Risk Likelihood of Planned and Unplanned Cyber-Attacks in Small Business Sectors: A Cybersecurity Concern

Tabisa Ncubukezi
Information Technology Department, Faculty of Informatics and Design, Cape Peninsula University of Technology, Cape Town, South Africa

Ncubukezit@cput.ac.za

Abstract: Human factors such as planned and unplanned cyber-attacks are a serious threat to any institution. The presence of planned and unplanned actions exposes the state of cybersecurity within the small business sector – leaving them vulnerable to a range of cyber-risks. This study used AgenaRisk package with Bayesian Network (BN) tools to illustrate the likelihood of risk in planned and unplanned attacks. Adopting the package demonstrates the dependent and independent variables of the human factors, which are planned and unplanned, with their relationships resulting in the ultimate data breach. The work also combined qualitative research with quantitative risk analysis techniques to determine the risk likelihood of the planned activities and unplanned employee actions and their behaviors influencing data breaches. The work used the judgemental sampling method to select twenty-five (25) research participants who are business owners, and Information Technology (IT) managers. An online survey was used to collect data from the selected research participants. Results were analysed using content analysis, and interpreted using the package with BN tools, and risk analysis techniques. The results were further discussed, and the study concluded with the remarks and future developments.

Keywords: AgenaRisk package, Bayesian Network tools, cyber-risks, cybersecurity, planned cyber-attacks, unplanned cyber-attacks, risk analysis techniques, risk likelihood

1. Introduction

The global transition due to the Covid-19 pandemic forced all institutions, including the small business sectors, to rely on Information and Communication Technology (ICT) for performing their daily activities and delivering services (Ncubukezi, Mwansa & Rocaries, 2020b). Every business sector is faced with increased risks which can be related to economic, technological, network, device, and human factors. The operators behind the increased use of technology are people who form part of the Information System (IS). People present employees and criminals who strive to gain access and work on systems (Japertas & Baksys, 2018). However, their interest in the high usage of ICT resources exposes businesses to ultimate planned or unplanned data breaches. People, as human factors, can generate cyber-risks which are two-fold: risks generated by criminals and risks caused by the employees as insiders (Ncubukezi, 2022a). The criminals exert their energies to exploit vulnerable and weak systems by gaining unauthorized access. Various reasons trigger this action. The employees as insiders also become agents of unplanned attacks, leaving room for intruding unauthorized access. Even though unplanned attacks can be caused by both insiders and criminals, the paper focuses on attacks caused by insiders.

The risks committed by the criminals are thoroughly planned, and internal risks triggered by employees or staff are unplanned. However, regardless of the source of the risks, businesses continue to be vulnerable to all kinds of cyber threats and cyber-attacks. As a result, businesses that do not have a strong cybersecurity plan in place and perform proper risk analysis for effective decision-making (Wang & Neil, 2021) become victims of the common attacks.

1.1 Research aim and objectives

This study demonstrates the risk likelihood of planned and unplanned cyber-attacks caused by human factors using the AgenaRisk package and the risk assessment techniques. To achieve this, the study:

- Identifies the causes of the planned and unplanned cyber-attacks;
- Determines the risk likelihood of the planned and unplanned attacks using quantitative risk analysis such as sensitivity analysis, scenario analysis, and decision tree analysis; and
- Demonstrates observations of the planned and unplanned cyber-attacks resulting in the risk likelihood.

The paper covers related literature about planned and unplanned cyber-attacks and threats, BN tools, related studies followed by the method of inquiry used, results, discussion, significance, and conclusion.

2. Background to the study

Regardless of the size of the business, all organisations suffer and are exposed to a range of planned and unplanned cyber-attacks (Khosravi & Ladani, 2020). The sudden Covid-19 pandemic caught institutions off guard, which resulted in a huge transition of operating from homes. That adjustment introduced remote access to the

system. The change from office to home forced employees to be independent and operate at the same homes, regardless of their level of computer skills (Khan, Brohi, Zaman, 2020). To some institutions, the change became easy due to their preparedness and readiness to use technology. The Covid-19 pandemic also became an opportunity for cybercriminals to hit all institutions and has had a negative impact on the global economy (Wijayanto & Prabowo, 2020). Even though the computer and network as the ICT were present, the issue of planned and unplanned cyber-attacks remain unclear. Planned attacks are initiated by intentional criminals that are after the lucrative benefit of any size and kind of business institution (Hakak, et al., 2020). On the contrary, unplanned attacks are unsafe and ignorant actions performed on the system by legitimate employees. All the negative and unsafe actions performed may expose the system to various negative risks.

2.1 Risks among small businesses

Risks always exist in every organisation or institution, and they are inevitable. The global Covid-19 pandemic also increased the risk likelihood in all businesses and institutions. Likewise, during the lockdown, people panicked and developed anxiety and stress. Some had to adjust from working in their comfortable office spaces to working at home. The current study focuses on the small and medium businesses described below. **Figure 1** illustrates human interaction in a networked business system with promoters of unsafe and unsecured connections. People who are legitimate employees and criminals use any type of end device to connect to the business system. With a secured connection, planned attacks are not likely to happen. The promoters of unsecured connections result in an ultimate data breach in the form of modification of information, deletion of information, and information loss. The planned or unplanned attacks that happen on the business system compromise the state of confidentiality, integrity, and availability of information (Ncubukezi, 2022b).

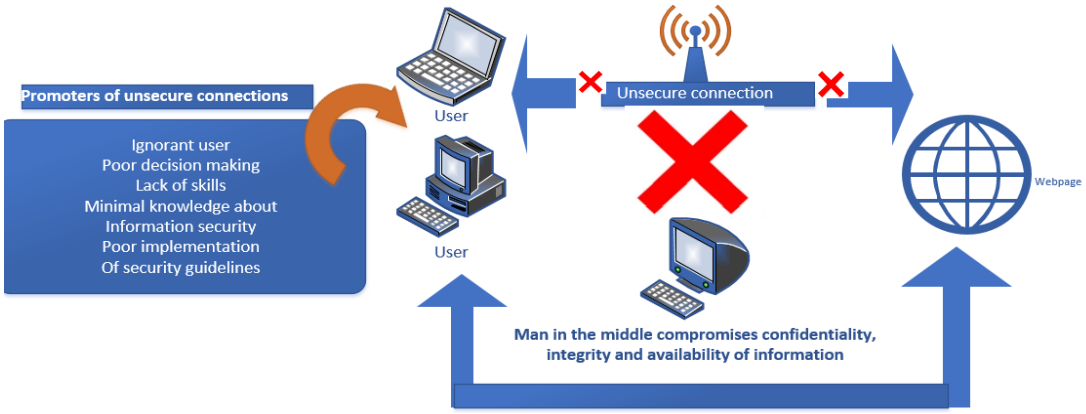

Figure 1: Promoters of the attacks in a business system (Source: Ncubukezi and Mwansa, 2021)

The attacks affect different resources of the businesses. Therefore, with the increased use of ICT among different sectors, it becomes essential to adopt and use artificial intelligence (AI), which imitates human actions and intelligence using applications and algorithms built in a computing environment (Ncubukezi, Mwansa, & Rocaries, 2020a; Fenton & Neil, 2014). These capabilities include planning, learning from experiences, and creating and adjusting input variables. This study adopted the BN, which is discussed below.

