Digital Risk Management: Investigating Human-Factor Security with a Behaviorist Approach

Ruan Pretorius and Dewald Blaauw
Stellenbosch University, Cape Town, South Africa
ruanpretorius.rp@gmail.com
dnblaauw@sun.ac.za

Abstract: The successful digitization of modern organizations relies on the cohesion between information technology and the workforce responsible for managing and operating it. Without proper management and operation, even the most sophisticated technologies may become vulnerable when operated by an incompetent worker. Numerous studies acknowledge human vulnerability in cyber security, known as human-factor security, as the "weakest link" in a digitized organization's security posture (Ani et al., 2019). It was found in literature that there exists a shortage of focus on the impact of human-factor security on information and data security in organizations. Through risk management frameworks, the focus is placed much more on the risks posed by technologies, as on the risks presented by humans implementing, managing or interacting with these technologies. Thus, the need to investigate how risk management frameworks could be applied to human-factor security in digitized organizations arise. This paper offers an in-depth understanding of the behavioral and cognitive science of people in relation to digital threat awareness and response. Thereby, insight is gained on how to decrease the human worker's vulnerability and susceptibility to cyber threats when interacting with technology onsite and offsite the organization. With the Behaviorist Learning Theory, the security posture of an authentic dataset consisting of South African workers in the digital environment was investigated, enabling the observation of stimuli-response behaviors. Appropriate risk management methodologies were applied to identify, classify, assess, and respond to the risks found in the investigated behavior from the dataset. This research project provides security and risk managers with insight into human vulnerabilities and behavior when interacting with technology. This insight emphasizes the importance of human-factor security in an organization's security posture. Additionally, this insight enables the enhancement of an organization's security posture with the emphasis on human-factor security within risk management plans. Through a survey investigation the majority of digital workers, in the exposure to digital threats, show high levels of readiness and awareness by appropriate actions. However, the study and analysis confirm that there is indeed evidence of digital workers who portray risky behavior which can result in devastating consequences regardless of the low probability of occurrence.

Keywords: Digitization, human vulnerability, risk management, information and data security, digital risks, cyber threats

1. Introduction

Cyberthreats aim to exploit the shortcomings within digitized companies. In many cases, the workers can be regarded as one of the weakest links in terms of cybersecurity (Ani et al., 2019). While the advancement of technology allows for more complex and sophisticated systems, various challenges and cyberthreats are introduced. Thus, more people are susceptible to making unintentional mistakes or errors that put the organization at risk. It is far easier to exploit humans than it is to exploit secure information systems or technology. Cyberthreats are magnified when managers of digitized companies overestimate the security of technology, while also neglecting the effects of human error. It is clear that the impact and management of humans are a crucial element in cyber security.

Employees can pose as one of the greatest internal risks to digitized companies. Therefore, the success of digitized organizations and the efficacy of information systems rely greatly on the employees who interact with these systems. The human role in digital risk management is of cardinal importance for organizations to establish a strong security posture.

This research project aims to provide insight into human vulnerabilities and behavior when interacting with information systems and technology in digitized organizations in order to improve risk management. To investigate this vulnerability, data will be collected through surveys provided to employees from digitized companies on the subject of human behavior in information and data security. The Behaviorist Learning Theory will be used in data collection to investigate stimulus-response behaviors when employees interact with information systems or technology. Additionally, risk identification, assessment and management will be applied to the stimuli-response scenarios presented in the survey. Specifically, various threats and vulnerabilities will be identified whereafter risk assessment will be conducted on the various identified threats.

2. Problem statement

The impact and risk that human workers hold in terms of information and data security for an organization is greatly underestimated (Evans et al., n.d.; Nobles, 2018). The focus is placed much more on the risks posed by technologies rather than on the workers implementing, managing or interacting with these technologies. Even the most sophisticated technology can become vulnerable when operated by an incompetent worker. The existing papers focus on the general principles of risk management and how to establish a foundation for effective and successful risk management strategies. None of these papers focus extensively on how risk management is applied to risks presented by human vulnerabilities within digitized companies. Additionally, these frameworks are rarely tested with an authentic dataset. More specifically, none of these studies implement a stimuli-response strategy to determine how people behave when exposed to certain stimuli within their day-to-day, onsite or offsite activities.

