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

Tabisa Ncubukezi
Information Technology Department
Cape Peninsula University of Technology
Cape Town, South Africa
Ncubukezit@cput.ac.za

Laban Mwansa
Electrical Engineering Department
Cape Peninsula University of Technology
Cape Town, South Africa
Mwansal@cput.ac.za

Francois Rocaries
Electrical Engineering Department
Cape Peninsula University of Technology
Cape Town, South Africa
Rocariesf@cput.ac.za

Abstract*—Cyber-risks have become a serious concern and a considered perspective in enterprise risk management configuration and reporting. Cyber-risks has the potential to harm information assets in this era of the internet of things, which ultimately quantifies cybersecurity crimes. For big corporations, it is now a legal requirement to report cyber-security preparedness to corporate shareholders as part of good governance. It is not clear whether small and medium-sized enterprises (SME) have a clear framework in place to combat cyber risks potential to harm information assets. There is minimal research done on the integration of the Monte Carlo simulation tool and artificial intelligence to recommend a proactive cybersecurity risk response plan. So, this paper proposes a cyber-risk assessment tool for small and medium-sized enterprises (SME's) in South Africa. Also, the article forms part of the on-going doctoral research about the analysis and design of cybersecurity risks framework within the SME's in South Africa. The proposed cybersecurity risk assessment tool aims to predict the risk cause, impact, cyber-risk likelihood, and the systematic trends within small businesses in South Africa.

***Keywords*—** *Bayesian network, cyberattacks, cybercrimes, cyber threats, Monte Carlo model, risk impact; risk probability; cyber risk assessment; risk response plan*

I. INTRODUCTION

Small businesses are vulnerable to sorts of risks, which could be planned or unplanned exposure to harm or put in danger the organization's assets. The risks are often associated with the loss of valuable assets or resources. However, the literature explains risk as a planned event, which leads to uncertain results [13]. The term risk relates to possible exposure to harm, danger, or uncertainty. However, various industries interpret and use the term differently and loosely. Within the business sector, it is impossible to separate the risk from the business cycle. Also, one cannot separate cyber threats from the internetworked world [2, 13]. Cyber risks are commonly interpreted as the lack of privacy, confidentiality on the personal or organizational data due triggered by cyber threats, and ransomware [15]. The term cyber risk is interchangeably used as the cyber-attack or cyber-crimes.

As the world becomes smart by connecting through smart devices to keep up with the technology, cyber risks also increase in number through innovative ways [3,14]. The cyber threats aim and penetrate all sorts of interconnected businesses regardless of the size, number of employees, and the annual turnover [16]. The primary focus for cyber attackers is mainly on the lucrative benefits than the size of the business sector. As a result, SMEs' has become the primary target for cyber threats.

As cited by [1], the Federation of Small Businesses (FSB) announced the monetary value amounting to £5.26 billion to the U.K. economy caused by cybercrimes. [4] says 8.8 Million South Africans have fallen victims to cybercrimes. The Minister of Telecommunications and Postal Services (TPS), Siyabonga Cwele, said in Cape Town Parliament that an estimated 32 percent of small and medium enterprises in South Africa are affected by the cyber threats and phishing attacks [9]. At the moment, the country currently does not have the public or national document that records cyber risks affecting the SMEs'.

[16] says that the study conducted by Ponemon Institute in the U.K. and U.S.; the main cyber-attacks which have hit the SME's were the use of weak passwords by employees, ransomware, data breaches, phishing. Asian Pacific SME's explained that the primary sources of the cyber-attacks are the malfunctioning of the SME systems, which affects the business continuity and eventually loses data. However, at this stage, it is not whether the loss of data is through the system itself or the human error. The human error could either be through the loss of the company devices with information or an employee unintentionally divulging due to the lack of skill [10].

Due to the high cybercrimes which SME's experience, the proposed work aims to develop a cybersecurity framework tool that will integrate Monte Carlo and the Bayesian network to combat cyber risks.