2.2 Why Bayesian Network

The study adopted the BN as the graphical model that illustrates the likelihood of the risks relating to planned and unplanned attacks. The probabilistic model denotes data about uncertain nodes holding the random variable and demonstrating conditional probability for any corresponding variable (Yang, 2019; Chen & Wang, 2017). The BN predicts the probability of risks that results from data breaches. The BN is demonstrated through the use of the AgenaRisk package, which created the interfaces (AgenaRisk, 2021). The package demonstrates, analyses, and predicts planned and unplanned risk likelihood caused by human factors. BN through the package was used to predict the risk likelihood based on the activities performed by legal or illegal users. The current scenario shows the relative probabilities of the risks, illustrating relationships between dependent and independent variables and their influence on the level of the risk likelihood (Khodakarami, Fenton & Neil, 2007).

The BN technique determines the risk likelihood based on the prior indicators, protection levels, risk likelihood, and the consequences of the risks (Fenton et al., 2007). Figure 2 shows a package that has been used to illustrate the risk likelihood of human factors such as planned and unplanned attacks. The application of the package has been demonstrated in section 4 of the study. The package interface was used to generate different scenario cases of planned and unplanned attacks.

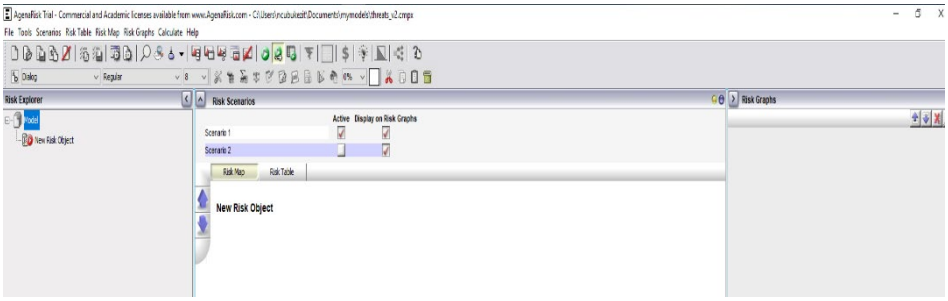

Figure 2: AgenaRisk interface

3. Method

The study collected data from the business owners and IT managers of small businesses from diverse sectors in the Eastern Cape from their natural settings, which shares the participant's activities and their actions toward their system. A total of twenty-five (25) respondents participated in the study and were selected using judgmental sampling. All the sectors that participated use the online business system to perform their daily operations, keep businesses running, and as well as increase revenues.

Data were collected using online surveys with open-ended questions. Participants were sent emails with the survey link. Collected data were categorized, analyzed, and interpreted using content analysis. The collected data was used to form the knowledge base for the development and illustration of the Bayesian Network model using the AgenaRisk technique. The agenaRisk technique is the graphical package that illustrates and determines the risk likelihood. In this study, the package determines the risk likelihood of the criminal's and employees' activities, which exposes the business to risks. Data was further interpreted using the BN through the AgenaRisk package to determine the risk likelihood of planned and unplanned cyber-attacks. The BN tool is used to support the model analysis using different analytical techniques such as sensitivity analysis, Tornado graphs.

In addition, the study used quantitative risk analysis techniques including scenario and decision tree analysis for further demonstration of the planned and unplanned attacks. Each analysis technique illustrates the uncertainty of the attacks.

The university's ethical processes, which approve research studies were complied with.

4. Results

4.1 Collected results

Data were collected from the relevant respondents who use the business systems to run their daily activities in cyberspace. Employees of the small businesses that took part in this study have a range of one to 150 per business sector and also generate a turnover of up to R1 million per year. Table 1 shows the respondent's background.

Table 1: Respondents background

Participant position	Number	Gender	Sectors	Age range
Business manager	7	Male	ICT, home improvement, retail, real estate, transport,	35-50
Business manager	5	Female		37-45
IT manager	7	Female		33-43
IT manager	6	Male		31-46

As shown on Figure 3 the selected businesses have been in existence for less than a decade. Most businesses have been operating for a year to two years, while 25% haves been operating between three to five years and 20% have been operating between six to nine years.

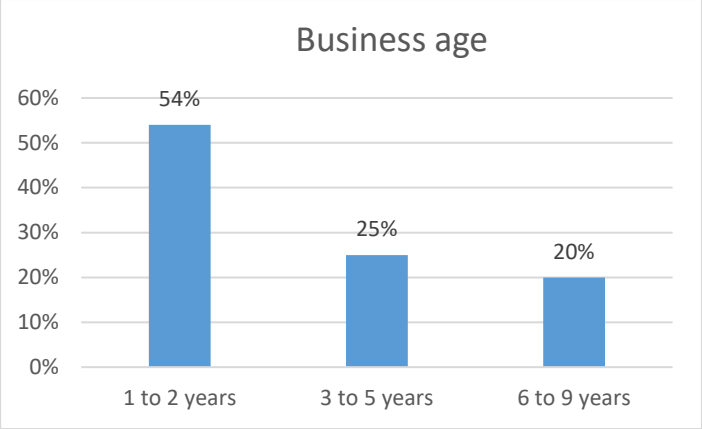

Figure 3: Business age

Figure 4 shows the causes of the planned and unplanned cyber-attacks experienced by the small business sector, due to different motivating human factors. These attacks are rated on a Likert scale from rare (1), unlikely to happen (2), moderate to happen (3), likely to happen (4), and certainly to happen (5). The respondents shared their insights about the main causes of unplanned and planned cyber-attacks.

