INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN PROGRESSIVE EDUCATION & DEVELOPMENT

OPEN ACCESS JOURNAL

Vol 13, Issue 4, (2024) E-ISSN: 2226-6348

Factors Influencing Cybersecurity: A Focus Group Approach

Anesu R. Dikito[1], M Shamim Kaiser[2] and J. Philip Vincent[3]

[1]PhD Researcher, Binary University of Management & Entrepreneurship, [2]Professor, Institute of Information Technology, Jahangirnagar University, Bangladesh, [3]Adjunct Professor, Binary University of Management & Entrepreneurship, Malaysia

To Link this Article: http://dx.doi.org/10.6007/IJARPED/v13-i4/23539 DOI:10.6007/IJARPED/v13-i4/23539

Published Online: 06 November 2024

Abstract

Cybersecurity has become a critical concern for organizations and individuals alike, driven bythe increasing frequency and sophistication of cyber threats. This study explores the factors influencing cybersecurity through a focus group approach, engaging professionals from the banking sectors to gain insights into the challenges and best practices in maintaining robust cybersecurity measures. A focus group approach was employed to collect data from information technology experts and senior managers from risk and audit departments in Zimbabwean commercial banks. The findings highlight human factors and technological factors, offering a comprehensive understanding of the multifaceted nature of cybersecurity. The results showed that human factors influencing cybersecurity were awareness, top management support, information sharing, cyber-response teams, research teams, enactment of cyber-laws, cyber governance framework and crafting of cybersecurity policy. The technical factors were application security, network security, database security, physical security, and internet security.

Keywords: Cybersecurity, Application Security, Network Security, Physical Security

Introduction

Cybersecurity is a dynamic and complex field, essential for protecting the Bank's sensitive information and ensuring the integrity of digital infrastructures (Mughairi et al., 2019). As cyber threats continue to evolve, understanding the factors that influence cybersecurity is paramount for developing effective strategies and solutions. This paper employs a focus group approach to explore these factors, providing a nuanced perspective from professionals actively engaged in cybersecurity.A focus group discussion is an exploratory research technique where data is collected via groupinteraction (Ho, 2006; Krueger & Casey, 2000). Thus a focus group discussion is another method of collecting primary data and was led by a moderator.

Problem Statement

Cybersecurity threats continue to escalate in both frequency and sophistication, understanding the factors that influence banking institutions and their customer responses to these threats is critical for developing effective security strategies.

Traditional approaches to identifying thesefactors often rely on quantitative data or theoretical frameworks, which may not fully capture the nuanced and contextual influences impacting cybersecurity practices and decision-making. The increase in cybersecurity threats require a deeper and more comprehensive understandingof the various factors influencing cybersecurity through a focus group approach. This method aims to explore and identify the human and technical factors that impact how banks perceive and respond to cybersecurity threats.

By utilizing a focus group approach, the study seeks to gather qualitative insights and perspectives from key stakeholders, including IT professionals, security managers, and end- users. This approach aims to uncover underlying issues, behavioural patterns, and contextual elements that quantitative data alone may not reveal. The ultimate goal was to inform the development of more tailored and effective cybersecurity model that address the problem of breaches posed by cybersecurity threats.

Limitations

The focus group approach may be limited by the sample size and composition, which might not fully represent the broader population of banks or individuals affected by cybersecurity issues. Thus findings from focus groups may not be easily generalized to all banking institutions in different geographical regions. The specific factors influencing cybersecurity inone context may differ significantly from those in another, limiting the applicability of the results across different settings.

Literature Review

Understanding the factors influencing cybersecurity is crucial for developing effective security measures and interventions. While traditional research often employs quantitative methods, focus group approaches offer valuable qualitative insights into the subjective and contextual factors shaping cybersecurity practices. This literature review explores recent studies that utilize focus groups to investigate these factors, highlighting key findings and methodologicalcontributions.

Human Factors Influencing Cybersecurity

Perceived Threats and Risk Perception**:** Perceptions of threat and risk influence how organizations and individuals approach cybersecurity. Focus groups have provided insights into how different stakeholders perceive cybersecurity risks and their implications for securitystrategies. Research by Carter and Kockelman (2022) found that varying perceptions of threatlevels among different departments within organizations impact their engagement with cybersecurity measures. This highlights the need for tailored communication and risk management strategies.