II. LITERATURE REVIEW

This proposed paper will look and focus on SME in South Africa. The study will look at SMEs' from all business sectors. The research suggests the design, development, and evaluation of cyber-risk assessment tool to proactively mitigate the cyber risks within the South African SME's. The main aim of the proposed structure is to reduce the time spent on cybersecurity risk management.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

A. *Cyber threats, attacks, targets, and impact*

The following section addresses cyber threats, cyberattacks, cyberattack platforms, as well as the ultimate cybercrimes, as shown in table 1. Cyber threats are possible malicious attempts that could damage or disrupt a computer network or SMB systems. Cyber threats are mostly caused by cyberattacks such as malware, data breaches, denial of service, and network exploitation. All these cyberattacks could happen through a standalone computer, or the connection to the cyberspace on a networked computer, or use of external storages.

Tab 1. Initiation of cybercrimes (Source: [14], Unpublished)

CYBER THREATS	CYBERATTACKS	CYBERATTACK TARGETS	CYBER CRIMES
• Information security threats that damage or corrupt data • Inavailability of data • Intrusion • Disrupt business continuity	• Malware (viruses, spyware) • Data breaches • Denial of Service (DoS) • Network exploitation	• Cyberspace • Stand alone computer • Networked computer • External data storages	• Harm SMB reputation • Cause physical damage on the devices • Discontinue business • Fraud • Threaten financial health
Caused by	Through	Lead to	
ALL BUSINESS SECTORS			

B. *Cyber Risk Management*

All adverse cyber-security risks exist to harm, interruption, damage, dent, and affect business growth and day-to-day operation [2]. Cybercrimes come in various forms of attacks in business with the primary goal that is to benefit in every possible way, for as long as they will get a lucrative portion of the company [7].

C. *Application of NIST Framework for risk mitigation*

The NIST cybersecurity framework represents the U.S. policy framework that provides the computer security guidance, best practices, and standard practices for helping all organizations to evaluate and improve the capacity to prevent, detect and respond to all cyber-attacks (NIST, 2014). The framework focuses on defining the standard methodology for managing cyber risks. NIST provides a broader and balanced cybersecurity that suits all business sectors.

The framework works around a sound set of five concurrent and continuous functions addressing different steps to process cyber threats: Identity, Protect, Detect, and Respond, Recover.

III. PROPOSED APPROACH

This paper will involve a detailed process of carrying out the research to offer specific answers for every problem provided through supporting literature and the data collection [6]. The research process will include the discussions of the research methodology, data collection methods, a sampling of the informants. The proposed method of inquiry will be carried out in five phases, as shown in **Error! Reference source not found.** to find answers to the research questions posed in this study.

Phase one reviews the relevant sources of literature, and conduct both the qualitative and quantitative study, one after the other. Qualitative research will be performed to gather common cybercrimes within the South African SME sectors. The quantitative research will be done to categories the dependent and independent variables. The data collection to form the knowledge base for the following phases.

Phase two will develop a knowledge base for the Monte Carlo model using the collected data to determine dependent and independent variables.

Phase three will use the Monte Carlo simulation model to determine the probability and *what-if's* situations.

Stage four will develop the cybersecurity risk framework by integrating the Monte Carlo model with the Bayesian network to generate conditional outcomes to combat cyber risks.

Stage five will evaluate the proposed structure and come up with five sample case studies that will test the effectiveness.

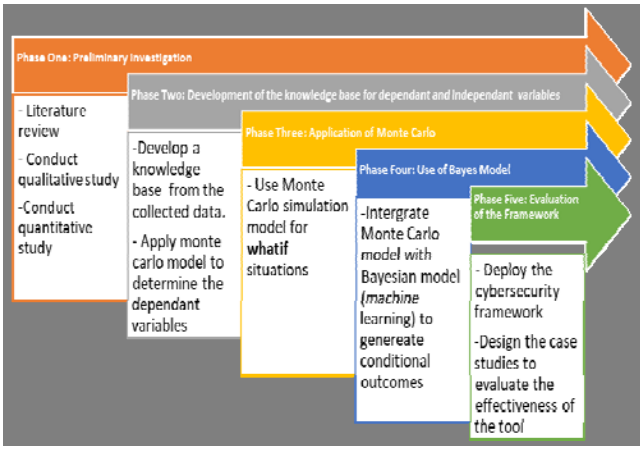

Fig. 1: Methodology Phases (Own work, 2020)

