Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses

Tabisa Ncubukezi
Information Technology Department, Faculty of Informatics and Design, Cape Peninsula University of Technology, Cape Town, South Africa
ncubukezit@cput.ac.za

Abstract: Cybersecurity is essential for all organizations, especially during this menacing Covid-19 global pandemic. The sudden transition of leaving the offices to work from home – the 'new normal' – has introduced information security-related risks associated with human factors. For example, both criminals and employees use the same platform for information exchange but with starkly different intentions. But both their actions compromise information and computer security. Criminals intentionally exploit systems to gain unauthorized access for their benefit, while employees make careless mistakes, leaving systems exposed and vulnerable. The present study examines human errors influenced by actions, attitudes, and behaviors that affect overall information security. Purposive sampling within the qualitative approach was used to select thirty (30) small business managers. Data was collected using a qualitative online survey as a Google Form. The study used thematic analysis. The results revealed that repeated human mistakes compromise information security principles and render employees the weakest link. The study explained the risks caused by employees due to ignorance or poor decision making, technical-related errors, and skills- and policy-based errors. Even though small businesses do not require a 'one-size-fits-all' security approach, recommendations to reduce human mistakes were made.

Keywords: Computer security, cybersecurity, cyber threats, data breaches, human errors, information security, skills-based errors, small businesses

1. Background of the study

The state of cybersecurity as an ongoing topic has gained popularity in academia. The literature presented the state of cybersecurity, common cyber threats, their impact on businesses, and technology-related issues (Akhtar, Sheorey & Bhattacharya, 2021). Studies expose increased cybercrimes that affect information security, economic and business growth (Tam, Rao & Hall, 2021). For example, during the IMB security week in 2020, Sizwe Dlamini stressed the financial impact caused by cyber incidents, estimated to be R40.2 million per breach. And the estimation of the study fell short of including all organizations in South Africa (SA). Many studies have explored security threats and attacks initiated by cybercriminals. As a result, most studies report that increased data breaches and loss of information among businesses are associated with cybercriminals. This present study's interest is on internal users rather than criminals. Schneier (2000) highlights that people have become the weakest link in the chain of handling information, despite that employees tend to believe that their actions on a system cannot yield to security breaches (Hadlington, 2017; Herath & Rao, 2009).

On the contrary, several studies reveal the ignorance of business employees who often become an entry for cybercrimes (Sasse, Brostoff & Weirich, 2001). Solvere (2021) believes that cyber-attacks can be generated inside or outside an organization, rendering employees the most significant threat. The main cyber-attacks are, in fact, from human actions (Annarelli, Nonino & Palombi, 2020). Despite numerous studies on the impact of human factors on cybersecurity, human factors remain at the core of many cybersecurity breaches. As in this study, humans are business employees who carry out business processes to achieve business goals. Some studies refer to employees as the weakest link because of their power in exposing organizations (Annarelli, Nonino & Palombi, 2020). The term links employee negligence in making decisions that weaken an organization's information security (Teufel et al., 2020).

Human mistakes can frequently result from a convenient use of shortcuts to make employees' lives easier while exposing businesses to threats. Such incidents qualify the human element as a channel for attacks and a significant source of data breaches (Kobis, 2021). This research is presented alongside the alarming increase in cyber incidents caused by human behaviors within the small business space. This paper responds to the study of Ncubukezi, Mwansa, and Rocaries (2021), explaining that human-generated mistakes should be acknowledged when planning and implementing best practices to promote good cyber hygiene. The current work examines human errors fuelled by attitudes, actions, and behaviors that have emerged recently as a serious concern and a door to increased data breaches. This paper further presents the common types of human errors, their impact, and vulnerability mitigation strategies to improve the overall security of information processing.

The rest of the paper is structured as follows: cybersecurity relating to human factors, followed by the method of inquiry, results, and discussions. The final section presents the recommendations, contributions, future study suggestions, and concluding remarks.