An in-depth understanding of the behavioral and cognitive science of people in relation to digital threat awareness and response is needed to gain insight on how to decrease their vulnerability and susceptibility to cyber threats. An in-depth analysis and research of organizational as well as digital risk management strategies and frameworks is needed in order to understand its level of success and effectiveness. From the problem statement, the following research questions arise:

1. Are modern digitized organizations aware of the impact and vulnerability of the workforce related to cyber threats? (RQ1)
2. Do digitized organizations implement risk management strategies that cater for or mitigate potential threats caused by the workforce? (RQ2)
3. Does the average worker possess the level of knowledge, skill and risk awareness to implement adequate security measures in their day-to-day activities within organizations? (RQ3)
4. Is environmental stimuli-behavior investigation effective enough at gaining an understanding of behavior when potentially exposed to cyber/digital threats? (RQ4)

3. Methodology

3.1 Research design

The aim of the research design was to determine the degree of security and digital risk awareness visible among employees working in digitized companies as well as the level of risk and security awareness and readiness from the organization itself. A semi-structured survey was deployed which targeted workers within the modern day digitized (technology driven) organization. Additionally, utilization the Behavioral Learning Theory, the behavior of digital workers when potentially exposed to cyber threats in different environments could be investigated. From this investigation, the various kinds of risks associated with the digital workers' behavior was identified and assessed.

3.2 Survey structure and design

The survey deployed which captured empirical data for a qualitative analysis, was structed into three main sections. The first section (Section A) consisted of multiple-choice questions, mostly in the form of Likert-scales. Section A was structured with questions that relate to four main themes. These themes are formulated as it encompasses a wide variety of factors and influences that are applicable to the modern-day employee where technology is prominent in every aspect of one's life. The first theme asks questions that relate to the participants trust within their organization with regards to the safeguarding of personal information and data. Additionally, this theme includes questions relating to participants experience of the usability of organization information and work device usage rules. The second theme related to password management. This includes password change frequency, reuse and complexity. The third theme related to the protection of personal devices. This included anti-virus usage, update frequency and data backup habits. The fourth theme related to overall technology proficiency and awareness. This included questions that related to participants' normal day to day activities with the usage of technology. Thereby insight could be gained on how aware and cautious participants are of the threats that revolve around everyday usage of technological devices.

The second section (Section B) consisted of open-ended questions with the focus on how the participants respond when exposed to certain stimuli. With this section utilizing the Behavioral Learning Theory, whereby participants provide their personal responses, it imitates an environment where stimuli-response behaviors can be observed. The questions were structured around exposure to stimuli that occur both within the organization

and offsite from the organization. The questions range from how a participant would respond when a virus warning notification appears on their workstation computer, how they would react when experiencing slow internet connection or when they are in need of an internet connection but are at an offsite location. The various responses or reactions to such stimuli exposure could potentially introduce many threats to the organization. For e.g., connecting to an organization's portal with an unsecure connection pose as a common threat as assumably many mobile devices use unsafe connections. When a respondent connects to their company portal with an unsecure connection it creates an exploitable vulnerability.

Similar to Section B, the last section (Section C) also consisted of open-ended questions. The focus of Section C was to investigate personal biases and perceptions relating to participants own posture and abilities in cyber security. Additionally, this section investigated participant's view on the security culture within their organization and what practices they employ to strengthen the over security posture.

3.3 Qualitative study

The goal of the qualitative study was to gain insight and an understanding of the types of threats and risks that arise from the behavior and activities of people who rely on technology in their everyday life. This includes work-related and non-work-related activities. Additionally, this study investigated people's understanding of digital risks and security behavior as well as how they perceive the security culture within their own organization. A QAC-DAS software, "Taguette" was chosen as the tool to conduct the qualitative analysis with, as this software allowed for the grouping and analysis of themes within a set of qualitative data.

The Behavioral Learning Theory was utilized to aid the qualitative study by setting up questions (Survey Section B) that emulate a stimuli-response environment. Thereby, the survey participants' responses when exposed to environmental stimuli, in this case digital threats, could be analyzed. Thereby, insight could be gained into the triggers and causes of certain behaviors. The Behavioral Learning Theory was deemed an appropriate method to be utilized in the survey as this theory states that all behavior can be learned and observed through conditional exposure in a certain environment (Western Governers University, 2020). Survey section B was thus developed, mimicking an investigation of participants' behavior when exposed to threats in certain conditions.

