Enhancing Employee Cybersecurity Awareness in Small Businesses

Abinet Onkiso

Marywood University

SLAS 6013: Qualifying Seminar

PhD in Strategic Leadership and Administrative Studies

Fall 2024

October 15, 2024

Abstract

With the increased reliance of small businesses on digital operations, the vulnerability to cyberattacks is also increasing, and most small businesses are insufficiently prepared because of a lack of cybersecurity awareness and limited resources. As small businesses increasingly become targets of cyber threats due to their weaker defenses, enhancing cybersecurity awareness among employees becomes paramount. This paper analyzes the factors influencing employee cybersecurity awareness and proposes customized strategies to improve cybersecurity policy compliance and reduce cyber breaches. Through a comprehensive literature review, this research paper discusses the behavioral, technological, and social perspectives that affect employee cybersecurity awareness by utilizing theoretical frameworks such as Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), and Social Cognitive Theory (SCT). It also examines the ethical implications of cybersecurity negligence, bringing out the moral obligation of business leaders to protect sensitive customers and corporate data. This paper highlights the importance of an integrated approach to improving cybersecurity awareness, combining behavioral insights with technological innovation to create a safer digital environment for small businesses. Motivational strategies can help small businesses improve their security posture and prevent potential data breaches by enhancing cybersecurity awareness. Some of the policy recommendations include the importance of increasing cybersecurity involvement through the creation of training opportunities, incentive programs, and collaborative knowledge-sharing platforms specifically targeted at small businesses.

Keywords: cybersecurity, awareness, small businesses, behavior, policy recommendations

Table of Contents

Introduction

In a world that is becoming more digital, cyber threats are becoming more and more imminent for small businesses, as hackers are more frequently selecting them as targets due to their relatively weaker defense systems. Small businesses often struggle to defend themselves when compared to large corporations due to a lack of resources, awareness, and knowledge. Indeed, 43% of cyberattacks are aimed at small businesses, and 57% of these businesses experience at least one cyberattack annually (Ponemon Institute, 2020). Such attacks can cause significant losses, legal consequences, and serious damage to the business reputation. Data breaches cost $4.45 million on average (IBM, 2023). Consequently, small businesses should prioritize cybersecurity and commit resources to defend themselves.

The Cybersecurity & Infrastructure Security Agency (CISA) reports that human error causes 85% of data breaches (CISA, 2022). Employees are the first line of defense against cyberattacks and should be trained to recognize and mitigate risks. According to De Bruijn & Janssen (2017), humans are the weakest link in an organization's cybersecurity strategy due to their lack of understanding. A significant 58% of employees are unaware of how to protect a company from malicious actions, while an overwhelming 98% think that security duties are solely the responsibility of system administrators (Hadlington, 2018). This highlights the necessity of comprehensive cybersecurity awareness programs that equip employees to protect against possible threats. Encouraging employees to embrace a security mindset through cybersecurity awareness training enables them to enhance the protection of their business against attacks. Investing in employee training serves as a forward-thinking strategy that can prevent significant losses.

The phrase "cybersecurity awareness" refers to a strategy focused on informing internet users (employees) about various types of cyberattacks and the weaknesses of data and computer systems in relation to these threats (Abd Rahim et al., 2015). A study by Shaw et al. (2009) characterizes cybersecurity awareness as "the extent to which users recognize the significance of information security and their responsibilities to maintain appropriate levels of information control to protect the organization's data and networks." The main objectives of cybersecurity awareness are to educate internet users about cyber risks and improve their comprehension of these threats. As a result, users are more inclined to embrace secure practices when navigating the digital landscape. As a result, enhancing security for individuals and organizations necessitates minimizing human-related mistakes and weaknesses (Shaw et al., 2009).

Employee behavior is critical for mitigating these risks. Creating cybersecurity effective strategies to protect company' data can be achieved through understanding the factors that influence employee cybersecurity awareness. This research paper investigates the key factors that affect employee cybersecurity awareness in small businesses, supported by relevant literature. This paper utilizes existing theoretical models to explore the factors influencing individuals' behavior and their decisions to participate in cybersecurity awareness programs. The primary research question is, “What factors influence employee cybersecurity awareness in small businesses?”

While there has been extensive research on cybersecurity awareness in general, there remains a significant lack of studies that concentrate specifically on small businesses. Several current frameworks and strategies for cybersecurity awareness are designed primarily for larger organizations, which may not be suitable for smaller businesses. This research paper aims to address that gap by examining customized motivational strategies that take into account the specific challenges and resource limitations encountered by small businesses. The research findings could provide small business leaders with valuable insights and innovative ideas to enhance employee awareness initiatives, thereby improving cybersecurity compliance among employees. Additionally, these strategies could boost employee engagement by fostering a cybersecurity awareness culture that aims to reduce or eliminate cyber breaches and threats.

Literature Review

The expansion of digital technologies and the surge in remote work, which have become increasingly vital due to COVID-19, have also contributed to a rise in risks for cyberattacks. Many small businesses escalated their digital operations in various ways; however, they remain vulnerable due to inadequate security defenses that continue to worsen the situation. Trend Micro 2021 Annual Cybersecurity Report (2021) emphasized that remote work has resulted in an increase in adverse impacts of phishing and ransomware on small businesses because home networks and small devices are less secure than corporate networks and gadgets. According to Keeper Security (2020), only 40% of small businesses have proper cybersecurity measures that they need when facing cyber threats such as phishing scams, ransomware targets, and data breach. Employees play a vital role in maintaining the security of sensitive information and systems. As a result, raising cybersecurity knowledge among employees is critical for protecting against cyber threats. The initial part of the literature review examines the importance of cybersecurity awareness among employees and its impact on organizations. This is followed by an analysis of the factors that influence employee cybersecurity awareness, and the challenges associated with implementing effective programs for enhancing this awareness.

The Importance of Cybersecurity Awareness for Small Businesses

Although organizations allocate significant resources to cutting-edge cybersecurity tools and technologies, relying solely on these measures does not ensure complete protection against cyber threats. Employees, frequently perceived as the most vulnerable point in the security framework, can unwittingly become targets of social engineering schemes or reveal confidential information. Human error is frequently recognized as a primary factor contributing to security breaches. Employees might unintentionally put the organization at risk by engaging in behaviors like clicking on phishing links and using weak password practices (Kraemer-Mbula & Wamuyu, 2020). Phishing attacks frequently utilize social engineering strategies to deceive employees into sharing sensitive information or installing malware (Bada et al., 2019). Organizations can mitigate the chances of human errors that jeopardize security by increasing awareness of these risks. Therefore, organizations must prioritize cybersecurity awareness training as a crucial component of their overall strategy.