User Attitudes and Training**:** User attitudes towards cybersecurity and the effectivenessof training programs are critical factors influencing security behavior. Focus group research bySmith et al. (2023) highlighted that users' attitudes towards cybersecurity training and awareness programs significantly affect their engagement and adherence to security practices.The study found that interactive and contextually relevant training programs are more effectivein changing user behavior.

Compliance and Regulatory Factors**:** Compliance with cybersecurity regulations and standards is a key factor influencing organizational security practices. Focus groups have beenused to explore how compliance requirements affect organizational behavior and decision making. A focus group study by Lewis and Li (2022) examined how compliance with GDPR and other regulations shapes cybersecurity strategies and resource allocation in multinational organizations.

Awareness of cybersecurity risks is crucial for preventing cyber attacks. Employees who are well-informed about potential threats are less likely to fall victim to phishing schemes and other social engineering tactics. Hadlington (2017) highlights the importance of cybersecurityawareness programs, which significantly reduce the incidence of successful cyber attacks by educating individuals about recognizing and responding to threats.

Top Management Support is vital for the successful implementation of cybersecurity measures. Support from senior leadership ensures that adequate resources are allocated to cybersecurity initiatives and that a culture of security is fostered within the organization. Chang and Ho (2006) emphasize that without top management commitment, cybersecurity policies and procedures are likely to be ineffective.

Information sharing among organizations can enhance cybersecurity by enabling the collective identification and mitigation of threats. Cross-sector collaboration and sharing of threat intelligence are essential for staying ahead of cyber attackers. Cavusoglu et al. (2018) discuss the benefits of information sharing frameworks and the challenges associated with trustand data privacy.

Technical Factors Influencing Cybersecurity

Technical-Physical security refers to the protection mechanisms built into hardware and software to safeguard information systems. It includes encryption, access controls, and vulnerability management. Physical security measures protect the hardware and infrastructure that support digital systems. This includes securing data centers, controlling access to critical systems, and protecting against physical threats such as theft or natural disasters. Krause and Tipton (2002) discuss the interplay between physical and cybersecurity and the necessity of comprehensive protection strategies. Recent studies highlight the evolving nature of technicalsecurity and its crucial role in defending against sophisticated cyber threats.

- **Encryption and Cryptography:** Advances in encryption technologies are essential for securing data both at rest and in transit. According to Patel and Shah (2023), the adoption of advanced cryptographic algorithms, such as quantum-resistant encryption,is becoming increasingly important in safeguarding data from emerging threats.
- **Vulnerability Management:** Proactive vulnerability management remains a cornerstone of technical security. Williams et al. (2024) emphasize the need forcontinuous vulnerability assessment and patch management to address newly discovered security flaws and prevent exploitations.

Internet security encompasses measures to protect data and systems when accessing or transmitting information over the internet. Internet security involves protecting online

activities, communications, and transactions. It includes measures such as secure protocols, anti-malware tools, and user education. Schneider (1999) outlines the challenges of internet security, stressing the importance of adopting a multi-faceted approach to protect against a broad spectrum of online threats. It includes technologies and practices such as secure webprotocols, firewalls, and anti-malware solutions.

- **Secure Web Protocols:** The implementation of secure web protocols, such as HTTPS, is critical for protecting data transmitted over the internet. Research by Chenand Liu (2023) demonstrates that widespread adoption of HTTPS and secure web practices significantly reduces the risk of data interception and man-in-the-middle attacks.
- **Anti-Malware Solutions:** Anti-malware tools play a significant role in defending against malicious software. According to Garcia et al. (2024), modern anti-malware solutions must employ behavioral analysis and machine learning techniques to detect and mitigate advanced threats effectively.

Network security involves protecting the integrity, confidentiality, and availability of data and resources as they are transmitted across or accessed through networks. Stallings (2013) emphasizes the importance of layered security approaches to safeguard networks froma wide range of cyber threats. Key components include firewalls, intrusion detection systems (IDS), and network segmentation.

- **Firewalls and IDS:** Firewalls and IDS are fundamental in monitoring and controlling network traffic. Singh et al. (2023) discuss the evolving capabilities of next- generation firewalls and IDS, which now incorporate AI and machine learning to detect and respond to sophisticated network attacks in real-time.
- **Network Segmentation:** Effective network segmentation can limit the spread of cyber threats within an organization. Patel and Kumar (2024) highlight that segmenting networks into distinct zones helps contain breaches and protect sensitivedata from lateral movement.