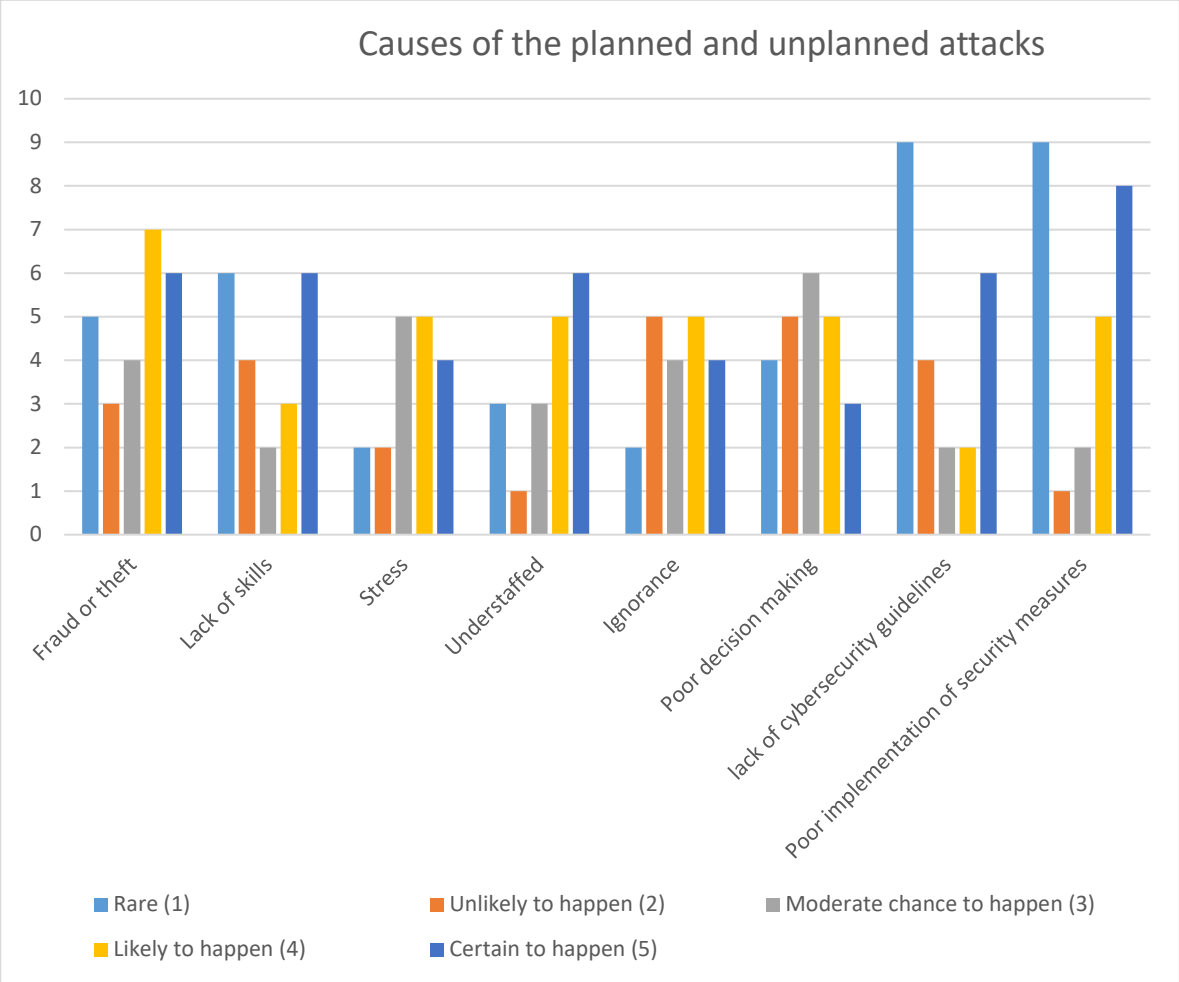

Figure 4: Planned and unplanned cyber-attacks

Results also showed different interpretations of the protection level of the businesses. Some businesses indicated that they only rely on the anti-virus as the protection measure while 100% believe in both passwords and anti-viruses.

4.2 Simulated scenario analysis

Simulated scenarios are an investigation of a particular phenomenon within its real-life context using different sources of evidence (Robson, 1993). Scenario analysis helps to separate and identify the main trends (certainties or uncertainties) by looking at the trends that may not or may be significant or may not change. The action avoids frustration and improves efficiency while saving time. The main focus is on the events involving attackers and cyber criminals, and employees demonstrating their influence on the system.

A simulated scenario of human factors was developed with two system users: a normal user and an experienced IT user. The normal user presents as an employee who is not well trained and informed to use the system, while an IT user is skilled and well-orientated towards cybersecurity best practices. In this scenario, both users can experience planned or unplanned attacks based on their actions, attitudes, and behaviours on the system. A planned attack presents a criminal looking for opportunities to gain unauthorised access to unsecured systems.

So the package predicts the risk likelihood based on different scenarios influenced by user activities and the state of security (system's protection level). The risk probability influences the risk impact. This scenario is presented owing to the high demand for Internet use and working off-site during the global pandemic, where data became the leading lucrative benefit in all organisations. Criminals always have the intention of gaining unauthorised access, while employees can commit unplanned actions which ultimately compromise the safety and security of the system. The following section demonstrates the prediction of the risk likelihood based on the different scenarios of the planned and unplanned attacks experienced by employees. An employee could be a normal system user or skilled Information Technology (IT) user who interacts with the system

4.2.1 Scenario analysis setting

These simulated scenarios are based on small businesses from diverse sectors that are mainly using technology to render services to clients. The work evaluates the cause of risk, the likelihood of the risk occurring, and its impact. This scenario describes, explores, and explains various elements that result in risks that ultimately compromise information security. They demonstrate the relationships between dependent and independent elements, the likelihood of risk, protective measures are taken, and the consequence of the risk. Scenario analysis pays more attention to the effect of risk in a certain situation. This analytical method uses specific information for certain scenarios to change the model's variables. Nodes used in the study are either ranked High, Medium, and Low. Some have the Boolean values of Yes or No and True or False. All these nodes have values that predict the likelihood of the risk and its impact.

4.2.1 Illustration of the risk likelihood on AgenaRisk

Figure 5 shows a scenario of an IT user interacting with the system. This employee experiences both planned and unplanned attacks. The planned attack could be caused by the level of employee ignorance, poor decision-making, or working under pressure. As illustrated, the planned attack has a Boolean of True and False where the prediction is 100% present. The same user also experiences an unplanned attack that could be coming from the criminals and has a Boolean of 50% False and 50% True. This means that there is a threat detected on the system which could compromise the state of security. So the risk likelihood is determined by the source of the attack and the protection level of the system ranked as High, Medium, and Low. The protection level has 50% dominating as high protection. The probability of risk is then predicted as 93.75% risk likelihood on a ranked node with High, Medium, and Low. The risk impact is then predicted as 51% high on a ranked node.