Encouraging employee awareness of cybersecurity in small businesses is essential for strengthening their defenses against cyber threats. As cyber threats continue to evolve, emphasizing cybersecurity awareness will be essential for safeguarding organizational assets and ensuring long-term sustainability. The Verizon Data Breach Investigations Report indicates that 43% of breaches targeted small businesses, highlighting the importance of strong cybersecurity measures (Verizon, 2023). Recognizing the potential threats to small business is essential for equipping employees to identify and spot attempts should they arise.

Today, remote and hybrid work environments are more common than ever. Establishing a security-oriented remote environment is essential for the seamless operation of small businesses. Companies that create internal policies to enhance password security, adopt multi-factor authentication (MFA), utilize virtual private networks (VPN), and educate all employees on securing their networks and devices can foster a safe work environment throughout the organization.

Companies that provide cybersecurity training for their staff can experience numerous financial advantages. Accordingly, employee training can reduce the financial impact of a data breach by $232,867 (IBM, 2023). Additional research, such as that carried out by Osterman Research, revealed that smaller companies with fewer than 1,000 employees can achieve an average ROI of 69% by implementing a cybersecurity awareness training program.

Small businesses that incorporate cybersecurity awareness education into their onboarding and continuous training for employees significantly reduce the likelihood of security breaches occurring. Attackers frequently seek the simplest route to infiltrate organizations, often targeting their employees. Employees who can identify phishing or social engineering attempts significantly decrease a company’s vulnerability to attacks.

Cybersecurity awareness safeguards the organization while fostering trust among customers and stakeholders. For small businesses, gaining customer trust is essential for fostering long-term retention. Organizations that emphasize cybersecurity are seen as more trustworthy and accountable. Understanding the significance of cybersecurity awareness among employees is crucial. Organizations can significantly reduce their vulnerability to cyber threats by mitigating human error, promoting a security-first culture, enhancing the overall security posture, ensuring regulatory compliance, and fostering increased trust and customer loyalty. Employees who are well-trained can actively contribute to fostering customer trust and loyalty by serving as advocates for security awareness within organization. Investing in cybersecurity awareness programs is crucial for developing a knowledgeable and proactive workforce that plays a significant role in the organization's long-term success and security.

Consumer data privacy and cybersecurity regulations are constantly changing. Numerous small businesses frequently need to follow specific compliance standards based on their particular industries. Many small businesses that process payments must adhere to PCI compliance requirements. Industries like healthcare or international businesses may also need to comply with HIPAA regulations or GDPR requirements. Employees who are well-trained and informed about potential threats can effectively assist businesses in achieving higher levels of compliance adherence.

Security policy compliance programs encompass several components, including training and communication, where employee motivation is essential for their success. Motivation plays a crucial role in enhancing effective learning and engagement in these programs. When provided with both intrinsic and extrinsic rewards, motivated employees frequently demonstrate improved performance and satisfaction with security policy compliance programs. Intrinsic rewards refer to psychological benefits, including feelings of self-efficacy, autonomy, or competence, whereas extrinsic rewards refer to recognition, feedback, or incentives (Odujinrin, 2023). Employees with higher intrinsic motivation show increased engagement in security training activities. Both types of rewards can boost engagement, enhance knowledge retention, and support skill transfer concerning security policy compliance topics (Odujinrin, 2023).

Particularly when staff members see real benefits or earn recognition for their efforts and successes in security projects, incentives and prizes can significantly boost the drive in compliance programs. Incentives can act as a form of positive reinforcement for individuals engaged in training and demonstrating safe practices (Manhas & Kaur, 2021). These driven individuals diligently seek out opportunities to gain the knowledge and skills necessary to protect organizational assets. Bhuiyan and Hossain (2022) showed that incentives like gift cards or recognition certificates had a positive effect on employee motivation and engagement in these programs.

Through the implementation of engaging training programs, the encouragement of leadership involvement, and the maintenance of clear communication regarding risks, small businesses can develop a culture of security. Support from leadership and clear communication are essential for encouraging other staff and employees to adhere to cybersecurity compliance programs. A strong dedication from leaders will transform and encourage the interest and motivation to participate in employee awareness companies. This positive reinforcement by the leaders will make employees motivated to safeguard the company assets through awareness campaigns Ghani et al. (2021). This can be a showcase that leaders will encourage employees by being involved in cybersecurity awareness campaigns. Furthermore, how personally relevant employees perceive cybersecurity and the threats they encounter influence their willingness to participate in compliance programs.

When employees see the connection between security practices and their professional and personal lives and become aware of the possible ramifications of security breaches, their willingness to engage in cybersecurity compliance initiatives grows (Odujinrin, 2023). One research emphasized the significance of taking personal relevance and threat perception into account to improve staff involvement in security compliance initiatives (Gupta & Rathee, 2021) The benefits of cybersecurity awareness training go further than just stopping data breaches and attacks. A knowledgeable and focused workforce can help the company to develop cybersecurity awareness. Those who understand possible risks and best practices are more likely to make wise decisions while handling sensitive data and using company devices. This proactive strategy can greatly decrease security incidents, thus lessening financial losses, legal liabilities, and harm to reputation.

Factors Influencing Employee Cybersecurity Awareness

Based on the literature, it is widely acknowledged that employees' behavior is much influenced by information, abilities, understanding of cybersecurity, experiences, opinions, and beliefs as well as by their background. Among these, personal motivation and personal ability stand out as two of the most significant sources of influence. Individuals may occasionally grow weary of security protocols and measures, particularly when they view security as a hindrance that obstructs their main activities (for instance, being unable to access a music download site due to a browser warning about potential malware). It can also be quite stressful to maintain a high level of security awareness and vigilance. The emotions outlined here illustrate what is referred to as 'security fatigue,' which can pose significant risks to the overall well-being of an organization or society.

Cultural factors are among the most crucial elements to consider when creating education and awareness messages (Kreuter & McClure, 2004). Culture plays a significant role that can positively impact the persuasion process in terms of security. When messages and ads match the recipient's culture, they work better. In cultures that emphasize individuality, like those in the West, individuals often define themselves by their internal characteristics, including their goals, preferences, and attitudes. In the realm of cybersecurity, a message conveyed in a Western country typically emphasizes the advantages of online security, rather than outlining the general risks associated with a lack of security. In cultures that emphasize collectivism, particularly those commonly seen in the East, individuals often define their identities through their relationships and affiliations with social groups. In this cultural context, individuals often refrain from behaviors that lead to social disruptions. Consequently, they prefer prevention strategies that emphasize avoiding negative outcomes rather than promoting positive ones that they aspire to achieve (Lockwood et al., 2005). Furthermore, risk is perceived as the counterpart to trust and confidence, a notion deeply rooted in social relationships. Addressing the emphasis on various risks within diverse cultural contexts is a crucial element when developing cybersecurity awareness campaigns.