Database security involves measures to protect databases from unauthorized access, misuse, or misuse. This involves access controls, encryption, and regular audits. Datta et al.(2009) highlight the significance of database security in protecting sensitive data and ensuring compliance with data protection regulations. It includes practices such as access control, encryption, and auditing.

- **Access Control and Encryption:** Database access controls and encryption are criticalfor protecting sensitive data stored in databases. Recent studies by Zhang et al. (2023) underscore the importance of implementing granular access controls and end-to-end encryption to safeguard data from insider and external threats.
- **Database Auditing:** Regular database auditing helps detect and respond to unauthorized activities. Research by Lee and Kim (2024) shows that comprehensive auditing practices, coupled with real-time monitoring, enhance the ability to identify and mitigate security incidents.

Application security focuses on protecting software applications from threats and vulnerabilities throughout their lifecycle. This includes secure coding practices, application testing, and vulnerability assessments. According to McGraw (2012), addressing security during the software development process is more effective and

less costly than fixing vulnerabilities post-deployment.

- **Secure Coding Practices:** Secure coding practices are essential for preventing vulnerabilities that could be exploited by attackers. According to Brown and Smith (2023), incorporating secure coding guidelines and performing regular code reviews significantly reduces the risk of application vulnerabilities.
- **Application Testing:** Regular application testing, including static and dynamic analysis, is vital for identifying and addressing security flaws. The effectiveness of integrating security testing into the software development lifecycle to enhance application resilience against cyber threats.

Research Objectives

- To determine the human factors that influence cybersecurity practices withincommercial banks of Zimbabwe through focus group discussions.
- To determine the technical factors that influence cybersecurity practices withincommercial banks of Zimbabwe through focus group discussions.

Research Questions

- What are the key human factors affecting cybersecurity practices within commercialbanks in Zimbabwe, as identified by focus group participants?
- What are the primary technical factors influencing cybersecurity practices within commercial banks in Zimbabwe, as identified through focus group discussions?

Research Methodology

Focus Group Design

The study employed a qualitative focus group approach, engaging cybersecurity professionalsfrom the banking sector and in particular Information Technology Experts and Senior managers. Participants were selected based on their expertise and experience in cybersecurity, ensuring a diverse range of perspectives.

Data Collection

Three focus group sessions were conducted, each lasting approximately two hours. The focus group discussion was considered appropriate in the study due to the exploratory nature of the study. The study sought to develop a new theory on cybercrime or to extend an existing one. The reason being cybercrime continues to rise despite the availability of theory and technical solutions.

The moderator presented the conceptual framework on factors contributing to cybersecurity tothree different sessions, each having seven (10) participants. The group sessions were configured to trigger the minds of participants and extract as much information as possible from the participants. The backgrounds of the participants were information technology, risk & audit compliance.

Participants were divided into smaller groups of ten (10) people in order to allow every participant room to express their views and opinions. A briefing session was conducted by theresearcher in order to ensure group members had the same objectives and were of similar backgrounds and understanding; the briefing session also allowed the researcher to discuss guidelines for the discussions. This led to three groups which the researcher became the sole moderator on different days.

Moderation provided guidance to the group and presented a talk free environment where participants freely expressed their views, opinions and experiences on a topic. The moderator would introduce discussion topics in a random order but did not offer any views or opinions during the discussion sessions. This was in accordance to (Kamarulzaman, 2011; Stewart, 2018) that a focus group environment should be relaxed, conversational and allow the free exchange of views amongst participants with minimum intervention from the moderator. Thusa focus group relies heavily on the ability of participants to openly communicate their views, and ideas. The participants would share their views, be asked questions and comment on the group's presentation.

Each group was given some plain sheets of paper on which to write their discussion points during the group discussions. A proposed conceptual framework was introduced and explainedto the participants. The study theorized cybersecurity as both a human and technical issue. Thus, in order to address cybercrime one had to consider both human and technical factors.

The *first group* which was composed only of information technology experts was given the cybersecurity conceptual model. The cybersecurity factors that were suggested to reduce cybercrime (identity theft) were application security, database security, network security, physical security and internet security. The factors were all drawn from previous studies on cybercrime and cybersecurity (ISO/IEC 27002 Organisational International Standard, 2008; ITU, 2014). It was explained that technical solutions such as firewalls, antiviruses, data encryption, and use of SSL certificates, Pins and passwords were key in reducing identity theftin Zimbabwean commercial banks. Participants were then allowed to share their views and opinions.