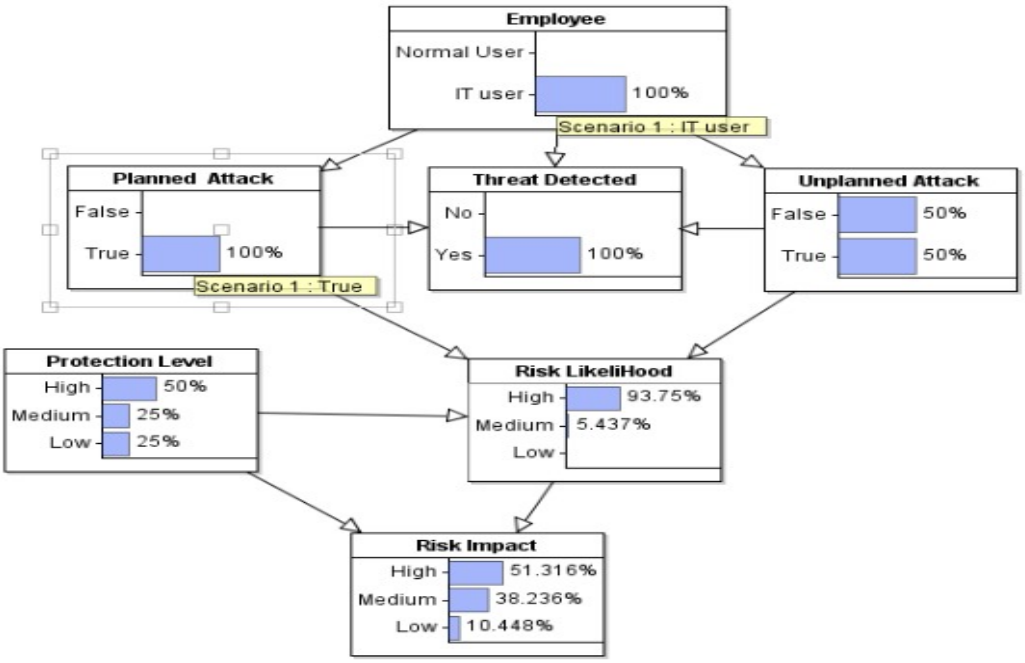

Figure 5: IT user experiences a partially unplanned and planned attack at a low protection level

Figure 6 shows an IT user with a detected threat level of 100% who experienced both 100% planned and 100% unplanned attacks. The level of attack and the partial level of protection of 50% in this scenario results in a 98% of risk likelihood. The risk likelihood and the protection level directly affect the risk impact.

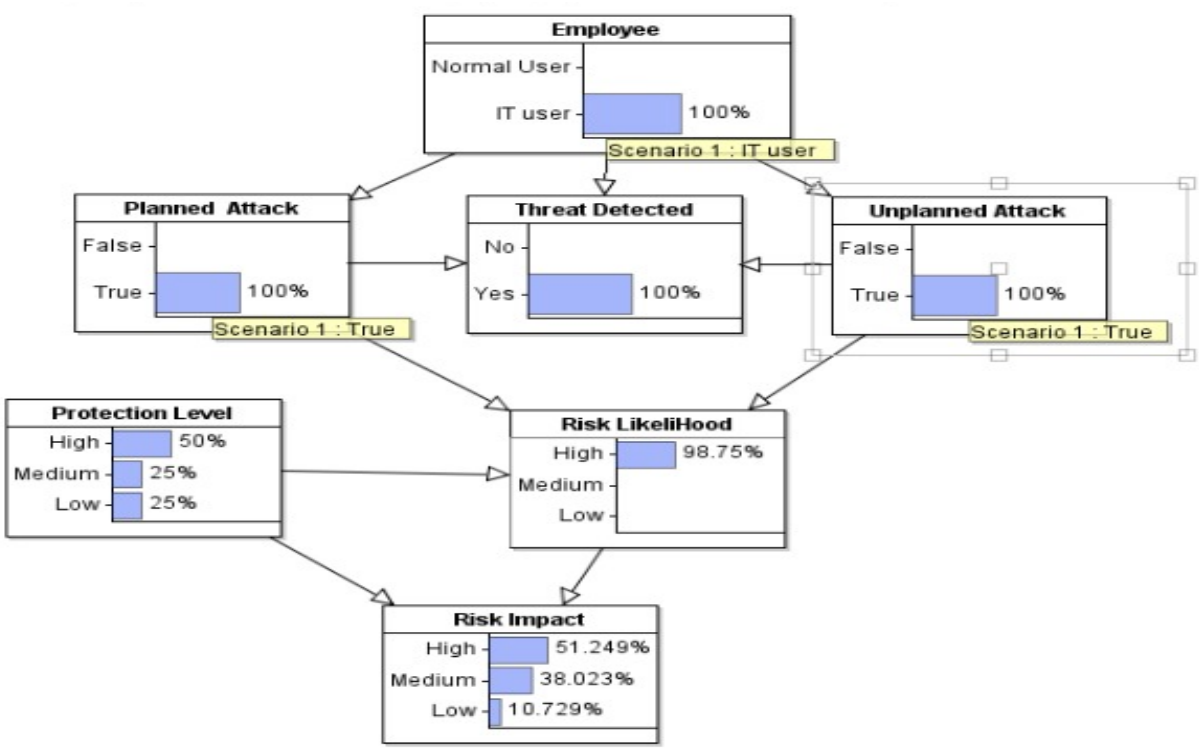

Figure 6: IT user experiences both planned and unplanned attack at the partial protection level

Figure 7 shows a normal user who experienced a 100% unplanned attack with a 100% planned attack with a 100% threat detected. These attacks happened at the 50% protection level, resulting in 98% risk likelihood and 51% risk impact.