Organizations encounter various challenges in achieving effective cybersecurity awareness, such as insufficient employee engagement, limited resources, complex concepts, human factors and resistance, as well as a constantly evolving threat landscape. The lack of employee involvement and motivation in cybersecurity policy compliance initiatives presents one of the key challenges organizational executives deal with. Rajkumar et al. (2020) underlined the need of using tailored training courses and interactive learning strategies to raise employee motivation. They highlighted how passive training approaches, and a perceived lack of relevance could hinder employees' involvement and motivation. Blythe et al (2015) proposed that future research should shift from using information security policies as a measure of compliance to concentrating on specific security behaviors. Therefore, understanding which cybersecurity behaviors to consider is crucial when developing a security awareness campaign.

Cybersecurity awareness in small businesses employs three distinct perspectives—behavioral, technological, and social/cognitive. Behavioral perspective focuses on understanding how individual behaviors and psychological factors influence employees' cybersecurity practices. Technological Perspective, on the other hand, considers the tools and technologies available for enhancing cybersecurity awareness. Social/Cognitive perspective explores the social dynamics and cognitive processes that affect how employees perceive and respond to cybersecurity risks. Together, these perspectives provide a comprehensive framework for understanding and improving cybersecurity awareness in small businesses.

Behavioral Perspective

The behavioral perspective centers on understanding how psychological factors affect employees' cybersecurity practices. It investigates the psychological and social elements that shape individual behaviors related to cybersecurity. Employees need education on the various cyber threats they may encounter, such as phishing and social engineering (Bada et al., 2019). Employee motivation plays a crucial role in shaping cybersecurity practices; when employees feel a personal responsibility for cybersecurity and recognize its importance in their roles, they are more likely to engage positively (Kraemer-Mbula & Wamuyu, 2020). Implementing motivational strategies, such as recognition and incentives, can further boost employee involvement in cybersecurity initiatives (Kraemer-Mbula & Wamuyu, 2020). Additionally, peer behavior has a significant influence on individual actions. A supportive workplace culture that encourages employees to share knowledge and experiences can strengthen positive cybersecurity practices (Bulgurcu et al., 2010). Employees are more inclined to adopt secure practices when they see their colleagues doing the same, fostering a culture of shared responsibility (Bulgurcu et al., 2010).

Fostering a culture where employees feel personally responsible for cybersecurity can enhance motivation. When employees see their role as integral to protecting organizational data, they are more likely to take proactive measures (Garrison et al., 2020). While a certain level of fear can motivate employees to engage in secure practices, excessive anxiety can lead to avoidance behaviors. Organizations must strike a balance by providing clear information about threats without overwhelming employees (Bulgurcu et al., 2010). Employees' confidence in their ability to recognize and respond to cyber threats affects their likelihood of engaging in cybersecurity behaviors. Building self-efficacy through training can enhance confidence and encourage proactive engagement (Chen & Zhao, 2020).

Attitudes toward cybersecurity significantly influence business owners perceived behavioral control regarding the implementation of protective measures. Positive attitudes—such as recognizing the importance of data security and customer trust—are likely to enhance the likelihood of adopting these measures. Conversely, negative attitudes, such as viewing cybersecurity as a nuisance or an unnecessary expense, may hinder timely action. Research indicates that business owners who view information security as essential to their operations are more inclined to implement defensive measures. Bulgurcu et al. (2010) found that business owners' attitudes toward compliance with cybersecurity regulations directly impact the status of their security measures. Therefore, initiatives aimed at changing attitudes—such as demonstrating the value of cybersecurity—can effectively promote preventive actions.

Technological Perspective

This perspective focuses on the role of technology in supporting and enhancing cybersecurity awareness. Technological factors play a vital role in shaping employee cybersecurity awareness in small businesses. This perspective emphasizes how the tools, systems, and resources available to employees impact their understanding and adherence to cybersecurity practices. The design and usability of cybersecurity tools can significantly influence employee compliance, and engagement. Tools that are intuitive and simple to navigate encourage adherence to security practices (Egelman et al., 2014). Implementing automated systems that provide immediate alerts about potential security threats keeps cybersecurity at the forefront of employees' minds, prompting quicker responses (Chen et al., 2020).

When security measures are complicated or cumbersome, employees may be less likely to follow them. Tools that are simple to use encourage employees to adopt security practices more readily. Systems that integrate seamlessly into daily workflows can reduce friction and promote adherence to security protocols (Egelman et al., 2014). Ensuring that cybersecurity tools are accessible to all employees, regardless of their technical expertise, can enhance awareness and compliance. Training that focuses on how to effectively use these tools is essential (Chen & Zhao, 2020).

Small business owners can rely on cybersecurity technologies, expecting them to be useful in defending their businesses. For instance, tools that enhance the ability to identify threats in real-time or simplify regulatory compliance can enhance their effectiveness and ease of use. When the owners know the need or usefulness of the cybersecurity tools then they prefer to use them since they will understand and appreciate the need to avoid data breaches or rather avoid paying a certain amount of money.

Social/ Cognitive Perspective

This perspective focuses on social learning theory adhesion, peer influence, and self-competency in predicting cybersecurity behavior. Understanding employee cybersecurity awareness in small businesses requires examining the interplay between social and cognitive factors. This perspective focuses on how social interactions, group dynamics, and individual cognitive processes affect employees' attitudes and behaviors regarding cybersecurity. Employees are likely to emulate the behaviors of their peers and supervisors. Employees often look to their peers to determine acceptable behaviors. If the group norms prioritize cybersecurity, individual employees are more likely to follow suit (Bulgurcu et al., 2010). When leaders demonstrate strong cybersecurity practices, employees are more inclined to adopt similar behaviors (Bandura, 1977). A culture of sharing experiences and knowledge among employees can reinforce positive cybersecurity practices. Colleagues who actively discuss security threats and solutions foster an environment that prioritizes cybersecurity (Bulgurcu et al., 2010).

To mitigate the risk of cyber threats, small business owners are forced to adopt best practice by mimicking their competitors. They may be influenced to follow the same because they see other people practicing good security measures in their places. Bohme and Moore studied small business owners' cybersecurity behavior and established that social influence played a huge role. This calls for formation of some communities or even networks where the owners of these businesses can share the experiences as well as the best practice. Formation of professional networks and association around the professionals in a certain field which is focused on information security or cybersecurity can be efficient, as it promotes cooperation and community within the field. Research indicates that firms tend to implement security procedures when they observe other related industries implementing similar measures.