2. Cybersecurity

Cybersecurity has many dimensions – cyberspace, information security, human factors, and computer security –necessitates that organizations identify loopholes and protect themselves from various cybercriminals (Ncubukezi & Mwansa, 2021). This study focuses on human factors, which presently receive less attention than technological or policy aspects related to security (Ergen, Ünal & Saygili, 2021). During the process of information flow, the human element is the key role player. Human errors are accidental actions influenced by attitudes, knowledge, and behaviors that expose businesses to quantified cyber threats and attacks. Figure 1 illustrates how employees work within the information flow to carry out their duties. The figure shows employees, services, a firewall to filter incoming and outgoing traffic, Internet connection, and the perpetrator. When proper security measures and firewalls exist with appropriate applications, employees receive error-free services. Perpetrators are unable to find a way to penetrate a system.

However, criminals use any opportunity to gain unauthorized access when security measures are absent, resulting in significant damage. This loophole is due to cyberspace and its nature, which is convenient, open, and grants equal access to all users (Ncubukezi, Mwansa & Rocaries, 2020). So access to timely and open cyberspace allows for cyber-attacks through user actions depending on safety measures applied.

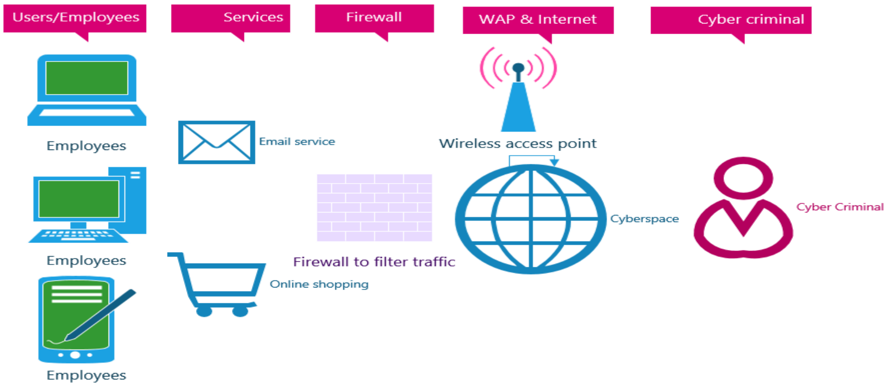

Figure 1: User processes during the information processing (Source: Own work, 2021)

2.1 Security risks posed by human errors

Human factors are regularly underestimated and overlooked (Hadlington, 2017) and are vital factors that affect a business's information security hygiene (Anwar et al., 2016). The challenge stems from the diverse range of human errors which ultimately grant unauthorized access to sensitive information and other business assets, resulting in significant data and security breaches. Employee mistakes pose a risk in companies. In fact, the rise and severity of security problems reported in recent years suggest that organizations are more vulnerable than ever (Sasse, Brostoff & Weirich, 2001). As illustrated in Figure 2, human errors are influenced by certain attitudes, behaviors, and actions that promote unsecured connections. These ignorant actions expose valuable, sensitive business information and resources to opportunistic criminals. Criminals then highjack secure sessions to violate privacy (Wallace et al., 2021). When cybercriminals take over, they compromise information security principles like data confidentiality, availability, and integrity. Confidentiality, a fundamental principle to promote protection against unauthorized disclosure of data or information, focuses on keeping information private. Data is only available to or can only be accessed by the correct recipient to carry out expected duties (Njoroge, 2020). The confidentiality principle includes people protecting others by restricting personal or sensitive information sharing unless explicit permission is granted (Alexei & Alexei, 2021).

The second principle focuses on the protection of data or information to promote its integrity. Business data should not be accessed for unauthorized modification, additions, or deletions. The integrity principle promotes trust and accuracy so that data remains the same (Angafor, Yevseyeva & He, 2020). Consequently, integrity encourages adherence to ethical tenets and fairness (Alexei & Alexei, 2021). Criminals typically take chances when an employee acts negligently on a system, thereby opening a door for data leakage (Ergen, Ünal & Saygili, 2021).