A. *Data collection methods*

The qualitative interviews with SME stakeholders will help to identify and describe critical themes. The study will use the focus groups to gather information from a group of participants within the same business. The questionnaires will be deployed on Google forms to collect qualitative and quantitative data about the existing cybersecurity risks, risk cause, effect of risk, risk likelihood, and risk probability. The questionnaire will also be the guideline for interviews.

B. *Sampling*

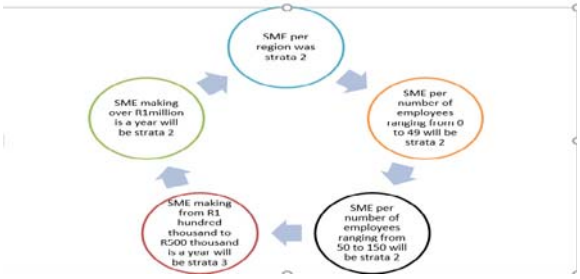

Fig. 2. Elements of selecting strata (Own work, 2019)

C. *Adoption of the Monte Carlo Model*

Monte Carlo, risk simulation model, will analyze the likelihood, impact, and the proximity of cyber-security risks within the small-medium enterprises in S.A. It will further investigate the systematic trends of the dangers. Monte Carlo, the risk simulation model, is selected among others based on its high sensitivity in the domain of enterprise. Secondly, it extremely grounded in the sense that it highly supports privacy and confidentiality security features.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

D. Integration of Bayesian Network

In the proposed study, the Bayes' model will evaluate the risk and updates predicted probabilities of the risk event by incorporating new information through mathematical formulas to calculate the conditional probability of the possible cyber risk cause for a given observed outcome [8]. The conditional likelihood computed from knowledge of the likelihood of each cyber risk cause and the probability of the outcome of each cause [5]. Thomas Bayes's model predicts to determine the likelihood and its conditions. In this study, the Bayes theorem will evaluate the risk probability of an event based on the prior knowledge of the terms that relate to the event.

E. Link to existing research

This research links to a significant Ph.D. research work on the design and development of cybersecurity. The researcher produces papers that report about various phases from the first to the last stage. Each article will address how the ultimate cybersecurity risk response framework has been planned, designed, developed, and evaluated.

F. Ethical considerations

The university's ethics committee issued an ethical clearance certificate which explained the rules and regulations. Every participant on the research project will receive the consent letter requesting their voluntary participation. The signed consent letter will represent legal practice. Research participants will receive the assurance that their details and the data collected would remain private and confidential.

IV. Research outcomes

The proposed study will draw and contribute to the literature on cyber-security risks within the SMEs. Use the Monte Carlo model to analyze quantitative cyber threats within the SMEs. Develop the knowledge base for the Bayesian approach.

V. CONCLUSION

This position paper links to the main doctoral research project. Outcomes of each framework development phase will be shared in the form of research papers. Cybercrime has become the main risk within SME's business cycle. The probability of cybercrimes could disrupt the businesses and eventually discontinue the business progress and performance.

One of the outcomes of this study will identify the common cyber crimes and their impact on SME's. Another report will look at the dependent and independent cyber risks, which will involve the probabilities of cyber threats. Lastly, the study will develop a cyber-framework which SME's could use to combat risks using the Bayesian model.

Authors

Tabisa Ncubukezi is a lecturer and a Ph.D. candidate at the Cape Peninsula University of Technology in South Africa. She has more than ten years of teaching experience at the University of Technology and colleges. Her primary teaching focus is on communication networks and security. Her research focus is on cybersecurity.