3.4 Participants and procedure

For the target audience of the survey and the qualitative study, any person who forms part of the working class in South Africa who works in the IT industry or related field are applicable. This includes any person who considers themselves heavily dependent on technology in order to do their day-to-day working activities. In terms of participant demographics, there is no specific age requirement, but the participant must be part of the labor market. This assumes that all participants will be older than the age of 18. In total, 58 responses were gathered from the survey. Participants were still prompted to provide their age in order to identify whether there exist various levels of threat and risk awareness, perception and behavior among different age groups. Participants' gender was prompted in order to identify and quantify any potential differences in awareness and behavior among gender groups. The age and gender distribution can be seen in Figure 1.

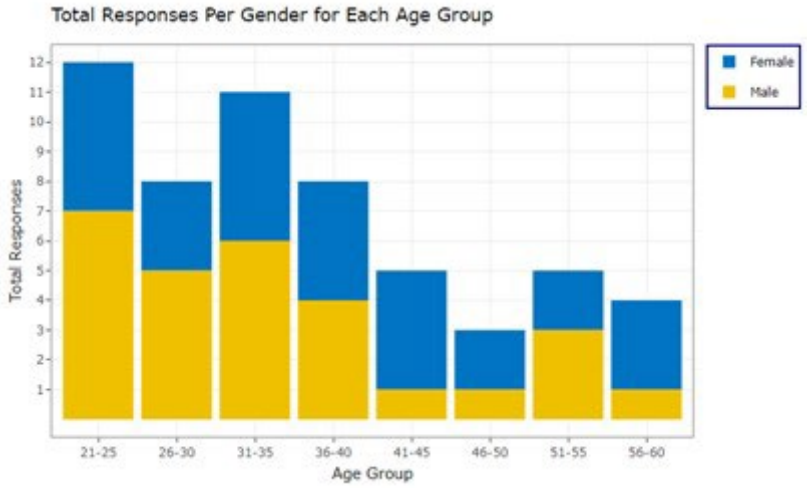

Figure 1: Total responses per age group per gender

Lastly, participants were prompted to specify their current job/role in the labor market. Through the specification of different job roles and titles, there was aimed to determine the general level of threat awareness and ability between different IT or related industries. These general demographic variables serve to identify trends in behavior and patterns among diverse groups in the dataset. It was expected that there is no significant difference among gender groupings. It was assumed that no specific variation in the behavior of gender groups will exist.

3.5 Data collection

Before any participation in the survey is made possible, participants were prompted to provide acknowledgement of the purpose and goal of the survey as well as indicate their consent to participate. For those who do not indicate acknowledgement and consent, the electronic survey was physically unable to start with the questions, ensuring that ethical requirements are met.

The survey was designed, created and managed directly from Google Forms. All data collected from the surveys was stored and secured on Google Forms and exported for analysis. A target with a minimum of 50 respondents was set in order to ensure diversity and accuracy in results as well as increasing the scope of unique answers. The survey was distributed through word of mouth as well as through an invitation message on LinkedIn.

4. Results and analysis

The purpose of the survey study was to investigate the overall level of security awareness and response to threats that are present and that any worker may encounter within the digitized environment. Through the deployment of the survey, it allowed to the capture of responses through the investigation on an actual dataset. Additional emphasis was placed on the actual observable behavior from employees when exposed to certain stimuli. In this case, the stimuli refer to the exposure to any form of security threat. The information found from the investigation aided in gaining a perception of the overall security posture that are already present within the digital workforce. Additionally, the investigation aids in gaining a perception what the type of potential risky behavior are and how to prevent or remediate the threat that may arise from such behavior. From the results of the analysis, the research questions could thus be answered.

As previously discussed, the survey study consisted of three separate sections, all which contribute to the overall understanding of the security posture of the sample. With regards to the gender distribution across the various questions for section A, there is no specific trend indicating a significant variation between Male and Female respondents. This confirms the pre-assumption that there would be no significant variation between gender groups. Within the analysis of survey Section A, it was found that the majority of respondents answers show that there indeed exist security and risk awareness through their interaction and usage of technological devices. This is visible from answers to questions across all four subsections. As can be seen in figure 2 and 3, the majority of participants do back-up their data at some time and the majority are confident that their interaction with technology is in a safe manner.