The third and final principle protects and promotes system functionality by ensuring that data is always available for authorized users (Zimmermann & Renaud, 2019). Any ignorant action of the user could expose the system and information to attackers who compromise the principle, resulting in poor service and delayed decision making.

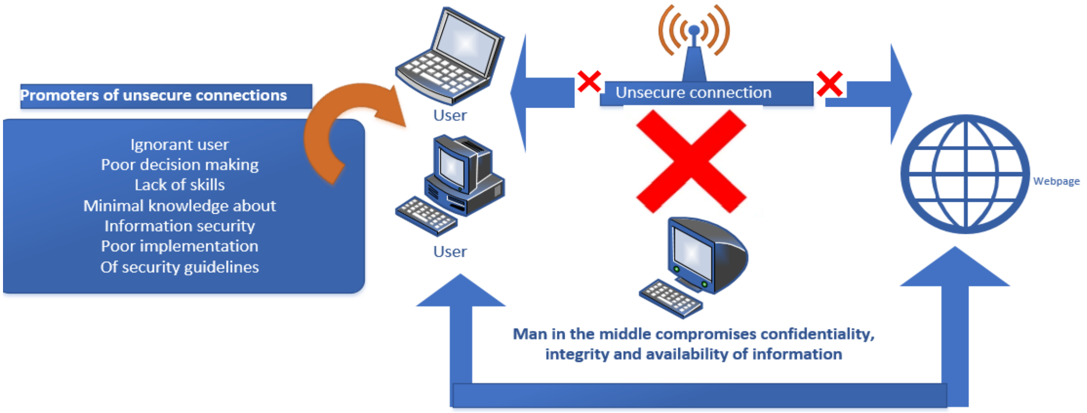

Figure 2: Illustration of the man in the middle attack (Source: Own work, 2021)

Given the above, human actions can undoubtedly affect the primary principles of information security, compromising business information and computer security. Information security principles are affected by threats associated with human factors such as social engineering, malware, phishing, worm, and spyware (Karaci, Akyüz & Bilgici, 2017). Alexei and Alexei (2021) insist that threats related to spoofing, access to unauthorized data lead to data theft and malicious programs. The implications of compromised information security as the result of human factors are presented below.

2.2 Common human mistakes

Cybersecurity risks relating to human mistakes affect various businesses because of the connection to standalone or networked computers. Moreover, Kobis (2021) believes that the human factor is the leading factor in infiltrating sensitive information. For standalone computers, employees may use memory sticks which a virus may infect. Or, for example, employees may follow a website's links or accidentally respond to unknown links that gather sensitive information. Increasingly, data breaches occur through the unauthorized disclosure of personal information (Richardson et al., 2020). Another example is when users curiously, recklessly, and ignorantly open fake emails containing malware attachments which automatically installs when opened.

Moreover, a user could install malware attached to standard applications. Often the infected installation package is available on a website to trap unknowledgeable users. In this case, the unaware user downloads and installs software from unverified sources (Kobis, 2021). Other users serve as a channel for criminals by the way they handle their passwords. Such behavior may result from a poor ability to remember accepted characters for password criteria, understaffing, and employee overload with work demands. At times, unacceptable user behavior is exacerbated by a lack of support or the absence of relevant training. This mistake is a gap that influences poor decision-making (Sasse, Brostoff & Weirich, 2001). Some user attitudes affect common mistakes; for example, when a user insists, "It won't happen to me" (Richardson et al., 2020).

3. Research method

This qualitative interpretive study used purposive sampling to select the research participants most likely to share valuable and appropriate information about the study. The sample comprises business managers representing the population of the study. The chosen sampling method aids the researcher in gaining insightful information based on participant knowledge and experience regarding human errors in small businesses. Furthermore, the process allows the researcher to detail the significant impact of the research findings.