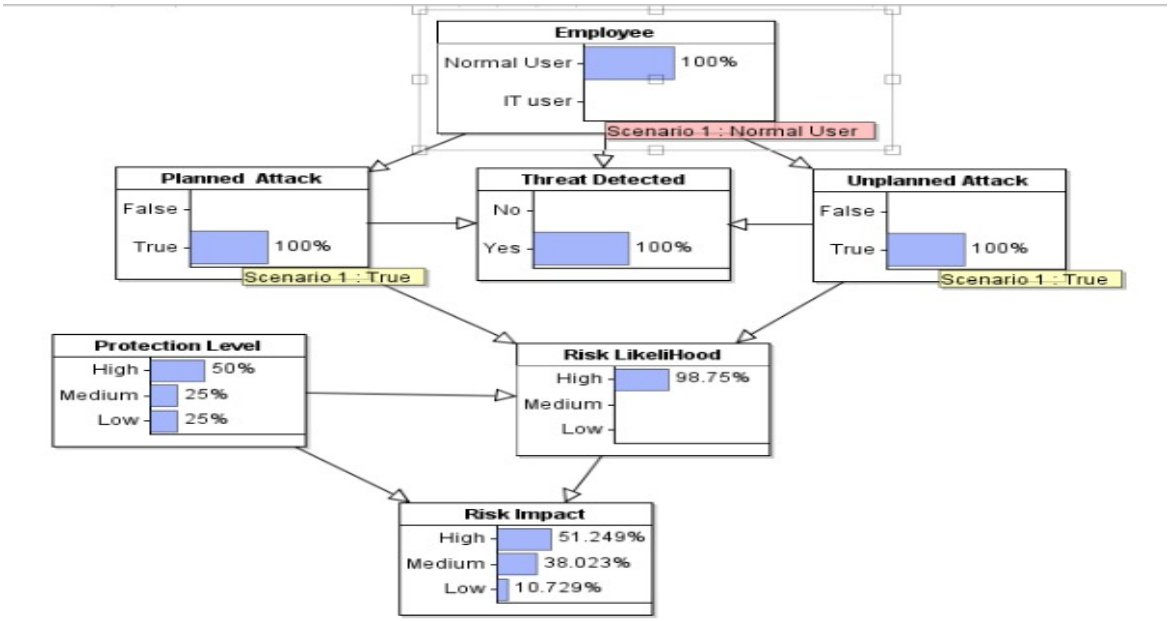

Figure 7: Normal user with 100% planned and unplanned attacks at a 50% protection level

Figure 8 shows a normal user with 68% planned and 65% unplanned attacks which means the threat is detected. The scenario shows a 100% low protection level, resulting in 96% of high-risk likelihood and 69% of high-risk impact.

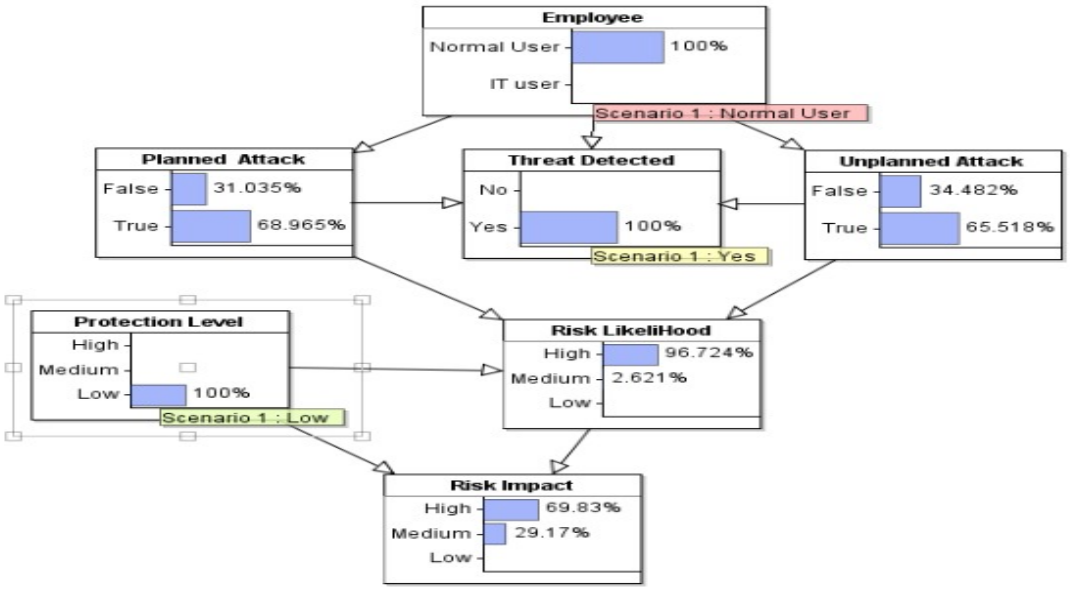

Figure 8: Normal users experience partial attacks at a low protection level

Figure 9 shows a normal user with 100% threat detected in 68% of the planned attack and 65% of the unplanned attack at 100% high protected level, resulting in 87% of the risk likelihood and 40% of the medium and high-risk impact.

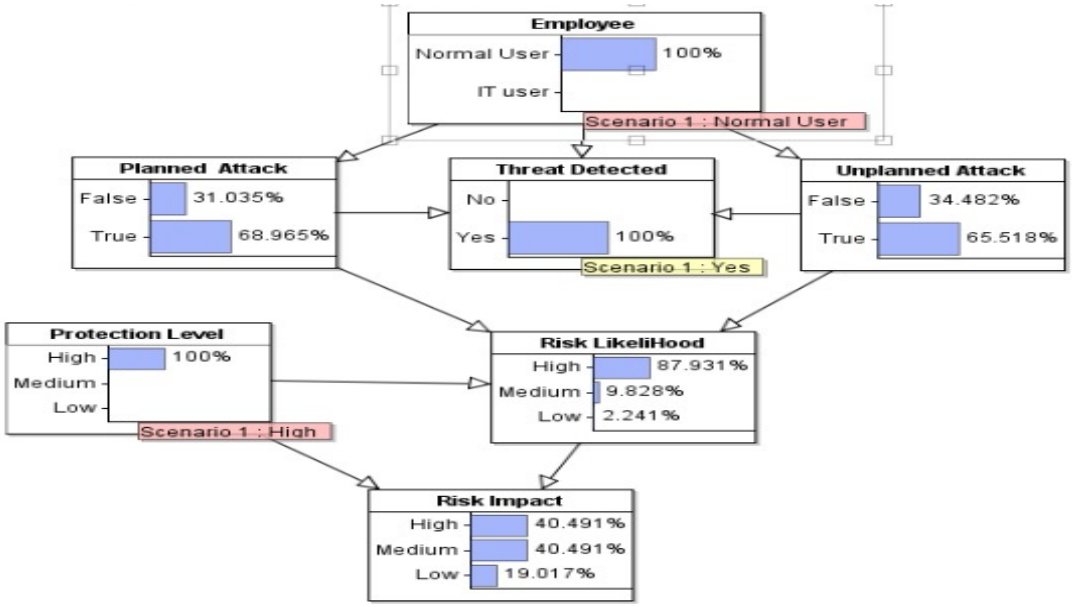

Figure 9: Combination of planned and unplanned attacks on normal user

The scenarios above illustrate both computer-literate and illiterate users who interact with the system. In all the scenarios, the user has a threat detected which could likely compromise the state of the business system safety. Even though there are all these scenarios, there is some level of security, the system remains vulnerable to both the criminals and the insiders who are legitimate employees. The absence of a dedicated cybersecurity manager could result in poor implementation of security measures (Ncubukezi, Mwansa & Rocaries, 2020b). Ignorance of internal employees caused by their level of awareness, and poor decision-making can directly contribute to the compromised business system (Ncubukezi, 2022a). The presence of both planned and unplanned attacks is caused by actions as a result of the human factors which criminals always look for an opportunity to benefit from.