Figure 2: Data backup regularity per gender group

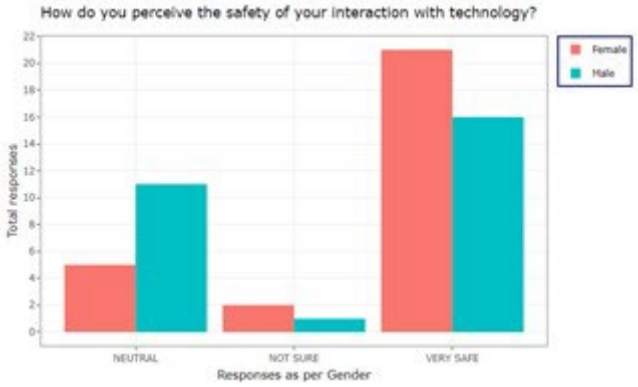

Figure 3: Gender group perception of technology safety usage

However, it is evident that many respondents (the minority) show actions that tend to be less secure or favorable such as with regards to password management. It was found that 11 respondents (19,6%) never update their account passwords. Additionally, it was found that 9 respondents (16,1%) create accounts with easy rememberable passwords, while 31 (56,4%) use repeatable passwords for various accounts as seen in figure 4.

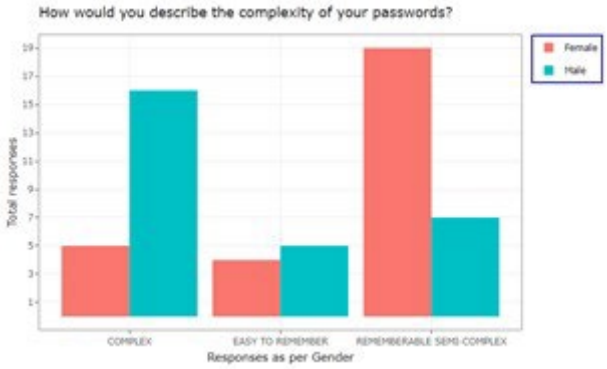

Figure 4: Password complexity per gender group

With regards to device and data security, just below half of respondents do not use anti-virus software on all their devices and four respondents never back-up any of their data as seen in figure 5.

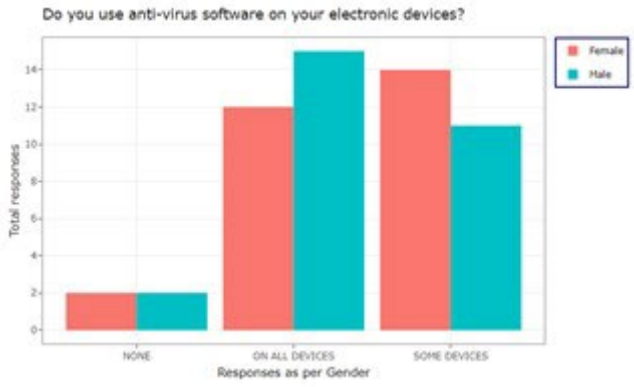

Figure 5: Anti-virus usage

Additionally, 14 Respondents either do not know how to take security precautions or do not feel the need to take precautions when working with technology. 24 Respondents do make use of their work-related Email accounts for personal matters. Additionally, there exist a high admittance to accidentally sending an Email to the wrong recipient (30 respondents). Related results are found for the usage of work-related devices for personal purposes. A high unattendance rate of work-related devices in the workplace was found (34 respondents). This number of respondents contradicts the amount (14) who do not take precautions when working with technology, as leaving a device unattended could be regarded as unsafe. This behavior is influenced

by the level of trust an employee has in the safety of the organization's working environment. Lastly, with regards to EFT purchases, over half of respondents make EFT purchases directly from a third-party website, which was found to be extremely risky (Business Insider SA, 2020). Although for some questions the amount of risky behavior from answers seems to be high, across the entire section, this in general is the minority.