Analysis

Through a review of the literature, four key theories have emerged that are instrumental in understanding employee cybersecurity awareness: Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), and Social Cognitive Theory (SCT). Each of these theoretical frameworks provides unique insights into how employees perceive and engage with cybersecurity practices. By leveraging these theoretical perspectives, organizations can design more effective training and compliance programs that resonate with their employees, ultimately improving their cybersecurity posture.

Protection Motivation Theory (PMT)

PMT is a popular theory in cybersecurity research because it provides a thorough and testable explanation of how fear appeals, and information security practices interact (Odujinrin, 2023). In order to gain a more comprehensive understanding of how individuals respond to fear appeals, Rogers (1975) developed the PMT. PMT suggests that individuals are driven to safeguard themselves from perceived threats by assessing the seriousness of those threats and their capacity to manage them. In 1983, he broadened his theory to include a broader view of persuasive communication. PMT comprises two primary cognitive processes: threat appraisal and coping appraisal. Threat appraisal determines susceptibility to the threat and the perceived severity of the threat, while coping appraisal determines the adequacy of the shield and an individual's capacity to employ it.

Small business owners can utilize PMT to evaluate threats and challenges in the cyber realm and determine whether to implement specific measures. Coping appraisal refers to the small business owner's perception of how effective protective measures are and their sense of self-competence in implementing them. This evaluation involves response efficacy, which refers to the effectiveness of cybersecurity measures in mitigating risk, and self-efficacy, which pertains to the confidence in one's ability to implement and sustain these measures. As for cybersecurity, the owners of small businesses assess potential threats if a cybercriminal attack occurs and their possibility to avert it. According to this theory, the chances of engaging in protective cybersecurity behaviors are high if the business owners think that cyber threats are severe and can affect them.

Key comprehension in respect of PMT entails how small business owners assess the risk of cyber threats. Perceived severity is defined as the magnitude of the harm an attack would pose if the attack was to occur while the perceived vulnerability captures the probability of such an attack. Sadly, small business owners often fail to realize just how big the threat is and fail to consider their businesses as potential targets of cybercriminals, thereby assuming that they do not have anything valuable enough to steal. It makes people lazy and completely unresponsive to even the most fundamental levels of security, like passwords or updating of software. A common misconception that small business owners have is that since they are small, few people will try and attack them compared to large companies. However, as indicated earlier, small businesses are often targeted for attacks because the hackers consider them to have poor security systems. This misunderstanding of risk hinders the adoption of protective cybersecurity measures and addressing it through education and awareness improves the level of protection motivation.

Small business owners feel empowered when they have resources at their disposal; this includes cybersecurity training, simple tools as well as recommendations for cheap security solutions. It also adds onto the chances of adopting protective measures. Moreover, by presenting the current state of cybersecurity as easy and available, through the almost universally applicable cloud solutions, business owners may feel capable of implementing these solutions even if they do not possess significant funds. Clearing the misconceptions about the level of cyber risks and presenting how protective measures can be useful and cost efficient can further improve the adoption of cybersecurity measures among the small business organizations. By enhancing threat perception and offering straightforward solutions, small business enterprises can better safeguard their interests against such challenges.

Theory of Planned Behavior (TPB)

TPB is a highly prominent theory in understanding human decision-making and behavior, having undergone significant testing, adaptation, and application in numerous circumstances. By means of analysis of the effects of attitude, subjective norms, and perceived behavioral control on the act of utilizing cybersecurity technologies, Ajzen's (1991) TPB enhances the knowledge of cybersecurity adoption. This theory presupposes that the actual behavioral intentions, for example, the adoption of protective measures like cybersecurity, are substantially influenced by the personal attitude towards the corresponding behavior, the perceived social norms and the perceived control over the behaviors.

Attitude in TPB is used as a measure that is predictive of the behavior. Small business owners with positive attitude towards cybersecurity – that is those who consider security measures to protect their assets and minimize risks are likely to develop cybersecurity measures. Conversely, some business owners tend to view cybersecurity as overcomplicated, overly expensive, or completely irrelevant, leading them to avoid implementing protective measures. For instance, Bulgurcu et al. (2010) demonstrated that confidence in the favorable results following the implementation of cybersecurity measures influenced the positive perceptions users held regarding security measures that complied with these protocols.

Shifting perceptions can be achieved through sensitization that emphasizes the benefits of enhanced security. If business owners understand the potential risks associated with cyberattacks and the benefits of implementing preventive measures, they may be more inclined to invest in cyberspace protection. Additionally, showcasing successful examples of similar enterprises that have effectively established cybersecurity perceptions can significantly enhance positive attitudes.

If cybersecurity is not valuable within the business owners’ professional network, the samples of which are coworkers who fail to use security measures or who consider them pointless—business owners will not prioritize security investments. Herath and Rao (2009) before having shown that social pressure has influence the intention of adoption of cybersecurity which have an implication on the need for leaders in industries to champion the cause of cybersecurity. To influence positively the subjective norms, measures that would create campaigns on proper handling of cybersecurity within the business circles can be good. Local business sectors through industry associations, local chambers of commerce or through business organization clubs and groups are important in creating awareness of cybersecurity to champion investment in security measures.

Perceived behavioral control is the subjective norm that is created concerning the ease or difficulty of performing a given behavior. Businesses that belong to small enterprises and whose owners believe that they have the skills, resources and knowledge to put up protective measures are therefore likely to protect themselves. Conversely, those who have a limited working knowledge of cybersecurity or who never read about it in the business context for whom addressing the problem or investing in the solution is beyond their capability or interest, might be passive.

TPB is beneficial when considering the determinants which affect small business owners' intention and behavior towards decision to take up cybersecurity adoption. Hence, based on attitudes, subjective norms, and perceived behavioral control, stakeholders can design strategies that can improve cybersecurity compliance and encourage protective practices among small businesses. Inclusion of positive attitude, building the right culture, and enhancing perceived enable users to create an environment that encourages the right image, the right efforts towards better cybersecurity infrastructure in small businesses hence making it resistant to cyber threats.

Technology Acceptance Model (TAM)

This model was initially created to explain how people embrace office productivity software. Based on apparent usefulness and simplicity of use, Davis (1989) proposed TAM as a basic two-factor model. TAM is useful to understand if and when people accept technology within the organizational context especially concerning cybersecurity. According to TAM, the adoption of new technologies is significantly influenced by two primary factors: perceived simplicity of use and perceived usefulness. These factors are important for small business owners to understand, especially when it is a decision to invest in cybersecurity measures to secure the business from cyber risks.

