occurred. An open-ended questionnaire forged detailed descriptions of participants' perceptions, experiences, and the most meaningful areas that contributed to understanding the phenomenon. Developed themes reinforced comprehension of the phenomena. Synthesizing the results with agency documents such as NIST SPs provided additional depth to the research narrative. Conclusion evolved based upon CIA protection of information, despite limited resources, and leveraging information security to capture competitive advantage and increase financial performance for all stakeholders.

References

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357–370. https://doi.org/10.1007/s10845-012-0683-0

Alshboul, Y., & Streff, K. (2015). Analyzing information security model for small-medium sized businesses. *Twenty-first American Conference on Information Systems*, Puerto Rico, 1-9. https://aisel.aisnet.org

Beebe, N. L., & and Rao, V. S. (2009). Examination of organizational information security strategy: A pilot study. *American Conference on Information Systems*, 1-13. Retrieved from https://aisel.aisnet.org

Beebe, N. L., & Rao, V. S. (2010). Improving organizational information security strategy via Meso-level application of situational crime prevention to the risk management process. *Communications of the Association for Information Systems*, *26*(17), 329-35. Retrieved from https://aisel.aisnet.org

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cybersecurity threats. *International Journal of Business Continuity and Risk Management*, *8*(3), 1-10. https://semanticscholar.org

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management and Computer Security*, *19*(5), 300-312. https://doi.org/10.1108/09685221111188593

Bowen, P., Hash, J., & Wilson, M. (2006). Information security handbook: A guide for Managers. *NIST*, SP 800-100, 1-178. http://10.6028/NIST.SP.800-100

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., & Sweetnam, J. (2020). Data integrity: Identifying and protecting assets against ransomware and other destructive events. *NIST*, SP 1800-25, 1-567, https://doi.org/10.6028/NIST.SP.1800-25

Chen, J. (2016). Cybersecurity: Bull's eye on small businesses. *Journal of International Business Law*, *16*(1), 97-118. https://heinonline.org

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences*, *19*(1), 54-67. https://alliedacademics.org

Coles-Kemp, L., & Hansen, R. R. (2017). Walking the line: The everyday security ties that bind. In Human Aspects of Information Security, Privacy and Trust*,* 464-480, Springer, Cham. https://doi.org/10.1007/978-3-319-58460-7_32

Colwill, C. (2010). Human factors in information security: The insider threat-who can you trust these days. *Information Security Technical Report*, *14*(4), 1-11.https://doi.org/10.1016/j.istr.2010.04.004

Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). Information security continuous monitoring for federal information systems and organizations. *NIST*, SP 800-137, 1-80. https://doi.org/10.6028/NIST.SP.800-137

Fleming, R. S. (2021). Small business resilience and customer retention in times of crisis: Lessons from the covid-19 pandemic. *Global Journal of Entrepreneurship*, 5(S1), 30. http://igbr.org

González, D. P., González, P. S., & Preciado, S. T. (2013). Strategy of information security in small and medium enterprises, and technology-enterprise approach: Analysis of its relationship with organizational and performance business variables. *International Journal on Information, 16*, 3883-3906. https://researchgate.net

Gordon, L. A., Loeb, M., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *9*, 133–153. https://doi.org/10.4236/jis.2018.92010

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*, 49–59. https://doi.org/10.4236/jis.2016.72004

Greig, A., Renaud, K., & Flowerday, S. (2015). An ethnographic study to assess the enactment of information security culture in a retail store. *World Congress on Internet Security*, 61-66. https://doi.org/10.1109/WorldCIS.2015.7359415

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, *29*(2), 340–362. https://doi-org/10.1111/isj.12202

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, *19*(3), 155-176. https://doi.org/10.1108/09685221111153546

Hallova, M., Polakovic, P., Silerova, E., & Skovakova, I. (2019). Data protection and security in SMEs under enterprise infrastructure. *AGRIS online Papers in Economics and Informatics*, *11*(1), 27-33. https://doi.org/10.7160/aol.2019.110103

Hayes, J., & Bodhani, A. (2013). Cybersecurity: Small firms under fire. *Engineering & Technology, 8*(6), 80-83. https://doi.org/10.1049/et.2013.0614

Hettiarachchi, S., & Wickramasinghe, S. (2016). Study to identify threats to information systems in organizations and possible countermeasures through policy decisions and awareness programs to ensure information security. *Information Security*, 1-13. https://researchgate.net/publication/307107552

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311-318. https://doi.org/10.7763/ijiet.2015.v5.522

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management, 22*(2), 7-19. https://doi.org/10.1201/1078/45099.22.2.20050301/87273.2

Kent, K., & Souppaya, M. (2006). Guide to computer security log management. *NIST*, SP 800-92, 1-72. https://doi.org/10.6028/NIST.SP.800-92

Kumar, S., & Rao, P. (2015). A conceptual framework for identifying financing preferences of SMEs. *Small Enterprise Research*, *22*(1), 99–112. https://doi.org/10.1080/13215906.2015.1036504

Maimon, D., Becker, M., Patil, S., & Katz, J. (2017). Self-protective behaviors over public WiFi networks. In The LASER workshop: Learning from authoritative security experiment results. *Usenix Association*, 69–76. https://www.usenix.org/

McCallister, E., Grance, T., & Scarfone, K. (2010). Guide to protecting the confidentiality of personally identifiable information (PII). *NIST*, SP 800-122, 1-59. https://doi.org/10.6028.NIST.SP.800.122

McKay, K. A., & Cooper, D. A. (2019). Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations. *NIST*, SP 800-52 Rev 2, 1-72. https://doi.org/10.6028/NIST.SP.800-52r2