The Cybersecurity Conceptual Model is given in Figure 1

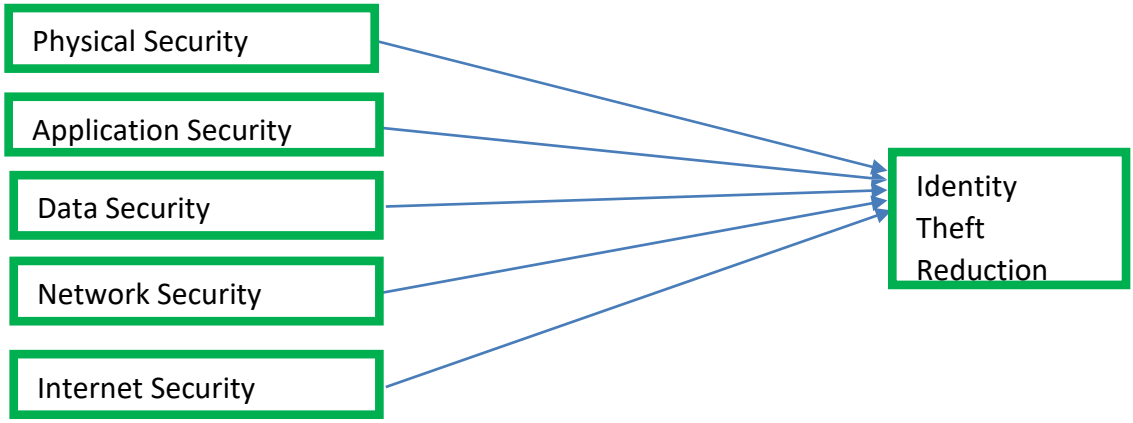

Figure 1: The Technical Conceptual Model

The first group discussing the technical conceptual model was given a discussion topic e.g network security and identity theft, and asked several questions in a random manner as a way to stimulate debate. Some of the questions in Table 7.2 came from the in-depth interviews andothers came from the participants themselves.

Focus Group Questions

1. Cybersecurity breaches are on the increase in Zimbabwe, what do you think are the factors contributing to breaches in cybersecurity?
2. Previous studies have proposed a conceptual framework on reducing cybercrime

asshown in Figure 3.1. What is your view or comment?.

3. Has Identity theft become a regular occurrence in Zimbabwe, at your bank in particular?
4. What do you believe to be the root cause of cybercrime (identity theft) in commercial banks of Zimbabwe?
5. Do you think raising awareness on cybersecurity threats, top management support andcybersecurity policy can positively influence employee behavior (e.g such as not releasing passwords) thereby reducing cybercrime?
6. The bank has implemented technology to secure their LAN/WAN networks, internet and application softwares. Why then does cybercrime (in particular identity theft) continue to occur?
7. What else do you recommend should be done on cybersecurity to curb cybercrime?

The *second* and *third* focus groups were composed of employees from Risk and Audit department and Senior Managers from various departments respectively. These two groups were introduced to the Cybersecurity Conceptual model. The cybersecurity factors that were suggested to reduce cybercrime (identity theft) were awareness, training, top management support, risk analysis, information sharing, punishments, perceived susceptibility, perceived severity, self efficacy and response efficacy. The factors were all drawn from previous studieson cybercrime and cybersecurity (Anupriya & Sebastian, 2018; Bulgurcu et al., 2010; Jansen & van Schaik, 2016; Reyns, 2013). Each factor was explained in terms of its meaning and how it would negatively impact cybercrime. Participants were then allowed to share their views and opinions. The Cybersecurity Conceptual Model is given in Figure 7.3