Ease of use is about the perception that a technology is easy to learn, but also easy to use. If small business owners consider cybersecurity tools as being complicated or something only an expert can do, they may not invest in it. Because of this hesitation, the implementation of the right cybersecurity measures becomes very slow and hampered. The study conducted by Venkatesh & Davis (2000) indicates that enhanced usability of cybersecurity technologies can motivate more small business owners to adopt these solutions. This can be achieved through the design of user-friendly interfaces, comprehensive documentation, and readily available customer support. The training and workshop tailored for small business owners could enhance their confidence and proficiency in utilizing cybersecurity solutions. Therefore, alleviating the perception of complexity surrounding these tools could ultimately inspire organizations to implement effective cybersecurity solutions within their operations. Additionally, the perceived ease of use may be enhanced through practical demonstrations, along with workshops. When business owners can test the technologies, they will be using in live environments for a period, they can overcome the necessary barriers and feel empowered to integrate these applications into their companies.

Perceived usefulness according to Compeau et al (1999) means the degree of perceived benefits in using a particular technology in improving the performance of a certain task. The suggested hypothesis concerning the acceptance of information security among small business owners is partially supported by the results of the study: small business owners will employ different kinds of security tools and implement security measures if these tools are efficient in protecting business from threats. According to the study done by Pahnila et al., 2007, perceived usefulness is followed by the intention to use the cybersecurity tools among the small business. When the owners of the businesses realize that cybersecurity measures can act as shields against hackers, shields the customer information, and increase the operational efficiency then they are willing to avail the technologies.

To help build a perception of usefulness, when introducing educational programs to raise cybersecurity awareness, the focus on the realistic opportunities and changes that have resulted from cybersecurity tools, for instance, the use of successful examples or evidence of the degrees of effective attacks, can be useful. Moreover, when one can show that cyber incidents pose significant long-term costs to a firm and its clients, the benefits of such prevention strategies as non-fines for non-compliance, maintaining the customer base, and avoiding losses due to reputation damage would prop up the perceived utility of cybersecurity investments.

Social Cognitive Theory (SCT)

Introduced by Albert Bandura in 1986, SCT emphasizes the role of capacity, observational learning, and social behavior. In the context of cybersecurity, SCT provides valuable insights that help small business owners safeguard themselves against cyber threats.

The theory posits that learning occurs not only through direct experiences but also by observing the behaviors of oneself and others, as well as understanding the consequences of those behaviors within a social environment (Bandura,1986). Self-efficacy is the belief of an individual in their ability to effectively complete specific tasks or behaviors. In the realm of cybersecurity, higher levels of self-efficacy correlate with a greater likelihood of adopting protective measures. Small business owners who believe they possess the skills and knowledge necessary to implement cybersecurity solutions are more likely to take proactive steps to safeguard their businesses.

Training programs that enhance cybersecurity knowledge and skills play a pivotal role in increasing self-efficacy among small business owners. By providing practical training sessions, workshops, and resources tailored to the unique needs of small businesses, stakeholders can empower owners to feel more confident in their ability to address cybersecurity challenges. For instance, hands-on training that allows participants to practice using cybersecurity tools in a supportive environment can significantly boost their self-efficacy. Additionally, mentoring and support from cybersecurity professionals can further enhance self-efficacy. When small business owners receive guidance and encouragement from experts in the field, it can reinforce their belief in their capabilities, making them more likely to embrace protective measures.

Another theoretical construct of SCT is social norms & these are defined as the prevailing patterns of social behavior that are expected from its members within respective group. Different standards set in society can have a major impact on the perceptions of small entrepreneurs about cybersecurity measures. This analysis established that in a business network people will always adopt the current industry standards and norms when protecting against cyber threats is seen as normal practice. Architecting a discourse around cybersecurity in those groups can compel people to embrace the practice as part of the social contract with the respective sphere of industry. When small business owners feel that cybersecurity is the concern of all, he or she is more disposed to practice measures that are in consonance with the general belief. When it comes to cybersecurity best practices, increasing engagement from the audience and making taking an action seem like the natural thing to do by posting through social networks thus contributes to the improvement of cybersecurity.

Promoting great conditions for small business owners is necessary for increasing the practical application of observational learning and perceived self-efficiency. This can be done by creating materials that will be close to the individuals' realities, including internet-based group discussion, workshops or seminars regarding security issues, support groups among them being, cybersecurity support groups. Since small business owners are members of the organizations, these institutions create avenues for sharing information and solutions. Besides, it is possible to involve local chambers of commerce and industry associations to bolster such actions. Cybersecurity cooperation schemes that focus on the improvement of foundational exercises similar to training and keeping consciousness of cybersecurity can complement the call for necessary protective measures, formally enshrine these practices in the organizational culture of the small business.

Ethical Implications

Thoughtful ethical and moral reasoning should be taken into account when trying to address the question, “What factors influence employee cybersecurity awareness in small businesses?” Ethical implications are at the heart of the world of cybersecurity for small businesses. The trust of clients and the protection of sensitive data are vital issues as these kinds of enterprises navigate the complexities of the digital terrain. If it fails to adequately deal with cyber threats, it jeopardizes both individual businesses and the broader digital economy at large. When small businesses fail to take cybersecurity seriously, they are putting their business and their customer base at risk. Sophisticated cyber threats such as data breaches and ransomware inflict damage beyond mere financial loss for an organization or the impacted business. From an ethical standpoint, it is the responsibility of business leaders to safeguard customer information and maintain the integrity of business operations. This duty hinges on trust, accountability, and a commitment to social responsibility.

When customers give their data to a business, it is their expectation that their data, ranging from financial data, contact information and any other sensitive data, will be safe. For a small business that has not implemented adequate cybersecurity measures, a data breach poses a significant risk not only to the information at stake but also to the trust of its customers, which can be severely compromised. Trust is fundamental to all forms of business interactions, and once it is lost, restoring it can be a lengthy process. From a survey conducted by IBM Security (2021), the resultant figure showed that 78% of customers said they would cease patronizing a company that fell victim to cyberattacks. These statistics show that customer trust preservation is one of the primary ethical responsibilities that business leaders have to manage.

Business owners are under moral imperative to exercise stewardship responsibility over information they gather and process. It also involves using measures to put in place measures to guard against breaches of the customer details. Lack of cybersecurity consideration can therefore be viewed as failure in this ethical responsibility. Victims of a breach may go to court, resulting in lawsuits and regulatory fines, which can be an anathema to a small business (Ponemon Institute, 2020). The ethical consideration does not only embrace individual business owners but calls for ethical responsibility of the whole system of small businesses. That is why cybersecurity malpractice in small businesses can affect the overall digital economy. It is quite evident that data breaches can cause businesses to lose lots of money to fraudsters and at the same time affect the business’s suppliers, partners, and customers. The average cost of a data breach was $4.24 million, an amount that small businesses can easily be overwhelmed by (IBM, 2021). Moreover, repeated instances of violations adversely affect customers' trust in online businesses and commerce, hindering the growth of the digital economy.