Miller, H. E., & Engemann, K. J. (2015). Threats to the electric grid and the impact on organizational resilience. *International Journal of Business Continuity and Risk Management*, *6*(1), 1-6. https://doi.org/10.1504/ijbcrm.2015.070348

Mishra, S., & Dhillon, G. (2006). Information systems security governance research: A behavioral perspective. *First Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, 27-35. https://researchgate.net

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). An introduction to information security. NIST, SP 800-12 Rev. 1, 1-101. https://doi.org/10.6028/NIST.SP.800-12r1

Patterson, M. (2020). A structured approach to strategic alignment between business and information technology objectives. *SA Journal of Business Management*, *5*1(1), 1-13, https://doi.org/10.4102/sajbm.v51i1.365

Paulsen, C., & Toth, P. (2016). Small business information security: The fundamentals. *NIST*, NISTIR 7621 Rev1, 1-54. https://doi.org/10.6028/NIST.IR.7621r1

Paulson, C., & Coulson, T. (2011). Beyond awareness: Using business intelligence to create a culture of information security. *Communications of the IIMA*, *11*(3), 35-54. https://iima.org/CIIMA/CIIMA

Pillitteri, V., Olumese, E., & Porter, E. (2020). Security and privacy control for information systems and organizations. *NIST*, SP 800-53 Rev. 5, 1-492. https://doi.org/10.6028/NIST.SP.800-53r5

Putte, V. D., & Verhelst, M. (2013). Cybercrime: Can risk analysis help in the challenges facing business continuity managers? *Journal of Business Continuity and Emergency Planning*, *7*(2), 126-137. https://henrystewartpublications.com

Raghaven, K., Desai, M., & Rajkumar, P. V. (2017). Managing cybersecurity and e-commerce risks in small businesses. *Journal of Management Science and Business Intelligence*, *2*(1), 9-15. https://doi.org/10.5281/zenodo.58169

Sadok, M., & Welch, C. (2019). Achieving sustainable business systems through sociotechnical perspectives. *Proceedings Twenty-Seventh European Conference on Information System*. https://aisel.aisnet.org/ecis2019_rp

Seeholzer, R. V. (2012). Information security strategy: In search of a role. *American Conference on Information Systems Proceedings*, 24, 1-18. https://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/24

Šikman, L., Latinović, T., & Paspalj, D. (2019). ISO 27001: Information systems security, development, trends, technical and economic challenges. *International Journal of Engineering, 17*(4), 45–48. Retrieved from http://annals.fih.upt.ro/

Singh, M. K. (2015). A conceptual study on leadership theories and styles of managers with a special emphasis on transformational leadership style. *International Journal of Advanced Research*, *3*(10), 748-756. https://doi.org/10.37284/2707-7810

Sleznick, L. F., & LaMacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be?, *13*(2), 217-253. *Journal of Business & Technology Law*. https://digitalcommons.law.umaryland.edu/jbtl/

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Souppaya, M., & Scarfone, K. (2013). Guide to enterprise patch management technologies. *NIST*, SP 800-40 Rev. 3, 1-26. http://doi.org/10.6028/NIST.SP.800-40r3

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems. *NIST*, SP 800-34 Rev. 1, 1-149. https://doi.org/10.6028/NIST.SP.800-34r1

Trist, E. (1981). Evolution of sociotechnical systems. *In Perspectives on Organizational* Design. Wiley, New York, 19-75.

Uffen, J., Guhr, N., & Breitner, M. H. (2012). Personality traits and information security management: An empirical study of information security executives. *Thirty Third International Conference on Information Systems*, *13*, 1-22. https://aisel.aisnet.org/icis2012/

Waltermire, K., Conroy, T., Harriston, M., Irrechukwu, C., Krishnan, N., Memole-Doodson, J., Nkruman, B., Perper, H., Prince, S., & Wynne, D. (2018). Privileged account management for the financial services sector. *NIST*, SP 1800-18, 1-213. https://doi.org/10.6028/NIST.SP.1800.18

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions. *International Journal of the Academic Business World*, *12*(1), 23-30. https://jwpress.com

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19. https://doi.org/10.1108/09685220910944722

Young, L., Kauffman, R., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems*. 51(4), 904-920. http://10.1016/j.dss.2011.02.009

Zaini, M. K., Masrek, M. N., Sani, M. K. J. A., & Anwar, N. (2018). Theoretical modeling of information security: Organizational agility model based on integrated system theory and resource-based view. *International Journal of Academic Research in Progressive Education and Development*, *7*(3), 390–400, https://doi.org/10.6007/IJARPED/v7-i3/4379

Zou, Q., Sun, X., Liu, P., & Singhal, A. (2020). An approach for detection of advanced persistent threat attacks. *IEEE*, 53, 1-7. https://doi.org/10.1109/MC.2020.3021548

Business Management Research and Applications: A Cross-Disciplinary Journal (BMRA) (ISSN 2769-4666) is an open-access (CC BY-ND 4.0), peer-reviewed journal that publishes original research as well as works that explore the applied implications of others' research, conceptual papers, and case studies (including teaching notes for review) that have a business administration and management slant. *BMRA* welcomes original submissions from researchers, practitioners, and Master's/doctoral students from the following disciplines: business management, occupational safety, cybersecurity, finance, marketing, entrepreneurship, public administration, health services, fire safety, human resources, project management, healthcare management, and information technology. Master's degree-level student authors must be co-authors with faculty or professional researchers in the field. *BMRA* is a participant with the LOCKSS archival system, **Alabama Digital Preservation Network | ADPNet**.

Register and submit your work to

Business Management Research and Applications: A Cross-Disciplinary Journal (columbiasouthern.edu)