Laban Mwansa
Senior Lecturer in the department of electrical, electronic and computer engineering. Laban obtained his Ph.D. in computer engineering from the Czech Technical University in Prague. He currently lectures and supervises postgraduate students in the department. He was also a visiting professor at the University of Paris (UPEC) in 209

Francois Rocaries
Professor Francois is a scientific director at the French South Africa Institute for Space studies. (FSATI). He has published and graduated many postgraduate students in France and South Africa

References

[1] A. Sword, "SMEs hit with 7 million cybercrime attacks per year in £5.26 billion blow to U.K. economy," Computer Business Review, 2018. Available in: http://www.cbronline.com/news/cybersecurity/business/smes-hit-with-7-million-cyber-crime-attacks-per-year-in-526-billion-blow-to-uk-economy-4919992/ [Accessed on 2 February 2020)

[2] B. Van Niekerk, "An analysis of cyber-incidents in South Africa". The African Journal of Information and Communication (AJIC), 2017, Vol. 20, pp. 113-132.

[3] C. Fripp, "Cybercrime costs South Africa about R5.5 billion a year". Available from https://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/ 2015, [Accessed: on 06 September 2019]

[4] D. Linington, "8.8 Million South Africans have fallen victims to cybercrime". Retrieved on 15 February 2020. http://www.itnewsafrica.com/tag/cybercrime-stats/, 2016

[5] D.S. Gupta, "Introduction to Conditional Probability and Bayes theorem for data science professionals" available from https://www.analyticsvidhya.com/blog/2017/03/conditional-probability-bayes-theorem/ 2017, [Accessed: 11 February 2020]

[6] E. Barbie, J. Mouton, "The practice of social research. South African edition Oxford University Press", Cape Town, South Africa, ISBN 0 19 571854 2, 2001

[7] F. Almeida, I. Carvalho, F. Cruz, "Structure and Challenges of a Security Policy on Small and Medium Enterprises." *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS* VOL. 12, NO. 2, Feb. 2018. Page 747-763.

[8] F.X. Aguessy, O. Bettan, G. Blanc, V. Conan, H. Debar, "Hybrid Risk Assessment Model Based on Bayesian Networks." 11th International Workshop on Security, IWSEC 2016, Sep 2016, Tokyo, Japan. pp.21 - 40,

[9] L. Peyper, "32% of SMEs in S.A. at risk of cyber-attacks – Cwele" Retrieved from https://www.fin24.com/Economy/32-of-smes-in-sa-at-risk-of-cyber-attacks-cwele-20160309, 2016 [Accessed on 8 March 2020]

[10] L.S. Howard., "SMEs Underestimate Cyber Risks Which Could Prove 'Fatal': Allianz Report." Available from https://www.insurancejournal.com/news/international/2018/02/21/481113.htm, 2016 [Accessed on 12 January 2020]

[11] R. Koeze, "Designing A Cyber Risk Assessment Tool For Small To Medium Enterprises." The Delft University Of Technology, Faculty of Technology, Policy and Management Research conducted at KPMG Advisory N.V. November 2017 Electronic version available at http://repository.tudelft.nl. [Accessed: 15 June 2018]

[12] S. Dilek, H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cybercrimes: A review". *International Journal of Artificial Intelligence & Applications (IJAIA),* Vol. 6, No. 1, 2015.

[13] T. Aven, O. Renn, "On risk defined as an event where the outcome is uncertain" Journal of Risk Research, 2009, vol.12, No.1, pp. 1-11.

[14] T. Ncubukezi, L. Mwansa, F. Rocaries, "A review of the current cybercrime hygiene within the small and medium-sized enterprises" (unpublished).

[15] T. Rid, B. Buchanan, "Attributing Cyber Attacks." Journal of Strategic Studies, 2014, Vol 38(1-2), pp. 4–37, 2014.

[16] W. Ashford, "SMEs more vulnerable than ever to cyber-attacks," survey shows https://www.computerweekly.com/news/450428246/SMEs-more-vulnerable-than-ever-to-cyber-attacks-survey-shows, 2017 [Accessed: 8 March 2020]

[17] NIST (2014). Cybersecurity Framework. From https://www.nist.gov/cyberframework [Accessed: 10 January 2020]

https://sites.google.com/site/ijcsis/
ISSN 1947-5500