The aim of section survey section B was to identify risks that arise from respondents' behavior when exposed to certain potential threats, which represents exposure to stimuli. Both the response to the exposure to stimuli within the organization as well as offsite from the organization was investigated to broaden the scope of exposure to threats. Within the analysis of this survey section, it is immediately evident that most respondents already portray a strong sense and awareness of security threats and how to react accordingly. This is visible in both subsections of the survey. With regards to stimuli exposure within the organization (Survey Section B1), it appears that when respondents are situated physically within the organization, the evidence of risky behavior decreases significantly. This may because of respondents being more cautious and aware when they are at work from potentially being under surveillance. Additionally, although not investigated, a physical organizational environment may stimulate focus that could improve caution and awareness as opposed to being offsite where the influence of distraction is present. The higher secure behavior could also be because of infrastructure provided by the organization for onsite use, such as internet connectivity and electronic devices. It was not evident in any respondents' answer that they were allowed to make use of their own data connection for onsite work-related purposes. However, when respondents are situated at an offsite location (Section B2) and in need of a data connection, thereby creating the need for self-provided data, risky behavior starts to occur. It was found that many respondents will make use of self-provided data or public Wi-Fi networks to carry out work related activities, without the mentioning or consideration of the risks associated with such actions. Most respondents will acknowledge the importance and need of secure connections and thus in many cases state the usage of VPNs to secure the connection. An interesting finding only noticed in single respondents was the belief that a certain threat has never or will not occur to them and as such they do not provide a response or answer.

As most respondents show an intense sense of awareness and caution, the identified risks only pose a threat by how easily an employee can be deceived/defrauded for their access authority. The more an employee has access to a certain level of data or information system, the higher the loss or damage can occur from the infiltration or exposure of the data or information system. Thereby, access and authority are identified as a particularly crucial factor for the security of information and data.

In order to assess and classify the risks that were identified in Survey Section B, a risk assessment formula was derived from many existing studies who utilize a standard formula within their risk assessment investigation (Kure et al., 2018; GOVERNANCE & STANDARDS DIVISION, 2017; NRECA, 2011; Ao et al., 2008). The risk formula derived and utilized are as follows:
RISK = LIKELIHOOD * IMPACT

The likelihood of a threat was determined by three underlying factors: the capability of the threat, the nature of the threat and the effectiveness of current controls in place to prevent an attack. Impact severity of a threat was classified on a scale of one to five, ranging from low to high, as described by GOVERNANCE & STANDARDS DIVISION (2017). The potential worst outcome from a breach that results from all identified risks can lead to very high fiscal damages and repercussions for any organization. As a result, an impact score of 5 was assigned to all identified threats from the results of the survey. After applying the risk assessment formulas to all scenarios presented in Survey Section B, all the identified risks had a probability of occurrence percentage lower than 15%. In combination with the impact assessment of the worst possible outcome for the organization, that is the infiltration of malware, all risks can be classified with a total score of 5. The number is calculated from the multiplication of the impact score of 5 with a probability score of one. Utilizing GOVERNANCE & STANDARDS DIVISION (2017)' s risk assessment matrix (Figure 6), all risks could be regarded as extremely low. However, due to the high impact and consequences of a breach, all potential risks show be avoided where possible.

		Impact				
		1	2	3	4	5
Likelihood	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Figure 6: Risk Impact Matrix (GOVERNANCE & STANDARDS DIVISION, 2017)

Due to the significant fiscal impact that malware can have on organizations, with R3 871 010.33 (+- $ 261673.57) being the total recovery cost for South African organizations respectively (Sophos, 2020), even the slightest human error should be prevented. It is thus clear that organizations should consider every potential action that an employee may take that could cause a security breach, regardless of the low probability of occurrence.

It was found through an investigation and research in a study that South African digital workers portray a high security posture (Mcanyana et al., 2020). Additionally, this research suggests that South Africa is in the top 5 global countries at preventing data encryption from malware (Mcanyana et al., 2020). In contrast to the beforementioned research, Sophos (2020) proves South Africa's defense capabilities otherwise. Sophos (2020) states that cybersecurity in South Africa is not on par or as robust as other global countries. Additionally, Sophos (2020) continues that as a result of South Africa's substandard security posture, various threat actors consider South Africa as a malware testing ground. These actors test tools and techniques on South Africa, before attempting the deployment on more sophisticated countries (Sophos, 2020).