Participants: The research participants had more than two years of experience and provided insight into the current study. A total of thirty (30) respondents were selected from the supply chain business sector, and each participating business had a range of twenty (20) to eighty (80) employees. The research participants comprised a combination of males and females between 38 and 50 years of age.

Selection criteria: This study focused on small information and communication technology (ICT) businesses. The ICT business sector has been chosen based on its dependency on ICT resource usage, especially during the global Covid-19 pandemic. The criteria for selecting these businesses are twofold: 1) that companies have a range of 1 to 50 employees, and 2) that companies have a turnover of less than or equal to R10 000 000 a year.

Recruitment of participants: Research participants were invited to a virtual Zoom workshop for small businesses. The researcher followed up with an email, a consent form, and a link to the online survey. All participants receiving the email took part in the study and completed the questionnaire, giving a 100% response rate. All respondents assured their details and the data collected would remain private, confidential, and anonymous.

Data collection method: The study used an online qualitative questionnaire to gather data from knowledgeable and experienced participants. The current Covid-19 pandemic has escalated the use of online surveys on Google Forms. The questionnaire contained closed-ended questions (such as participant position, number of years in the company, number of employees in the business). In addition, open-ended questions were asked to ascertain the participants' awareness and their businesses about various types of human errors, the impact of the errors, and their businesses' current vulnerability mitigation strategies.

Analysis of data: This research used thematic analysis to uncover relevant themes by analyzing patterns, differences, and similarities in the collected data. This flexible, interpretive data analysis method assists a researcher in investigating participants' points of view, searching for differences and similarities (Braun & Clarke, 2006). The analysis method involved data preparation by searching across data sets to identify data, analyze pieces of data, and interpret data in a meaningful manner for the presentation of data. The process allowed the researcher to categorize data using the visual color-coding method for the initial codes generation. The researcher then prepared and organized the collected data using the visual method to search for themes. Data was then reviewed and explored to validate the themes using a thematic map. The data were categorized and interpreted on a board to search for patterns and similarities to define the themes. A final report of the findings was generated based on the interpretation of the collected data. The following themes emerged and were cohesively presented:

- factors influencing human errors;
- impact of the human errors; and
- vulnerability mitigation strategies.

4. Results and discussions

The current study examined human errors influenced by employee actions, behaviors, and attitudes that negatively influence the state of information and computer security. Every effort performed by employees on a system results in either a positive or a negative impact. This study demonstrated the different experiences relating to human factors that threaten information resources in information management. This research pertains to small businesses in the supply chain industry.

Table 1 shows several questions asked to gather data relating to types of human behaviors in information security and their root causes. These questions are based on employee experiences that influence unauthorized access to a business system. Human actions on business systems are generally shaped and influenced by the nature of the business environment, the level of awareness, and the enforcement of existing policies. Employee ignorance and decision-making typically cause these actions: inadequate skills for interacting with the system, related technical errors, and policy-based errors. The table's four columns present questions based on types of human error, followed by employee actions related to human errors. The table also has 'yes' and 'no' columns. Those businesses that experienced employee activities that negatively impacted the system are presented on the 'yes' column, while those which have not experienced employee mistakes are in the "no" column. Both the 'yes' and 'no' columns show the percentage of participant responses.