4.3 Sensitivity Analysis

BN tools with the package simulated the potential cybersecurity risk probabilities and their impacts in the business space. The sensitivity analysis method examined the main causes of the risk likelihood as the results of the planned and unplanned attacks. The sensitivity analysis is performed through AgenaRisk with BN tools by selecting a single target node, and the sensor nodes are preferred based on the rank of sensitivity nodes (AgenaRisk, 2021). In this study, Boolean nodes with two values (either true or false) or ranking of (High, medium, and low) were used. Sensitivity analysis challenges the reliability, difference, and significance of the assumptions to address the 'what if' analysis. The analysis method on the scenarios checked the sensitivity of the answers against the technique and its related parameters. For the tool's effectiveness, the researcher determined the technique's sensitivity to the Conditional Probability Tables (CPT). Sensitivity analysis communicates data and outcomes, understanding the link between the input and output variables while identifying sensitive variables. It then helps to make assumptions that allow decision-making and examines the amount of risk in given scenarios.

Figure 10 shows the sensitivity analysis for the risk likelihood of a planned attack. The risk likelihood ranks from low to medium to high, while the planned attack has Boolean values (true and false). When the risk likelihood is true, it gets a high rating of the risk likelihood. When the risk likelihood is false, then the likelihood is low. The values of the sensitivity analysis are shown in the figure below.

		Planned Attack	
		False	True
Risk LikeliHood	High	0.336	0.664
	Medium	0.952	0.048
	Low	0.672	0.328

Figure 10: Risk likelihood for planned attacks (Data source: Survey, 2021)

Figure 11 shows an analysis of the unplanned attacks, which are actions performed by insiders. These attacks could be activities that are the result of poor decision-making with regard to the system of an ignorant, extremely tired, and computer-illiterate employee. Unplanned attacks hold the Boolean values (true and false) while the risk likelihood ranks from low to medium to high. The risk likelihood value becomes high when the planned attack is true and the risk likelihood becomes low when the planned attack is false. These values are shown in the figure below.

		Risk LikeliHood		
		High	Medium	Low
Unplanned Attack	False	0.563	0.427	0.01
	True	0.978	0.018	0.004

Figure 11: Risk likelihood for unplanned attacks (Data source: Survey, 2021)

4.4 Tornado graphs for planned attacks

Tornado graphs are generated based on the simulated scenario for planned and unplanned attacks. Tornado graphs are generated using the package. The Tornado chart was used to evaluate the sensitivity analysis of planned human-induced attacks. Figure 12 shows the planned attack that carries a true value with medium (0.048) and high risk (0.664) likelihood.

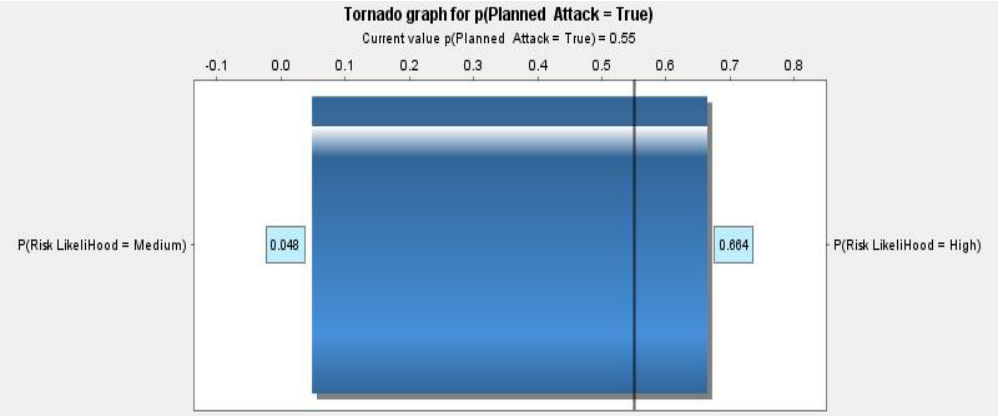

Figure 12: Tornado graph for planned attack = True

Figure 13 shows the false planned attack with high (0.336) and medium (0.952) risk likelihood.

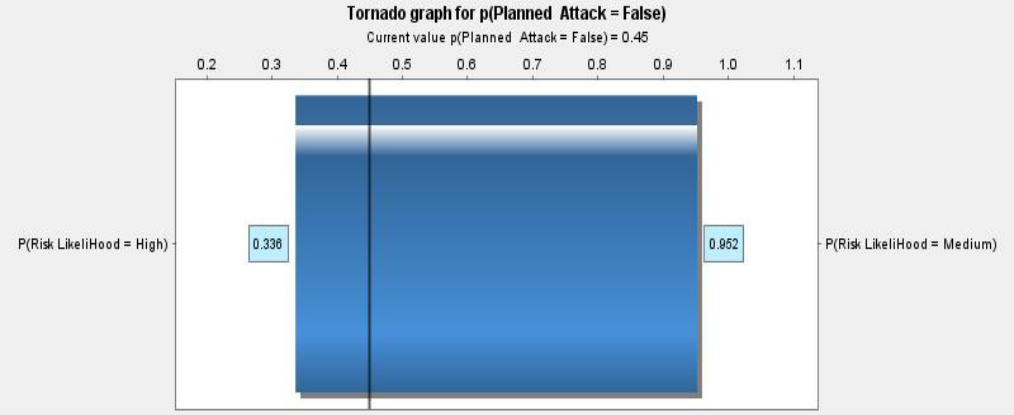

Figure 13: Tornado graph for planned attack = False

4.5 Decision Tree Analysis (DTA)

DTA as a quantitative risk analysis technique is used to assess the potential risks caused by planned and unplanned cyber-attacks. It determines the risk likelihood leading to the destruction of the business service. Every risk likelihood is determined by the appropriate and proactive security measures deployed to reduce,

avoid, separate, and mitigate risks. Figure 14 shows DTA with possible risks caused by human factors relating to planned and unplanned cyber-attacks. In the figure, people operate the system where their performed activities get processed on the business system. So these actions can be part of the planned attacks coming from intentional criminals and also from legitimate employees who sometimes ignorantly operate the business system and leave it compromised. For example, an unexpected attack could be an ignorant employee downloading a file or software from unverified sources, while the planned attack could be a criminal who has gained unauthorised access to the business system. Usually, the planned attacks are network-dependent, where a criminal searches for an unsafe network port or interface.