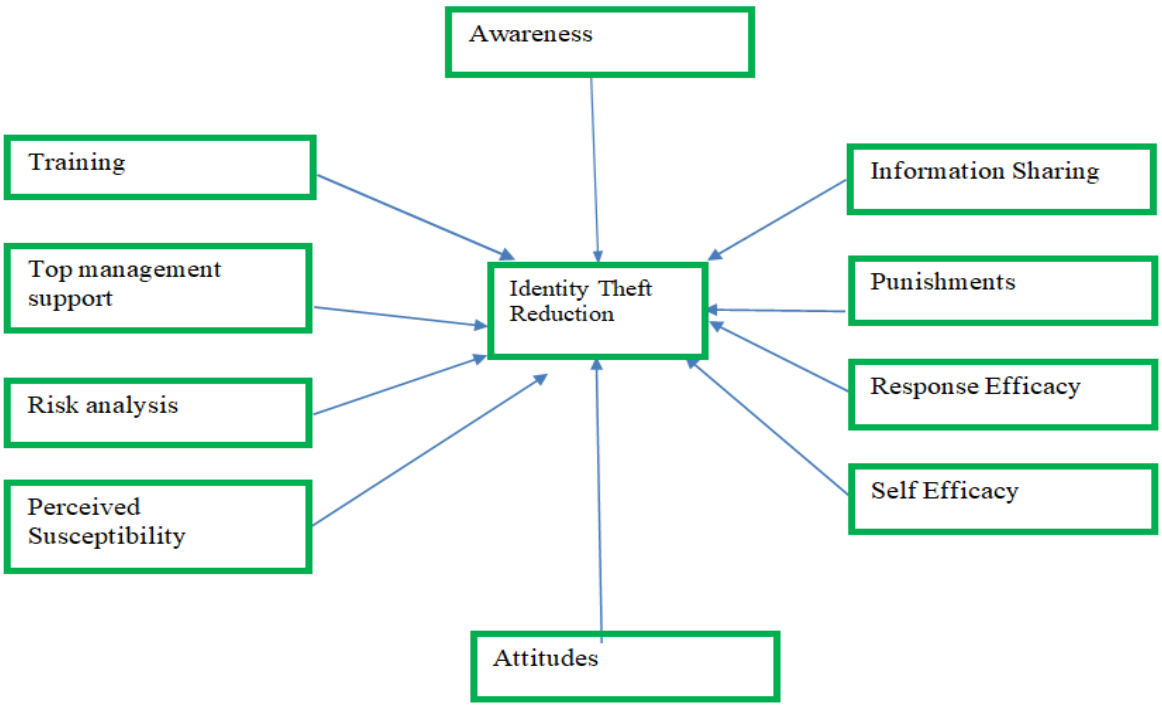

Figure 2: The Human Conceptual Model

The objectives of the focus group discussions were: to determine the factors leading to reducedcybercrime in Zimbabwean commercial banks.

Data Analysis

The grounded theory method as proposed by Egan (2002) was used for data analysis with a slight modification. Only axial coding was used to label the concepts and these concepts wererevealed the key factors which supported the hypothesis set in this study.

The discussions were transcribed and analyzed using thematic analysis to identify recurring factors and insights related to the factors influencing cybersecurity. The overall results of thefocus groups are shown in Table 7.4.

Table 1

Focus Group Discussions Summary

Item	**Group 1** (Information Technology Experts)	**Group 2** (Audit, Risk & Complianceexperts**)**	**Group 3** (Senior Managers)
Factors leading to Identity theftreduction	Network Security,Internet Security, Application Security, Database Security& Physical Security	Awareness, Risk Analysis, Information Sharing, Top Management Support, Technology	Awareness, Risk Analysis, training, Top Management Support, Cybersecurity policy, Punishment
Causes of cybercrime identity theft	Failure to harness AI(artificial intelligence and machine learning) Lack of latest tools	inadequate awareness campaigns risk analysis to must include the cyberspace	lack of awareness poor training (low frequency)
Why does cybercrime continue to rise	Lack of awarenesson employees	Lack of awareness	Poor policy, cybercrime mustbe properlydefined Banks must continuous update their policy
Does Technical Solutions curb cybercrime	Use of Artificial intelligence and Machine learningcan solve cybercrime	Cybersecurity is both a Technical and Human Issue Risk Analysis,	Cybersecurity must define interms of cybercrime

		Employee Training and awareness campaigns are ofimportance	Technical solutions must be married to agood cybersecurity policy in banks
What is the impact of human factors(e.g awareness, training, top managers support) in combating cybercrime	Top managers are needed for budget support Employees require training o ncybersafe behavior	About 50%, we also need Technology andcomputers to help counter cyberthreats	Huge, ICT departmentcannot go italone they need support of everyone sinceemployees canleak vital information to would be offenders
Recommendations	Strong budgetary support from Management International collaboration on AI and machinelearning Pass control to the customer to enableor disable accounts	Training on latest cyber threats More awareness Creation of cyberlaws and a national cybersecurity governance framework fo rZimbabwe Banks must be proactive insteadof reactive	Creation of cyber responseteams Good cybersecurity policies Raise awareness Creation of bank cybersecurity framework, national cybersecurity framework and international cybersecurity framework

From the results of the conceptual framework all the three groups agreed to the proposed conceptual framework although with minor variations. The views of the each individual groupwill be discussed next.