Table 1: Questions asked that relate to the employee errors

Questions based on the human error type	*Employee actions relating to the error type*	*Yes*	*No*
1. Do you experience human errors relating to employee ignorance and poor decision-making?		*81%*	*19%*
2. What are the employee actions relating to employee ignorance and poor decision-making?	• Deleting important files without a clear understanding of their value	58%	42%
	• Sending emails or documents with sensitive data to incorrect recipients or public platforms	39%	61%
	• Making unnecessary changes in documents	23%	77%
	• Sending sensitive business data via unsecured platforms	19%	81%
3. Do you experience skill-related to human errors?		*36%*	*64%*
4. What are the employee actions relating to the application of skills?	• Lack of awareness due to employee age	46%	54%
	• Following and opening email links and attachments from unknown recipients	69%	31%
	• Lack of proper understanding about cybersecurity	82%	18%
	• Using unsecured connections when sending sensitive data	12%	88%
5. Do you experience technical-related errors?		*51%*	*49%*
6. What technical errors have you experienced?	• Misconfigured business assets to permit unauthorized access	28%	72%
	• Lack of backup systems for critical data	78%	22%
	• Ignoring software updates	64%	36%
	• Downloading unauthorized software applications	47%	53%
	• Performing unauthorized system changes	38%	62%
7. Do you experience policy-based human errors?		80%	20%
8. What are the causes of those policy-based human errors?	• Poor handling of passwords and sensitive data	73%	27%
	• Misuse of access of rights and privileges	40%	60%

4.1 Factors influencing human errors

As illustrated in **Table 1**, participants shared their different experiences, including their take on human errors and how employees make those errors. Businesses have become victims of human error, and human mistakes are one of the biggest challenges for small businesses (Kobis, 2021). Several respondents confirmed the notion of the "human as the weakest link." With the growing rate of common mistakes by the employees within the business space, Kobis (2021) suggests that the cybersecurity behaviors of employees should be scrutinized as they form a significant part of the business. Various negative actions and employee behaviors are detrimental to the business sector, especially in organizations' private information and financial aspects (Ergen, Ünal & Saygili, 2021).

The results revealed that some human mistakes are caused by employee ignorance and poor decision-making, which Turk (2013) associates with staff shortage, fatigue, or working speed. Every business has a technical side that should not be ignored, and employees need to be equipped to understand technical terms (Campean, 2019). The business sector should engage a vigilant management team to enforce policies and security measures for information processing, people, hardware, and software (Greavu-Serban & Serban, 2014). The absence of a dedicated cybersecurity team and management involvement poses a risk, increasing poor adherence to and enforcement of policies and guidelines.

4.2 Impact of the human errors

Table 2 presents the questions regarding the impact of human errors within the small business sector. The effect of human errors has increased significantly during Covid-19. The study posed the following questions to gain an understanding of the effect of human behaviors.

Table 2: Impact of the human errors

Questions based on the impact of human errors
1. How have human errors during the global Covid-19 pandemic affected your business?
2. What is the primary area of the business negatively impacted as a result of human errors?
3. What are the main influencers of and contributors to human errors?
4. What employee actions relate to the application of skills?

The sudden Covid-19 global pandemic introduced changes in all institutions and persons. Everyone relies on the Internet as the backbone for communications and other daily operations during this present season. With increasingly convenient use and dependency on the Internet, criminal innovation has spiked and attempted new strategies. Sometimes, human mistakes serve as a channel for attracting a diverse range of attacks and threats that negatively affect the system. When asked about *the impact of human errors within the business during the pandemic,* the results revealed various experiences. Fifty-two percent of the respondents indicated a loss of data; 49% admitted to a loss of client trust; 28% were affected by psychological risks of managers; and 46% indicated societal implications, which eventually marred the business reputation. Sixty-eight percent of the respondents further indicated that the consequences of human errors resulted in the loss of money and investors; 68% experienced business disruption, and 60% indicated that their business eventually verged on discontinuing. Participants believe that human errors pose a significant threat to businesses. The primary sources of human errors are employees' diverse attitudes, behaviors, and actions influenced by employee moods and feelings.