Overlooking cybersecurity risks raises substantial ethical issues regarding the overall performance of small businesses. Previously, ethical business practices were defined as adhering to laws and regulations while safeguarding the interests of stakeholders. Engaging cybersecurity services during the establishment of a small business reflects a commitment to ethical standards and business integrity. This dedication can enhance and fortify their reputation, fostering customer loyalty and creating a competitive advantage (Caruana, 2021).

There is a fundamental correlation between ethical corporate practices and cybersecurity. Small company organizations that improve cybersecurity not only protect themselves and their clients, but also advance the fairness and accountability of firms in the market. This paper argues that ethical business practices require businesses to preserve their consumers' personal and financial information rather than exploit them. Examples in these instances include customers are put at danger when businesses or organizations do not have adequate cybersecurity safeguards. This unfair treatment might include identity theft, financial loss, and suffering. The ethical aspect of business relations requires one to be proactive in avoiding these hazards, as consumers' rights must be respected and appreciated (Raji, 2021).

The emphasis on cybersecurity can be evaluated in terms of corporate social responsibility (CSR), which states that businesses should only do what is good for them and their stakeholders (Kolk, 2021). Implementing sufficient cybersecurity is one of the fundamental points of the corporate social responsibility of companies. Understanding the responsibilities of a company to society is crucial; it must safeguard its customers' data and personal information. The consequences of cybersecurity negligence by small businesses go beyond a business shutting down and even put the lives of customers and the whole community at risk. The negative impact of inadequate protection of personal information goes beyond simple monetary loss. Any firm that experiences a data breach typically faces serious repercussions, including damage to its reputation, loss of customer trust, and increased regulatory scrutiny. Also, the aftermath of security breach results in long term impacts such as increased insurance costs, loss of credibility to attract investors and partners. These consequences explain why ethical perspectives call for small business organizations to pay attention to cybersecurity as part of operations (O'Leary, 2020).

That is why it is crucial to stimulate the culture of cybersecurity among the representatives of small businesses to contribute to the formation of ethical business practices in the sphere of the digital economy. The prioritization of cybersecurity by small businesses fosters a conducive environment within their industry, setting a positive example for others to follow. This culture change can extend to enhanced cybersecurity measures throughout the sector, through this making the interests of all stakeholders positive (Pratt, 2020). Therefore, there are immensely severe consequences of the ethical considerations of small business cybersecurity negligence. When a business owner prevents cyber threats, he or she complies with the requirement to protect customer information and enhances the values pertaining to electronic commerce. The connection between ethical business practices and adequate cybersecurity highlights the importance of security as a cultural concept for small business owners. Ultimately, acknowledging the significance of cybersecurity is essential for safeguarding individual businesses and ensuring that all market participants are operating in good faith.

Policy Recommendations

In challenging times for small business owners, it is essential to implement specific cybersecurity policies aimed at enhancing awareness, promoting the adoption of security measures, and fostering collaboration among small businesses. This paper outlines policy recommendations aimed at strengthening the cybersecurity stance of small business owners. The main obstacle in this area remains the insufficient awareness and comprehension among owners and staff in small businesses. To address this gap, it is essential to establish intervention measures that involve developing specialized training sessions aimed at helping small business owners and their employees understand and become familiar with the importance of integrating cybersecurity measures into their operations. These programs ought to concentrate on the following elements.

The training programs should outline common threats and risks, ensure familiarity with these issues, and cover fundamental security actions such as password creation standards and software updates. Incorporating real-life examples and applications of the concepts discussed in class will enhance learning outcomes (Gordon, et.al 2021). Dissemination can effectively aid the training when its methods are adapted with flexibility to suit the receivers. Training can take many forms, such as in-person sessions, tutorials or seminars, webinars, online classes, and guided tutorials. Utilizing technology in training can improve accessibility for small business owners.

Government organizations, industry groups, and cybersecurity companies themselves must organize and create training. In this manner, the identified stakeholders can develop efficient and specialized programs that are important for the development of small business. For instance, the Cybersecurity and Infrastructure Security Agency (CISA) must help with the necessary support and orientation for program development (CISA, 2022). Small business owners should ensure that they take their time to learn more about cybersecurity, especially now that the threats are ever-changing. Regularly refreshing minimum and maximum training can help businesses tackle emerging challenges and continually reinforce the idea that cybersecurity is an integral part of their operational model (AlHogail, 2015).

One reason small businesses do not explore cybersecurity protection is the lack of capital. To promote the adoption of established cybersecurity frameworks and technologies, it is advisable for governments and industry organizations to explore the implementation of various financial incentives: Significant investments in security upgrades can place a strain on the finances of small businesses. Providing options like tax deductions or credits for these investments can alleviate some of that pressure. For example, any business can acquire cybersecurity products, tools, or provide certification for their employees in cybersecurity, which would qualify them for tax credits to offset these expenses, as highlighted by Chalabi (2020). It achieves this not only by making cybersecurity investments more accessible but also by emphasizing the importance of protecting small businesses through government support.

Initiating and funding grants to meet the needs of small business owners looking to enhance their security systems provides essential funding for technological investment. These grants may cover expenses related to purchasing cybersecurity tools, hiring consultants, or providing employee training (Jiang et al., 2021). Reducing the expenses of these programs also guarantees that small businesses take the appropriate measures to improve their security against cyber threats. To enhance motivation, small businesses may also be provided with approachable financing options by partnering with banks and credit unions for stockpiling. For instance, financial institutions can provide affordable funds specifically intended for security enhancements, facilitating the sourcing of such funds (Sullivan, 2021). Encouraging small businesses to commit to cybersecurity through incentive schemes fosters motivation. By publicly acknowledging local businesses that pursue recognized cybersecurity certification schemes, governments can foster a culture of cybersecurity within organizations (Chau et al., 2020).

Consequently, the policy recommendations provided in this paper focus on improving training and awareness, funding opportunities, and developing strong networks as a way of overcoming the cybersecurity hurdles those small businesses experience. By implementing these measures, stakeholders can foster an environment where small business owners can prioritize cybersecurity, thereby strengthening the overall security of this crucial aspect of the economy. Enhanced security measures benefit not just the individual organization but also play a vital role in the growth and sustainable operation of the overall digital economy.

Summary

Cybersecurity awareness is a crucial issue for small businesses, particularly in today's world. This issue impacts small companies, which are the economic foundation of many economies. Failure to safeguard them from cyber threats is increasingly prevalent, as most of these companies do not possess sufficient capital or knowledge to protect their data from hackers. This role is further complicated by a dismissive attitude towards risk that is prevalent among small businesses, where numerous owners continue to believe that their businesses are immune to hacking. This misunderstanding not only exposes them to potential breaches but also jeopardizes customer trust and threatens their operational stability.