Findings

Group 1 had only information technology experts. The group members were more inclined to use of technologies and artificial intelligence in solving cybercrime. One participant said “dueto the high volume of transactions in commercial banks, no single person will be able to actively monitor the events. No matter what amount of training or awareness we give”. Artificial intelligence becomes useful in alerting employees and monitoring their behaviors when online. The group consented to the technical conceptual model on factors for reducing cybercrime. It was pointed out that cybercrime i.e “identity theft would be reduced if banks secure their network infrastructure, application softwares, encrypt data and use SSL or https when connected to the cyber-environment”. The causes of cybercrime were thought to be lackof latest cybersecurity hardware and software tools to combat cybercrime. Artificial intelligence and machine learning was also said to be “in its infancy stage, its use may prove to be a viable solution in tackling identity theft”. Group members recommended more budgetary support from senior

managers especially with regards to investments in cybersecurity technologies and training on capabilities of artificial intelligence and machine learning algorithms.

Group 2 stressed the need for an "all-encompassing risk management framework". "IT (*information technology*) must be roped in to identifying cyber threats, vulnerabilities and the counter measures", said one participant. The factors which were considered as important in reducing cybercrime were Awareness, Risk Analysis, Top Management Support and Technology. The moderator asked for further clarification on Technology, and this was the response from one participant "Technology is IT experts, security devices and software necessary for protecting a certain resource". The group noted that the problem of cybercrime required both human and technical interventions. "People (Bank Employees) require training and awareness to ensure safe behavior when utilizing the bank's cyber-resources", was anothersentiment echoed during the discussions. The group was also of the view that technology and human aspects had a 50:50 chance of solving the cybercrime in Zimbabwean commercial banks. The group also recommended the "creation of national cyber laws and Cybersecurity governance framework to help curb cybercrime". One participant said "Bank must embark onresearch or sponsor research teams for them to remain on top of the situation". Proactive preparedness was emphasized by group members.

Group 3 agreed to the human factors impacting identity theft reduction. One participant said "Itotally agree with the proposed conceptual framework". The human factors that were emphasized were awareness, senior management support and a good cybersecurity policy. "It is the policy that must define what and how a cyber-resource has to be protected", said one senior manager. Another participant suggested that "the bank framework must feed into the Zimbabwean National cybersecurity framework, and the National Framework must also feed into the International or *Internet* framework". The group opined that fighting cybercrime is therole of everybody in the world, and as such governments and experts must join their hands together. The group members also suggested that "another problem is failure to definecybercrime, solutions must be tailor made to tackle a specific form of cybercrime". Properly define the scope of identity theft and its facets would enable commercial banks in Zimbabwe to counter or reduce identity theft. Group 3 also recommended "creation of cyber-response teams at various levels, such as Bank, government and international".

The focus group discussions identifying the human and technical factors leading to cybercrime reduction, particularly identity theft. The human factors awareness, top management support, information sharing, cyber-response teams, research teams, enactment of cyber-laws, governance framework and crafting of cybersecurity policy were regarded as instrumental in addressing the problem of cybercrime. The technical factors were application security, networksecurity, database security, physical security, and internet security.

Discussion

The findings from the focus group discussions underscore the multifaceted nature of cybersecurity. Human and Technological factors all play interrelated roles in shaping

cybersecurity outcomes. Addressing these factors holistically was essential for developing robust cybersecurity strategies.

The emphasis on human factors aligned with existing literature, reinforcing the need for ongoing education and awareness programs. The discussion on technological factors highlightsthe dual nature of technology as both a solution and a source of new challenges. Policy and regulatory frameworks provide a necessary structure for cybersecurity practices, but their dynamic nature requires organizations to remain agile. Finally, the pivotal role of awareness, and top management support underscores the need for leadership commitment and a security-first mindset across all levels of the banking institutions.