According to participants, various reasons influence employee actions, attitudes, and behaviors. For example, participants mentioned that human errors are caused by the following: downloading suspicious attachments; following unknown links; minimal data backup systems; employee ignorance; employee attitudes; poor decision making; lack of cybersecurity skills and awareness; failure to use strong passwords; unlimited user access privileges; and other technical-related errors. Ignorance and poor adherence to mitigation measures cost businesses money, investors, growth, and societal impact resulting in a poor reputation, business disruption, data loss, client loss, and eventually business discontinuity (Ncubukezi, Mwansa & Rocaries, 2020). Human errors cause significant damage to businesses and remain a primary security concern. Cyber-attacks result in substantial economic harm that ruins businesses (Teufel et al., 2020). One participant believes that *"risks are not for small businesses."* Another respondent suggests that *"taking security measures should not be the employee responsibility; instead, it should be the company's responsibility*." Results indicate that human attitude contributes to the actions of the system. Unsurprisingly, 50% of the respondents confirmed that "*applying safety measures is time-consuming*." In contrast, 37% of the participants did not regard human errors as contributing to business risks. Some participants admitted that they are a human *"who is bound to make mistake*s."

4.3 Vulnerability mitigation strategies

Table 3 lists the questions about mitigation strategies that small businesses are adopting to protect their assets. Various participants shared their security measures to guard against unauthorized access.

Table 3: Security measures used

Questions based on the security measures used
1. How is the state of your current mitigation strategies?
2. How are the systems continuously updated?
3. What are the current protection measures used?
4. What are the employee actions relating to the application of skills?

With all the apparent human-related challenges, participants were queried about the *state of the current mitigation strategies. M*ost participants indicated that their businesses currently have mitigation strategies even though proper implementation is not guaranteed. As one participant explained, *"We currently do not have a dedicated person to enforce the creation of strong passwords."* When asked about the continuous updates of the system and software, 62% of the respondents admitted to not running automatic updates because they feel the process consumes time. One respondent explained that *"sometimes we do not run the system updates as they delay us on our activities."* When asked about *current protection measures,* the respondents identified measures such as antivirus software and passwords. Only 78% of the respondents claimed to back up their information, while 22% believed their data was "*protected and out of reach*." All participants agreed that their primary security measure is based on the use of username and password. The nature of cybersecurity involves humans – both legitimate (users) and illegitimate (criminals) – fighting for access to information and other resources (Assante & Tobey, 2011). Torten, Reaiche, and Boyle (2018) assert that as it is challenging to manage and guard human behavior, mitigation strategies are essential for every business. They further suggest that users should consistently practice safe and secure behaviors on the system.

Ncubukezi, Mwansa, and Rocaries (2021) explain that good security hygiene results from consistent, effective mitigation strategies. The continuous protection of business assets reduces human mistakes which threaten a business (Kobis, 2021). Many business systems are vulnerable to a diverse range of attacks and require proactive security measures that guard against every form of threat. Then, it is essential to continuously improve information security awareness (Aldawood & Skinner, 2018) by introducing programs that address strategies to protect against data breaches and reduce the likelihood of human-related risk (Alshaikh & Adamson, 2021). Unskilled users are most likely to make skills-related and technological errors from their lack of awareness and use of jargon. The absence of centralized account management is a significant challenge requiring an immediate solution. This risk is associated with policy-based errors, which arise when no detailed guidelines steer the use of a management database. As a result, poor management of user accounts and passwords opens a door for attackers (Greavu-Serban & Serban, 2014). Highly skilled employees promote good cyber hygiene for business systems (Lee & Rid, 2014).

The diverse business experiences reveal minimal practices of strategies that promote effective cybersecurity. As deliberated in section 2 of the paper, cybersecurity should be implemented on all levels. It becomes essential for every business to implement effective protection measures to decrease exposure to threats. Cybersecurity should be enforced and regularly reviewed for its effectiveness on all levels.

4.4 Recommendations

This paper forms part of ongoing Ph.D. work. With previous papers also linking to the main research, this study explores the business sector's human aspect. This study adopted best practices that should be taken into account (see Kayumbe & Michael, 2021; Coventry et al., 2014): use and management of passwords; use of updated antivirus and firewalls; use of updated software; shutting down of a computer; use of secure connections and websites; avoidance of phishing scams; limiting personal information; continuously checking physical surroundings when online, and reporting cybercrimes. Even though the 'blanket approach' is not overtly practical or serves all businesses, this study suggests general measures promote healthy systems.