The aim of survey Section C was to investigate respondents' personal perceptions of digital risks, the importance of information and data security, as well as their view on the security culture within their respective organizations. This qualitative analysis, in addition to the analysis of Section A provided more context for the formulation of the general perception of the security posture already portrayed by the respondents and their respective organizations. From the analysis of this section, similar insights are gained regarding the overall level of security and awareness among the respondents and digitized organizations. The majority of respondent's show a good understanding of the term "digital risks" as well as of the importance of data and information security in modern organizations. Only two respondents out of 58 did not show interest in the importance of the topic. Most respondents who acknowledged the importance of the topic provided motivations that ranged between the repercussion from the lack of ample security, or the value gained from protection of sensitive information. With regards to the understanding of the term digital risks, the majority correctly associated digital risks to those introduced by conducting business in the digital environment, data being digitally used and stored, the usage of technology or any form of cybercrime. Only 7 respondents show unawareness of the term. The remainder of questions in this section focused on respondents' perspective of their organizations, with the aim to gain insight on the security culture, requirements and expectation within the workplace. It was found that 15 respondents do not receive adequate security training or education from their organizations. This raises a concern as assumed that training and education should form an integral part of any risk management plan. This high number of respondents who do not receive adequate security training could contribute to explaining why there is risky behavior found by several respondents' answers throughout the entire survey. With regards to perceived organizational security culture, it was found that the majority of respondents work in organizations that have a strict view on information and data security. Only in single cases did respondents mention a relaxed security environment.

From those respondents who indicated a relaxed security environment, one respondent stated that the security measures taken in the organization differ from person to person. This finding aids in the confirmation that although an organization may portray a strong security culture, the acts of one person can jeopardize or put the entire posture at risk. To investigate security culture in more depth, questions were asked regarding the required response to breach detection, what additional security measures are used to secure accounts, information system access and security, support group availability and accessibility within the organization. It was found that all the beforementioned organizational factors contribute positively to the general security posture of digitized

organizations. Additionally, it was found that regardless of the respondents' level of experienced stress in the workplace, stress does not appear as a determining factor of technology proficiency.

Overall and in general, adequate and responsive support groups are evident within organizations. Additionally, organizations do require employees to make use of multiple layers of security for the safeguarding of accounts. Additionally, they require employees to make timely escalations of security breaches and equip employees to safely establish networks connections. This is mostly done with the use of VPN's. This general conclusion is made through the consideration that the majority of all responses are positive in nature and promotes behavior that contributes to the strengthening of the security posture of respondents as well as their respective organizations. Although not explicitly stated, sufficient evidence exist that allows the assumption that organizations do implement risk management strategies. This assumption is made from the majority of respondents' answers that indicate strict security policies and requirements from their organizations. As a result, Q2 can thus be answered. It is also clear that organizations are aware of the impact and vulnerability of the workforce. This is seen through evidence captured by respondents that organizations do employ adequate measures to strengthen and prepare the workforce. Thereby, RQ1 is answered. The combined results from survey section A and B in conjunction with questions on security in Section C, the majority of respondents show high existing levels of security and threat awareness. RQ3 can thus be answered.

In conclusion of the analysis, it is clear that there exist a strong security culture within organizations and the reflection of such a security culture is visible within its employees. However, regardless of the level of security protocols in place within the organization, there will always be an employee who indulge in risky behavior. This can either be intentionally or unintentionally. Additionally, it is clear that observable environmental stimuli-response behavior is not adequate enough at forming an understanding of human behavior, thus answering RQ4. As such, proving the Behavioral Learning Theory to be less effective as proposed by Western Governers University (2020). The effectiveness of the Social Learning Theory to aid in the understanding of human behavior can thus now be brought into question.