Statistics reveal the extent of this problem: about 57% of small businesses that have fallen prey to hackers shut down within six months (Haffke et al., 2020). Verizon (2023) indicates that cyberattacks have increasingly targeted small enterprises, with 43% of the cyberattacks. Regrettably, numerous small businesses lack IT departments or the financial resources to implement effective safeguards against cybercrime. The absence of a culture surrounding cybersecurity policies and training exacerbates these effects; thus, it is crucial to improve awareness through practical solutions (Bada et al., 2019).

The literature review provided a comprehensive examination of the factors influencing cybersecurity awareness in small businesses through three distinct perspectives—behavioral, technological, and cognitive/social—integrated with four theoretical frameworks: PMT, TPB, TAM and SCT. From the behavioral perspective, PMT and TPB proved to be very effective in explaining how small business owners assess cyber threats and develop intentions to act. The technological perspective mainly emphasizes the adoption of cybersecurity tools, along with the TAM. The cognitive/social perspective, based on SCT, examined role of social influences and observational learning within cybersecurity practices.

The ethical implications of oversight regarding cybersecurity are notably substantial. It is fundamentally a core business duty to guarantee the protection of customers' data and to foster their ability to place confidence and trust in the organization. Neglecting to address these threats can lead to significant consequences, including financial loss, harm to reputation, and a decline in consumer confidence in the digital economy (Tsohou et al., 2019). This practice prompts inquiries into ethics related to liability and justice. How can that business expect to recover if its customer or stakeholder experiences harm due to the company's failure to implement adequate cybersecurity measures? In these circumstances, ethical business practices become evident, as small businesses are required to implement suitable cybersecurity measures to protect sensitive information and demonstrate responsible operational practices (Fuchs, 2019).

The measure for boosting awareness of cybersecurity among small businesses is an ethical imperative in the pertinent context for the overall digital economy. In short, the overall analysis here reflects the nature of cybersecurity challenges as involved and calls for targeted interventions based on collaborative efforts. Training, financial incentive, and information sharing mechanisms to small business owners can address the root factors that impact cybersecurity behaviors as a way of empowering them on how to take proactive measures against securing their operations and customer data.

Lastly, this study will provide specific policy recommendations that should be adopted in order to reduce the emerging cybersecurity threats affecting small businesses. Through the suggested targeted training programs and financial incentives along with the use of collaborative information sharing platforms, the study seeks to raise cybersecurity and improve the security of small business organizations. The study's results will be viable to owners of businesses, cyber experts, policymakers, as well as scholars focused on enhancing cybersecurity within the small business enterprise.

Further research is necessary regarding cybersecurity awareness training, as it will be particularly beneficial for business leaders or security awareness practitioners involved in developing awareness and training programs, along with businesses that offer learning software modules. Understanding the effectiveness of different training methods and delivery formats can help improve the overall cybersecurity posture of an organization. Additionally, studying the impact of cyber awareness training on employee behavior and decision-making can aid in developing more targeted and impactful training programs. By investing in ongoing research in this area, businesses can stay ahead of evolving cyber threats and better protect their sensitive data and information. Unfortunately, cyberattack activity is expected to escalate.

About the Author

Abinet Onkiso is originally from Ethiopia and has resided in the United States since 2007. He is happily married to his wonderful wife Mety, who is currently in her second year of PsyD studies. They both take great joy in being the parents of two amazing boys: Nathan, who is in 11th grade, and Eli, who is in 4th grade. Abinet earned a bachelor's degree from Addis Ababa University in Ethiopia and a master's degree from Oregon State University in Corvallis, Oregon. During his time at OSU, he effectively utilized his research skills to analyze large volumes of data. In his role as a performance analyst for the State of Washington, Abinet consistently embraced a culture of high performance, emphasizing the importance of excellence and data-driven decision-making. Upon graduating from Marywood University, he aims to become a university professor to impart his knowledge and experience. Alongside his academic career, he plans to engage in applied research projects and provide consulting services for research institutions, government entities, and private sectors. In his spare time, Abinet enjoys traveling with his family and playing tennis and soccer with his kids.

References

Abd Rahim, N.H., et al. (2015), A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 2015. 44(4): p. 606-622.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

AlHogail, A. (2015) “Design and Validation of Information Security Culture Framework,” *Computers in Human Behavior*, vol. 49, no. August, (2015), pp. 567–575.

Alabdulatif, A., Al-Emran, M., Shaalan, K., & Tarhini, A. (2021). Factors affecting employees’ cybersecurity awareness training: An empirical investigation in Saudi Arabia. *International Journal of Information Management*, 58, e102289. https://doi.org/10.1016/j.ijinfomgt.2021.102289

Al-Emran, M., Shaalan, K., & Alabdulatif, A. (2021). The role of psychological factors in employees’ security behavior intention: An integration of protection motivation theory and theory of planned behavior. *Journal of Information Security and Applications*, 60, e102643. https://doi.org/10.1016/j.jisa.2021.102643

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint, arXiv:1901.02672. https://arxiv.org/abs/1901.02672

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (1977). *Social Learning Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bhuiyan, M. A., & Hossain, M. A. (2022). The impact of rewards on employees' participation and behavior in security awareness training programs: A systematic literature review. *Computers & Security*, 122, e102584. https://doi.org/10.1016/j.cose.2022.102584

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *Paper presented at the Eleventh Symposium on Usable Privacy and Security* (SOUPS} 2015), 103-122.

Brown, A., Taylor, B., & Johnson, C. (2022). Strengthening cybersecurity awareness training: The impact of phishing simulations integrated into comprehensive training programs. *Journal of Cybersecurity Education, 10*(3), 217–230.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). *Information Security Policy Compliance: An Empirical Study of the Role of Social Influence and Knowledge*. Journal of Management Information Systems, 27(1), 193-220.

Caruana, R. (2021). Ethics and small business cybersecurity: A corporate social responsibility perspective. Journal of Business Ethics, 179(3), 567-589. https://doi.org/10.1007/s10551-021-04795-7

Chalabi, A. (2020). Government incentives for cybersecurity adoption in small businesses. Cybersecurity and Information Systems Journal, 15(2), 45-56. https://doi.org/10.1016/j.cybsec.2020.101789

Chau, Dorothy & Ngai, Eric & Pullin, Jennifer & Thatcher, Jason. (2020). The Effects of Business-IT Strategic Alignment and IT Governance on Firm Performance: A Moderated Polynomial Regression Analysis. *MIS Quarterly*. 44. 1679-1703. 10.25300/MISQ/2020/12165.