The planned attacks are usually in the form of phishing, malware, denial of service, and device failure attacks, while unplanned attacks relate to the lack of skills, ignorance, poor decision-making, poor implementation, unlimited access to sensitive resources, and use of the affected external hard drives. These attacks pose risks related to the lack of confidentiality, financial loss, other losses, manipulation and deletion of sensitive data, unauthorised access to private information, damage or unavailability of a resource, and delayed services.

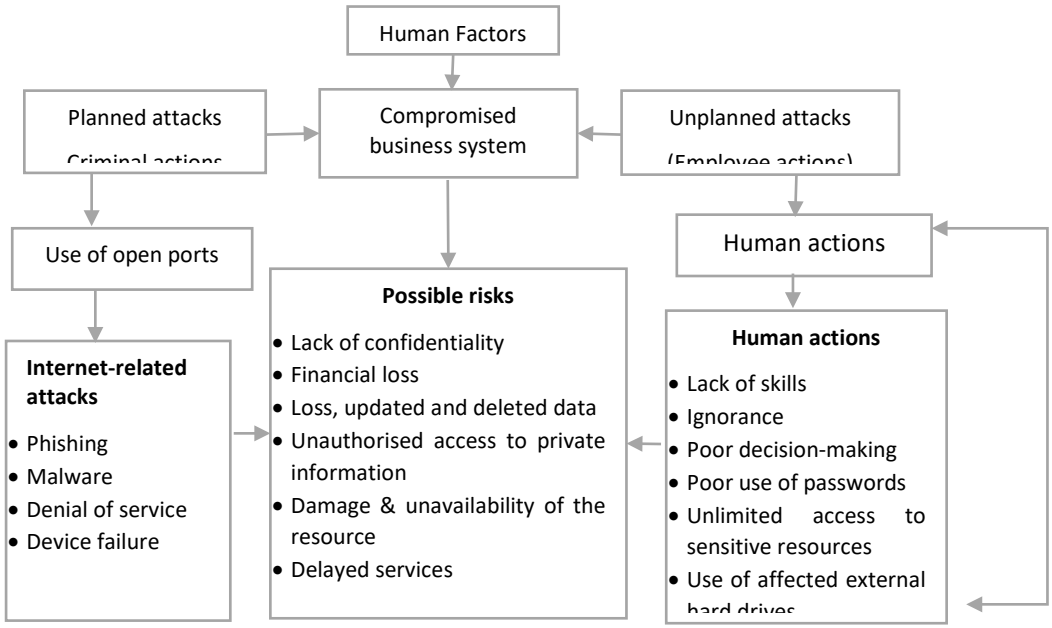

Figure 14: Risks associated with planned and unplanned attacks (Survey, 2022)

4.6 Discussions

In South Africa, there is not much deployment of artificial intelligence that replaces human actions, which makes businesses rely more on people. Even though people form a significant part of businesses, they still become the main source of various planned and unplanned cyber-attacks. Hadlington (2017) states that human errors are one of the attacks that are underestimated and ignored. The case scenario demonstrated that human factors could be the source of attacks compromising the system in one way or another. Some harmful human actions are caused by insiders, while intentional errors compromise the systems. Sometimes, human mistakes expose businesses to risks that significantly affect information and computer security (Anwar et al., 2017).

Criminals take advantage of gaining unauthorised access to the system owing to insider action. Criminals usually take time to plan for their activities, while insiders react based on their attitudes, behaviour, and opportunities. The ignorant, pressured actions reveal valuable, sensitive information and other business resources to opportunistic cybercriminals. Criminals hijack unsecured sessions intending to violate privacy and security. Minimal use of safety measures increases the chances of data breaches (Ncubukezi, 2022a). Sometimes, human errors are caused by inadequate staff members, fatigue owing to work overload, and operating under pressure (Turk, 2013).

Similarly, insiders create a loophole in the system when they have bad intentions. Understaffing in businesses creates human errors because some employees may be highly ignorant of their actions in the system. Some employees do not have adequate skills to help them make informed decisions. In this scenario, the risk probability is influenced by the presence and adherence to the available security policies, rules, procedures, and guidelines. The amount of risk likelihood influences the risk impact in the system. The higher the risk probability, the greater the impact. As stated in the previous section, cybersecurity risk results in reduced profit, poor

performance, loss of clientele, and a bad reputation, affecting overall business continuity (Ncubukezi, 2022c). Ncubukezi (2022a) states that employees can be the weakest link of the chain and a channel for criminal activities, as the criminals use every opportunity they have. A malware attack simulated scenario is presented below. Employee mistakes put businesses at risk, while the SME sector pays little attention (Ergen, Ünal & Saygili, 2021).

Often, criminals gain unauthorised access owing to employee work overload and other related factors. The challenge is the diverse range of human errors, which open doors to unauthorised access to people who steal sensitive information and other valuable assets. This action results in a significant data and security breach (Richardson et al., 2020). For example, criminals take advantage of the unsure network sessions by violating safe surfing and privacy (Wallace et al., 2020). Some threats are harmful malware such as viruses, phishing, Trojan, adware, spyware, and worms (Karaci, Akyüz, & Bilgici, 2017). For example, the software automatically gets installed without the user's knowledge when a victim ignorantly clicks on harmful links or uses automatic pop-up messages.

Table 2 shows the summary of the collected risks caused by human factors. The respondents revealed different interpretations of the protection level of their systems. Even though most businesses have indicated some awareness and understanding of the protection level of the system, none of the businesses mentioned the use of multi-factor authentication. The promoters of human errors are ignorant users who cause poor decision-making and show a lack of skills, and minimal knowledge about information and computer security, leading to poor implementation and not adhering to security guidelines.