Conclusion

This study provides valuable insights into the factors influencing cybersecurity through a focusgroup approach. By engaging cybersecurity professionals, the research highlights the critical human and technological factors. The human factors were awareness, top management support, information sharing, cyber-response teams, research teams, enactment of cyber-laws, governance framework and crafting of cybersecurity policy. The technical factors were application security, network security, database security, physical security, and internet security. These findings offer a comprehensive understanding of the complexities of cybersecurity, guiding the development of effective strategies to protect against evolving cyberthreats.

Recommendations

Based on the findings from the focus group approach to understanding factors influencing cybersecurity, several recommendations can be made to enhance cybersecurity practices and strategies. These recommendations are designed to address the key insights gathered from stakeholders and improve overall security posture.

Enhance Cybersecurity Training and Awareness Programs

- **Recommendation:** Develop and implement comprehensive cybersecurity training and awareness programs tailored to different roles within the organization. Trainingshould include interactive elements, real-world scenarios, and ongoing updates to address emerging cybersecurity threats.
- **Rationale:** Focus group discussions revealed that effective training significantly impacts employee behavior and adherence to security policies. Regular and engagingtraining can help employees recognize and respond to cyber threats more effectively.

Top Management Support

- **Recommendation:** Allocate sufficient resources and budget for cybersecurity initiatives, including personnel, technology, and ongoing maintenance. Ensure technical support teams are adequately staffed and equipped to manage and upgrade security measures.

  Foster a strong cybersecurity culture by integrating security into organizational values and practices. Management should actively support and promote cybersecurity initiatives through clear communication, leadership, and resource allocation.
- **Rationale:** Focus group participants noted that resource constraints and inadequate technical support can hinder effective cybersecurity. Proper allocation of resources can

address these challenges and enhance the effectiveness of security measures. Insights from focus groups indicated that top management support play a crucial rolein shaping cybersecurity practices. A culture where top managers prioritize security can enhance employee compliance and overall security effectiveness.

Adopt Cybersecurity Technologies

- **Recommendation:** Invest in and deploy advanced cybersecurity technologies, such as next-generation firewalls, intrusion detection systems (IDS), and endpoint protection solutions. Ensure these technologies are integrated and managed effectively to provide comprehensive protection.
- **Rationale:** Technical factors discussed in focus groups highlighted the importance of advanced technologies in detecting and mitigating threats. Integrated and up-to-date security tools can improve threat detection and response capabilities.

Enhance Information Sharing

- **Recommendation:** Promote open communication and collaboration between different departments, such as IT, security, and management, to ensure cohesive and coordinated cybersecurity efforts. Regularly share updates on security policies, incidents, and best practices.
  Create mechanisms for employees and stakeholders to provide feedback on cybersecurity practices and initiatives. Use this feedback to make continuous improvements and adapt to changing security needs
- **Rationale:** Effective communication and collaboration were identified as key factorsin addressing cybersecurity challenges. Cross-departmental cooperation can lead to a more unified approach to managing and mitigating security risks.

Address Policy and Compliance Challenges

- **Recommendation:** Stay informed about relevant cybersecurity regulations and compliance requirements. Develop and maintain policies and procedures to ensure adherence to these regulations, and seek external expertise when needed.
- **Rationale:** Compliance with regulations was a significant concern among focus group participants. Addressing these challenges can help avoid legal issues and improve overall cybersecurity practices.
  By implementing these recommendations, organizations can address the factors influencing cybersecurity more effectively and enhance their overall security posture. These actions willhelp create a more resilient and proactive approach to managing cybersecurity risks.

Acknowledgement

The successful identification of factors influencing cybersecurity would not have been possible without the contributions and support of several individuals and commercial banksin Zimbabwe.

First and foremost, we express our deep gratitude to my supervisor *Professor Shamim Kaiser* for his dedication, expertise, and tireless efforts throughout my work. His contributions in guiding the research work were instrumental in achieving the objectives and *Adjunct Professor J Philip Vincent*, Binary University for proof reading.

A special thanks goes to the sponsor Chinhoyi University of Technology in Zimbabwe who supported this research financially. Their investment in this project reflects their commitmentto advancing cybersecurity and protecting individuals and organizations from phishing attacks.

Finally, we are grateful to the individuals working in various commercial, banks whoparticipated in the focus group discussions

This acknowledgment would be incomplete without recognizing the ongoing support from my wife Sue, whose encouragement and understanding were vital in completing this work.