Chen, T. M., & Zhao, W. (2020). *Real-Time Cyber Threat Detection and Mitigation Strategies for Small Businesses*. Computers & Security, 98, 101964.

Compeau, D. R., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. MIS Quarterly, 23(2), 145–158. https://doi.org/10.2307/249749

Cybersecurity and Infrastructure Security Agency (CISA). (2022). Cybersecurity training and exercises. https://www.cisa.gov/cybersecurity-training-exercises

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340.

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. doi:10.1016/j.giq.2017.02.007

Egelman, S., et al. (2014). *Does Password Expiration Encourage Good Security Habits? A Field Trial of Password Expiration Policies*. ACM Transactions on Internet Technology (TOIT), 14(3), 1-24.

Garrison, B., et al. (2020). *Incentives and Motivation: Enhancing Cybersecurity Compliance in Organizations*. Journal of Cybersecurity Research, 5(2), 1-15.

Ghani, A. W., Supramaniam, M., Ramayah, T., & Othman, S. N. (2021). Cybersecurity compliance behavior in organizations: The role of leadership support and communication. *Journal of Business Ethics, 169*(3), 571–591. https://doi.org/10.1007/s10551-019-04277-2

Gordon, L. A., Loeb, M. P., & Zhou, L. (2021). Cybersecurity investment decision making: Accounting, economics, and behavior. Springer.

Gupta, S., & Rathee, S. (2021). The impact of rewards on employee engagement in security awareness training programs: A systematic review. *Security and Privacy*, *9*(2), 35–48. https://doi.org/10.1002/spy2.1010

Hadlington, L. (2018). The human factor in cybersecurity: Exploring the accidental insider. *In Psychological and Behavioral Examinations in Cyber Security*, 46-63.

Hershey, PA: IGI Global. doi:10.4018/978-1-5225-4053-3.ch003

Haffke, L., Kalgovas, B., & Benlian, A. (2020). The leading role of the CIO in digital transformation: Results from a quantitative study. Journal of Information Technology, 35(1), 57-69. https://doi.org/10.1177/0268396220907086

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for understanding security policy compliance. Journal of Computer Information Systems, 49(4), 52-61. https://doi.org/10.1080/08874417.2009.11645853

IBM Security. (2021). Cost of a data breach report 2021. IBM. Retrieved from https://www.ibm.com/security/data-breach

IBM. (2023). *Cost of a Data Breach Report.*

Jiang, Y., Cui, W., & Wang, J. (2021). Grants and subsidies for small business cybersecurity: A policy perspective. Journal of Cyber Policy, 6(2), 177-191. https://doi.org/10.1080/23738871.2021.1890010

Johnston, A. C., Wech, B., & Jack, E. (2020). Engaging Remote Employees: The Moderating Role of “Remote” Status in Determining Employee Information Security Policy Awareness. *Journal of Organizational and End User Computing (JOEUC), 25*(1), 1-23. http://doi.org/10.4018/joeuc.2013010101

Keeper Security. (2020). 2020 data breach industry forecast. https://www.keepersecurity.com/blog/data-breach-industry-forecast-2020.html

Kolk, A. (2021). Corporate social responsibility and small business cybersecurity: A theoretical exploration. Corporate Governance: The International Journal of Business in Society, 21(4), 563-579. https://doi.org/10.1108/CG-06-2021-0227

Kraemer-Mbula, E., & Wamuyu, P. (2020). *Cybersecurity Awareness and Employee Behavior: A Behavioral Perspective*. International Journal of Information Security, 19(4), 341-355.

Kreuter, M. W., & McClure, S. M.: The role of culture in health communication. *Annual Review of Public Health, 25*, (2004) 439-455.

Lockwood, P., Marshall, T., & Sadler, P.: Promoting success or preventing failure: Cultural differences in motivation by positive and negative role models. *Personality and Social Psychology Bulletin, 31* (2005) 379-392.

Lee, S. H., & Kim, J. W. (2022). Communicating for cybersecurity: The efficacy of continuous reinforcement through internal communication channels. *Journal of Information Security Management, 12*(1), 45–62. https://doi.org/10.4018/JISM.2022010103

Manhas, S. K., & Kaur, H. (2021). The impact of rewards on employee participation and behavior in security awareness training programs: A systematic literature review. *Security and Privacy, 9*(2), 49–62. https://doi.org/10.1002/spy2.1011

Mkhize, D. N., & Mavetera, N. (2020). The role of cybersecurity awareness training in mitigating cybersecurity threats in organizations: A South African perspective. *South African Journal of Business Management, 51*(1), e1805. https://doi.org/10.4102/sajbm.v51i1.1805

Odujinrin, A.O. (2023) Promoting Effective Cybersecurity Policy Compliance in Small Businesses, Doctoral Dissertation, Walden University

O'Leary, D. (2020). Data breach consequences and regulatory responses in small businesses. Journal of Information Systems, 34(3), 215-230. https://doi.org/10.2308/isys-19-095

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. Computers & Security, 26(1), 80-89. https://doi.org/10.1016/j.cose.2006.09.001

Ponemon Institute. (2020). The state of cybersecurity in small and medium-sized businesses. https://www.ponemon.org/local/industryspecific/2020/2020-state-of-cybersecurity-report.pdf

Pratt, J. H. (2020). Creating a cybersecurity culture among small business owners. Journal of Digital Economy, 6(1), 111-124. https://doi.org/10.1016/j.digeco.2020.100212

Raji, I. D. (2021). Ethical considerations in small business cybersecurity: The role of fairness and responsibility. Journal of Business Ethics, 172(4), 791-807. https://doi.org/10.1007/s10551-020-04725-7

Rajkumar, R., Krishnamoorthy, S., & Dhamija, R. K. (2020). Factors influencing employees' cybersecurity behavior: A literature review. *Journal of Information Security and Applications*, 51, e102430. https://doi.org/10.1016/j.jisa.2020.102430

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). Guilford Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93-114.

Shaw, R.S.; Chen, C.C.; Harris, A.L.; Huang, H.J. The impact of information richness on information security awareness training effectiveness. *Comput. Educ*. 2009, 52, 92–100.

Sullivan, K. (2021). Financial institutions and small business cybersecurity: Partnerships for protection. Journal of Financial Regulation and Compliance, 29(3), 243-259. https://doi.org/10.1108/JFRC-04-2021-0041

Trend Micro 2021 Annual Cybersecurity Report (2021) *Navigating New Frontiers: Trend Micro 2021 Annual Cybersecurity Report.* https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Verizon. (2023). 2023 *Data Breach Investigations Report*. Verizon Communications. Retrieved from https://www.verizon.com/dbir