5. Conclusion

It is clear that the understanding of human vulnerability and susceptibility to cyber threats are much deeper than an observable investigation. Human behavior is determined by a combination of both the understanding of personal psychological influences and the exposure to environmental stimuli, thus answering RQ4. The insight gained from this understanding provides great benefit to every aspect of an organization's security culture. Additionally, the human employee is at the forefront every facet of cyber security. It is crucial that organizations take every necessary step in order to prepare and promote security and risk awareness among the workforce. This trait is already visible within the workforce as the majority of respondents from an authentic dataset portray mindfulness towards cyber threats, thereby answering RQ3. With the rapid improvement and sophistication of modern cyber-attacks, it is impossible for organizations to completely prevent every attack. As attacks and breaches are inevitable, organizations should expect the worst and react accordingly, as it only takes one minor human mistake or error that leads to an organization's downfall. A strong sense of organizational awareness of the risk an impact of human vulnerability to cyber threats is visible. Organizations do in fact implement risk management strategies to prepare and improve the security posture of the workforce, thus answering RQ1 and RQ2. From the results there can be concluded that the impact of human vulnerability to cyber security is a risk that should not be overlooked or underestimated. The results from this paper emphasizes the importance of human-factor security in risk management and should receive priority of focus over the impact of technology itself.

6. Recommendation for future research

This study's investigation focuses solely on security awareness and behavior in relation to organizational information and data security. However, human behavior as a single factor is only one of many factors that defines the overall security posture of an organization. An organization's security posture and readiness to cyber threats cannot be derived only from the overall posture of the workforce. Due to the inevitability of a cyber-attack, the organization's ability to recover from such an attack holds significant weight. Sophos (2020) highlights that cybersecurity insurance aids in the recoverability of an organization after a ransomware attack. It was found that from all companies worldwide that had data encrypted from a ransomware attack, 94% of cases were the ransom was paid the cost was covered by insurance (Sophos, 2020). Additionally, Balbix (2021) highlights five factors that define an organization's security posture. These factors include existing protection controls and

processes, attack detection and containment, attack recoverability, the level of automation in the organization's security program and level of visibility in the organization's asset inventory. It is visible that the human employee has a role in each of these factors and needs to be investigated in order to determine an organization's security posture. It is thereby proposed that human behavior should be investigated in deeper detail that considers the human worker's role in the above-mentioned factors.

It is assumed that respondent's answers are subjective to their own perceptions of their security posture as well as their respective organization's posture. There exists the possibility that subjectivity in the answers could misrepresent reality. Thereby the question arises whether respondents' perception of their personal and their organizations security posture align with how security officials from the organization perceive it. It is thus proposed that in order to fully determine the security posture of an organization, additional investigation is needed with the focus on security officials in order to determine alignment of perceptions and expectations between organization and employee. The utilization of interviews as data collection methodology would allow the draw of more meaningful insight and improve the quality of data collection. This would prevent the collection of meaningless answers as seen with the usage of anonymous surveys. As it was concluded that The Behaviorist Learning Theory does not provide adequate support for the understanding of human behavior, further investigation with the use of The Social Learning Theory could be utilized to broaden this understanding.

References

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028

Ao, S. I., International Association of Engineers, WCECS (2008.10.22-24 San Francisco), & World Congress on Engineering and Computer Science (2008.10.22-24 San Francisco). (2008). *WCECS 2008, World Congress on Engineering and Computer Science, San Francisco, USA, 22-24 October, 2008*. IAENG International Association of Engineers.

Balbix. (2021). *What is Security Posture?* https://www.balbix.com/insights/what-is-cyber-security-posture/

Business Insider SA. (2020). *Beware of 'instant EFT' when buying online, regulators warn – you risk a great deal*. https://www.businessinsider.co.za/reserve-bank-fsca-warns-against-instant-eft-for-online-shopping-2020-11

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (n.d.). *Human Behaviour as an aspect of Cyber Security Assurance*.

GOVERNANCE & STANDARDS DIVISION. (2017). *IT Risk Management Framework DOCUMENT REVISION HISTORY*.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences (Switzerland)*, *8*(6). https://doi.org/10.3390/app8060898

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *INSIGHT INTO THE CYBERTHREAT LANDSCAPE IN SOUTH AFRICA*.

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

NRECA. (2011). *NRECA / Cooperative Research Network Smart Grid Demonstration Project Guide to Developing a Cyber Security and Risk Mitigation Plan*.

Sophos. (2020). *THE STATE OF RANSOMWARE 2020*.

Western Governers University. (2020). *What is the behavioral learning theory?* https://www.plutora.com/blog/digital-risk