Employees: It is necessary to understand the importance of cybersecurity. There should be regular training and awareness programs about essential security topics (including real-world scenarios), encouraging regular discussions, creating open platforms for questions, using daily security reminders, and monitoring employee activities. These security practices will keep users updated and abreast of the latest trends of attacks, thereby diminishing the chances of privacy violations.

Management: Business leaders should make informed decisions to set clear policies, rules, guidelines, and procedures for enforcing cybersecurity compliance; for example, enforcing the generation of passwords with adequate characters or enforcing two-factor authentication to reduce the chances of unauthorized access on a business network. Two-factor authentication is an electronic technique that increases security on applications or websites by enabling multiple authentications per session. It is one of the authentication mechanisms which grants access only after multiple verifications.

Information: Businesses must back up their systems daily to recover business data if a system is compromised, control physical access, and improve the security of payment processing.

System and technical: Businesses must limit access rights and privileges, install and update methods to protect against network attacks, including firewalls and encryption methods, conduct ongoing vulnerability testing on networks, and implement tools to scan networks and applications to detect a breach automatically.

5. Concluding remarks

Security of information and computers is a challenging task for any organization. While most research focuses on cybersecurity's technological and policy aspects, fewer studies have investigated human factors. This study reveals the impact of human error influenced by employee behaviors, attitudes, and uncontrolled actions in cyberspace. These activities have the potential to weaken business systems. It cannot be denied that human error is the primary contributing factor of cyber risk in the small business sector. In these uncertain times, cybercriminals use every opportunity to gain access to business systems.

Consequently, all businesses must resort to solutions that promote the longevity of the company. This work reports the causes and types of human errors and small business employee human error impact. This work also presents the recommended strategies for reducing cyber risks relating to human errors. The outcome discovered a range of factors relating to human error that compromise the privacy and security of business systems.

As a contribution: This work shares insights and escalates awareness of unintentional actions of small business employees. The study further shares insights about employee ignorance, which leads to poor decision-making, deficiency of awareness, understanding, and skills, and the necessary implementation of information procedures and computer security guidelines.

In the future: The researcher should explore employees' intentional actions (inside attempts) that result in successful data breaches within the small business sector. Furthermore, a study should include other business sectors. It would be of good value for the researcher to embed artificial intelligence to reduce risks.

Acknowledgements

I thank the reviewers for the time spent generating the feedback. I acknowledge and thank National Research Foundation (NRF) Black Academics Advancement Programme (BAAP) for financing this work.

References

Akhtar, S., Sheorey, P.A. and Bhattacharya, S. 2021. Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward. *International Journal of Business Intelligence Research*, 12(1), 82-97.

Aldawood, H. and Skinner, G. 2018. Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62-68.

Alexei, A. and Alexei, A. 2021. Cyber Security Threat Analysis in Higher Education Institutions As A Result Of Distance Learning. *International Journal of Scientific & Technology Research,* 10(3), 129-133.

Alshaikh, M. and Adamson, B. 2021. From awareness to influence: toward a model for improving employees' security behavior. *Personal and Ubiquitous Computing*, 1-13.

Angafor, G.N., Yevseyeva, I. and He, Y. 2020. Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and privacy*, 3(6), e126.

Annarelli, A., Nonino, F. and Palombi, G. 2020. Understanding the management of cyber-resilient systems. *Computers & Industrial Engineering*, 149, 106829.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.

Assante, M.J. and Tobey, D.H. 2011. Enhancing the cybersecurity workforce. *IT Professional*, 13(1), 12-15.

Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Campean, S. 2019. The Human Factor at the Center of a Cyber Security Culture. *International Journal of Information Security and Cybercrime (IJISC)*, 8(1), 51-58.