Table 2: Summary of collected cyber-risks table (Data source: Survey, 2022)

<table>
<tr><th colspan="6">Human factors = (Planned and unplanned cyber-attacks)</th></tr>
<tr><th>Causes of attacks</th><th>Affected asset</th><th>Security principle</th><th>Risk cause and source</th><th>Risk Impact</th><th>Risk consequence</th></tr>
<tr><td rowspan="2">• Poor decision-making
• Lack of management involvement
• Work overload & stress
• Ineffective access & resource management.
• Outsourced IT services</td><td>• Employees
• Files
• Websites
• Third parties
• Personal information</td><td>• Confidentiality
• Integrity</td><td rowspan="2">• Planned and accidental actions
• Ignorance - poor decision-making
• Lack of skills
• No management involvement
• No cybersecurity personnel
• Poor compliance with guidelines and procedures
• Low-security awareness and understanding
• Poor password creation and management
• Unauthorised use of access rights
• Incomplete configuration management
• Lack of skills</td><td>• Loss of information
• Lack of client trust
• Financial loss
• Declined production and business growth</td><td>• Lack of a cybersecurity policy
• Take your own device to work
• Physical security
• Identity theft, fraud.
• Deletion, theft, and corruption of data.</td></tr>
<tr><td>• Poor configuration management
• Malicious and accidental activities
• Careless handling of data
• Unsecured network ports</td><td>Measure: Adherence to business and cybersecurity policies and guidelines</td><td>Measure: Protect the
• Network
• Password
• Device
• Email
• System</td><td>• Mistakes leading to a significant data breach
• Ignorance can lead to legal fines, loss of client trust
• Bad Reputation</td><td>• Ultimate data breaches</td></tr>
</table>

4.6.1 Significance of the study

This study shares insights about the literature relating to the state of cybersecurity and the risk likelihood of planned and unplanned cyber-attacks in small businesses. The work used the BN tools in the AgenaRisk package to demonstrate the predicted risk likelihood of planned and unplanned cyber-attacks, which is a human factor. In addition, the research used quantitative risk analysis techniques. It provides risk managers with benchmarks that can help adjust security resources in order to position ideal protection levels. This study provides risk managers with benchmarks to help adjust security resources to position ideal protection levels. The following section addresses the future developments and the concluding remarks.

5. Concluding remarks and Future developments

This study determined the risk likelihood relating to human factors which are planned and unplanned activities in the business system. The study used BN on the package to observe the planned and unplanned cyber-attacks on the business system. The observations of the risk likelihood on the package were done based on the

sensitivity analysis and Tornado graphs. In addition, decision tree analysis and scenario-based analysis were used as the techniques to analyze and determine the risk likelihood of cyber-attacks.

In the future, the observations from this study can be extended to big organisations and also be performed per sector. The scope of the work can also include other different provinces in South Africa.

Acknowledgments

I would like to thank National Research Foundation (NRF) Black Academics Advancement Programme (BAAP) Grant for financially supporting this work.

References

AgenaRisk. 2021. AgenaRisk. Available: http://www.agenarisk.com. [Accessed: 13 November 2020]

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, pp.437-443.

Chen, T.T. and Wang, C.H., 2017. Fall risk assessment of bridge construction using Bayesian network transferring from fault tree analysis. *Journal of Civil Engineering and Management*, *23*(2), pp.273-282.

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), pp.210-210.

Fenton, N. and Neil, M., 2014. Decision support software for probabilistic risk assessment using Bayesian networks. *IEEE Software*.

Fenton, N., Neil, M., Marsh, W., Hearty, P., Marquez, D., Krause, P. and Mishra, R., 2007. Predicting software defects in varying development lifecycles using Bayesian nets. *Information and Software Technology*, 49(1), pp. 32-43.

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.

Hakak, S., Khan, W.Z., Imran, M., Choo, K.K.R. and Shoaib, M., 2020. Have you been a victim of COVID-19-related cyber incidents? The survey, taxonomy, and mitigation strategies. *Ieee Access*, *8*, 124134-124144.

Japertas, S. and Baksys, T., 2018. Method of early staged cyber-attacks, detection in IT and telecommunication networks. *Elektronika ir Elektrotechnika*, *24*(3), pp. 68-77.

Karaci, A., Akyüz, H.İ. & Bilgici, G. 2017. Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), pp. 2079–2094.

Khan, N.A., Brohi, S.N. & Zaman. N. 2020. Ten deadly cyber security threats amid COVID-19 pandemic. *TechRxiv Powered by IEEE*: pp. 394–399.

Khodakarami, V., Fenton, N., & Neil, M. (2007). Project Scheduling: Improved Approach to Incorporate Uncertainty Using Bayesian Networks. *Project Management Journal*, 38(2), pp. 39–49.

Khosravi, M. and Ladani, B.T., 2020. Alerts correlation and causal analysis for APT based cyberattack detection. *IEEE Access*, *8*, pp.162642-162656.

Ncubukezi, T. and Mwansa, L., 2021. Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid-19 Pandemic. *Journal of Internet Technology and Secured Transactions*, *9*(1), pp. 714-721.

Ncubukezi, T., 2022a. Human errors: A cybersecurity concern and the weakest link to small businesses. In *Proceedings of the 17th International Conference on Information Warfare and Security* (p. 395).

Ncubukezi, T., 2022b. Impact of information security threats on small businesses during the Covid-19 pandemic. In *European Conference on Cyber Warfare and Security*, 21(1), pp. 401-410.

Ncubukezi, T., 2022c. *Design development and evaluation of the cybersecurity risk tool: a case of small and medium-sized enterprises in South Africa. (*Doctoral Thesis, Cape Peninsula University of Technology, unpublished).

Ncubukezi, T., Mwansa, and Rocaries, F. 2020a. "A Proposed: Integration of the Monte Carlo model and the Bayes network to Propose Cyber Security Risk Assessment Tool for Small and Medium Enterprises in South Africa." *International Journal of Computer Science and Information Security*, 3(18), pp. 152-155.

Ncubukezi, T., Mwansa, and Rocaries, F. 2020b. "A review of the current cyber hygiene in small and medium-sized businesses." *International Conference for Internet Technology and Secured Transactions*, 15, pp. 283–288.

Robson, C. 1993, *Real world research: A resource for social scientists and practitioner-researchers*. Oxford: Blackwell Publishers.

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

Wang, J. and Neil, M., 2021. A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples. *arXiv preprint arXiv:2106.00471*.

Wijayanto, H. and Prabowo, I.A., 2020. Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, *9*(3), pp. 395-399.

Yang, X.S. 2019. *Introduction to algorithms for data mining and machine learning*. London: Academic Press.