References

Brown, A., & Smith, J. (2023). Secure Coding Practices and Application Security: AnOverview. *Journal of Software Security*, 19(2), 142-159.

Bulgurcu, Cavusoglu, & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

Carter, J., & Kockelman, K. (2022). Risk Perception and Cybersecurity Engagement: Insights from Focus Groups. *Cybersecurity Review*, 11(4), 75-89.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2018). Emerging issues in responsible information security management. *MIS Quarterly Executive,* 17(2), 105-120.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems,* 106(3), 345-361.

Chen, L., & Liu, M. (2023). The Role of HTTPS in Internet Security: A Comprehensive Study. *Cybersecurity Journal,* 21(3), 115-128.

Datta, A., Jajodia, S., & Brodsky, A. (2009). Foundations of Data Security and Privacy.Springer.

Egan, T. M. (2002). Grounded Theory Research and Theory Building. *Advances inDeveloping Human Resources*, *4*(3), 227–295.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems,* 86, 13-23.

Garcia, R., Lee, H., & Patel, A. (2024). Modern Anti-Malware Solutions: Advances and Challenges. *Journal of Cyber Defense*, 30(4), 212-229.

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

Ho, D. (2006). The focus group Interview: Rising to the challenge in focus qualitativeresearch. *Australian Review of Applied Linguistics*, *29*(1), 1–19.

Jansen, J., & Leukfeldt, R. (2016). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License Phishing and Malware Attacks onOnline Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

Kamarulzaman, Y. (2011). A Focus Group Study of Consumer Motivations for e-Shopping:UK versus Malaysia. *African Journal of Business Management*, *5*(16), 6778–6784.

Khan, A., & Sebastian, M. P. (2018). Understanding the Human, Managerial and Organizational Aspects of Information Security Management: A Literature Review. *Indian Institute of Management Kozhikode Working papers*, (225).

Krause, M., & Tipton, H. F. (2002). *Handbook of Information Security Management*. CRCPress.

Krueger, R. A., & Casey, M. A. (2000). *Focus Groups: A Practical Guide for AppliedResearch* (3rd ed.). SAGE PublicationsSage UK: London, England.

Lee, J., & Kim, Y. (2024). Real-Time Database Auditing: Techniques and Benefits. *Database Management Journal*, 27(3), 144-159.

Lewis, M., & Li, Y. (2022). Compliance and Cybersecurity Strategies: A Focus Group Studyon GDPR Impact. *Cyberlaw and Regulation*, 19(2), 45-60.

McGraw, G. (2012). Software security: Building security in. *Datenschutz und Datensicherheit-DuD*, *36*(9), 662-665.

Mughairi, B.M.A, Hajri,H.A., Karim, A. M, Hossain, M. I. (2019). An Innovative Cyber Security based Approach for National Infrastructure Resiliency for Sultanate of Oman. *International Journal of Academic Research in Business and Social Sciences*, 9(3) 1180–1195.

Patel, D., & Kumar, R. (2024). The Importance of Network Segmentation in Cybersecurity. *Network Security Review*, 23(1), 54-68.

Patel, S., & Shah, A. (2023). Advancements in Cryptography and Technical Security. *Journalof Information Security and Privacy*, 16(2), 112-126.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime andDelinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Schneider, B. (1999). *Secrets and Lies: Digital Security in a Networked World*. Wiley.

Singh, N., Brown, J., & Thomas, R. (2023). Next-Generation Firewalls and IDS: Innovationsand Impact. *Cyber Defense Quarterly*, 18(3), 89-104.

Smith, J., Anderson, H., & Green, R. (2023). User Attitudes and Cybersecurity Training:Focus Group Insights. *Journal of Cyber Behavior*, 12(1), 98-115.

Stallings, W. (2013). Network Security Essentials: Applications and Standards. Pearson.

Stewart, D. W. (2018). Focus groups. In *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation* (pp. 687–692). SAGE Publications, Ltd.

Williams, E., Anderson, J., & Roberts, T. (2024). Proactive Vulnerability Management: Best Practices and Strategies. *Journal of Cybersecurity*, 22(1), 67-82.

Zhang, X., Wang, Y., & Liu, J. (2023). Enhancing Database Security through Encryption and Access Controls. *Information Security Journal*, 29(2), 134-150.