Coventry, L., Briggs, P., Blythe, J. and Tran, M. 2014. Using behavioral insights to improve the public's use of cyber security best practices. *Gov. UK Report*.

Dlamini, S. 2020. *Data breaches cost SA companies R40.2 million on average in 2020.* Available from https://www.iol.co.za/business-report/companies/data-breach-costs-sa-companies-r402-million-average-in-2020-6649ae0a-b803-482c-978f-b395517c7fa7 [accessed on 12 September 2021].

Ergen, A., Ünal, A.N. and Saygili, M.S. 2021. Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies*, 10(4), 210.

Greavu-Serban, V. and Serban, O. (2014). Social engineering is a general approach. *Informatica Economica*, 18(2), 5.

Hadlington, L. 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon*, 3(7), e00346.

Herath, T. and Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Karaci, A., Akyüz, H.I. and Bilgici, G. 2017. Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094.

Kayumbe, A. and Michael, L. 2021. Cyber threats: Can Small Businesses in Tanzania outsmart Cybercriminals? *International Research Journal of Advanced Engineering and Science*, 6(1), 141-144.

Kobis, P. 2021. Human factor aspects in information security management in the traditional IT and cloud computing models. *Operations Research and Decisions*, 31(1), 61-76.

Lee, R.M. and Rid, T. 2014. OMG Cyber! Thirteen Reasons Why Hype Makes for Bad Policy. *The RUSI Journal*, 159(5), 4-12.

Ncubukezi, T., Mwansa, L., and Rocaries, F. 2020. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. *International Conference for Internet Technology and Secured Transactions (ICITST)*, 15, 283-288. IEEE.

Ncubukezi, T., Mwansa, L., and Rocaries, F. 2021. Analysis and Impact of the Cybercrimes in the Western Cape Small and Medium-Sized Businesses. *International Conference on Cyber Warfare and Security*, 16, pp. 425-235. Academic Conferences Limited.

Ncubukezi, T. and Mwansa, L. 2021. Best Practices Used by Businesses to Maintain Good Cyber Hygiene during Covid19 Pandemic. *Journal of Internet Technology and Secured Transactions*, 9(1), 714-721.

Njoroge, GM 2020. *Human Factors Affecting Favourable Cybersecurity Culture-a Case of Small and Medium-sized Enterprises SMEs Providing Enterprise-Wide Information Systems Solutions in Nairobi City County in Kenya* (Doctoral dissertation, University of Nairobi).

Richardson, M.D., Lemoine, P.A., Stephens, W.E. and Waller, R.E. 2020. Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, 27(2), 23-39.

Sasse, M.A., Brostoff, S. and Weirich, D. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), 122-131.

Schneier, B. (2000). *Secrets and Lies: Security in a Digital World.* John Wiley & Sons.

Solvere, O. 2021. *Cyber Attacks on Small Businesses Increase.* Available from https://www.solvereone.com/pages/cyber-attacks-on-small-businesses-increasing-in-2021/ [accessed on 16 September 2021].

Tam, T., Rao, A., and Hall, J. 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, 102385.

Teufel, S., Teufel, B., Aldabbas, M. and Nguyen, M. 2020. Cyber Security Canvas for SMEs. In *International Information Security Conference*, 20-33. Springer, Cham.

Torten, R., Reaiche, C. and Boyle, S. 2018. The impact of security awareness on information technology professionals' behavior. *Computers & Security*, 79, 68-79.

Turk, R.W. 2013. *Preparing a Cyber Security Workforce for the 21st Century*. Army War College Carlisle Barracks, PA.

Wallace, S., Green, K., Johnson, C., Cooper, J., and Gilstrap, C. 2021. An Extended TOE Framework for Cybersecurity Adoption Decisions. *Communications of the Association for Information Systems*, 47 (2020), 51.

Zimmermann, V. and Renaud, K. 2019. Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.