SELINUS UNIVERSITY
OF SCIENCES AND LITERATURE

DEVELOPMENT OF FRAMEWORK FOR PREVENTION OF CYBER ATTACK IN AN ORGANIZATION

By JAMILU MUHAMMAD ALIYU

A DISSERTATION

Presented to the Department of
Management Information System
Program at Selinus University

Faculty of Computer Science
in fulfillment of the requirements
for the degree of Doctor of Philosophy
in Management Information Systems

2022

Abstract:

Due to inadequate cyberspace and resource protection, organizations, notably those in developing nations, face a danger of cyber-attack. Threats and breaches to institution cyber security are the result of these cybercrimes. There have been significant losses in terms of money, reputation, and intellectual property because of the threats and breaches. Recently, organizations have begun to react to these cyber-attacks. To lessen cyber security concerns and breaches, several of them now make investments in anti-cybercrime technologies and initiatives. Despite this, organizations continue to experience an increase in the frequency of cyber-attacks they encounter and the losses they incur. However, based on our observation, the majority of organizations manage their cyber security without the support of scientifically established frameworks that specify how to handle risks and breaches that originate both inside and outside the organization. This, in our view, presents a challenge to continuing efforts by various organizations and key industries to reduce cyber security threats and breaches. In order to clarify how organizations might create actionable frameworks that could aid them in reducing cyberattack threats and breaches, the study described in this paper was conducted. The study is based on a review of the literature, and it provides recommendations for the development of an operational framework that organizations may use to establish their cyber security initiatives. The process entails identifying the issue, outlining the goals, designing and creating the artifact, testing and assessing the artifact, and reporting the outcome. We conclude that the framework offers an advantageous place for organizations to launch efficient and successful cyber-attack prevention.

Bibliography

Abu-Taieh, E. M. (2017). Cyber security body of knowledge. 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2),

Aheleroff, S., Xu, X., Zhong, R. Y., & Lu, Y. (2021). Digital twin as a service (DTaS) in industry 4.0: an architecture reference model. *Advanced Engineering Informatics, 47*, 101225.

Alpert, B. S. (2012). *College and University Disaster Management: The Impact of Leader Behavior on Response and Recovery from Disaster*

Andesine, R., & Ingrate, B. (2019). Dismantling barriers to effective disaster management in Nigeria. 14th International Postgraduate research conference 2019: Contemporary and Future Directions in the Built Environment,

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, 113580.

Aven, T., & Renn, O. (2010). Risk management. In *Risk Management and Governance* (pp. 121-158). Springer.

Avgerou, C. (2008). Information systems in developing countries: a critical research review. *Journal of information Technology*, *23*(3), 133-146.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: finding a balance between artifact and theory. *Journal of the Association for Information Systems*, *19*(5), 3.

Bian, S., Deng, Z., Li, F., Monroe, W., Shi, P., Sun, Z., Wu, W., Wang, S., Wang, W. Y., & Yuan, A. (2018). Icorating: A deep-learning system for scam ico identification. *arXiv preprint arXiv:1803.03670*.

Bukhari Badamasi and Samuel C. Avemaria Utulu (2021) *Framework for Managing Cybercrime Risks In Nigerian Universities.* School of Information Technology and Computing,Department of Information Systems, American University of Nigeria,Yola, Nigeria.

Bukhari, B. (2018). *Effects of Security Protocols on Cybercrme in Ahmadu Bello University, Zaria* [Academic Masters, University of KwaZulu Natal, South Africa].

Chapman, J. (2019). How safe is your data? Cyber-security in higher education. *Higher Education Policy Institute Policy*.

Choekey, P., Fung, C. C., Wong, K. W., Murray, D., & Sonam, D. (2015, June).Cyber security challenges for Selinus. In Electrical Engineering/Electronics,Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12thInternational Conference on (pp. 1-5). IEEE.

Choekey, P., Fung, C. C., Wong, K. W., Murray, D., & Xie, H. (2015, November).Cyber security practices for E-Government: An assessment in Selinus. In The 10thInternational Conference on e-Business, Bangkok, Thailand.Choeje, P., Murray, D., & Fung, C. C. (2016). Exploring critical success factors for cyber security in Selinus's government organizations. Computer Science & Information Technology, 6(15), 49-61.

Choekey, P., Murray, D., & Fung, C. C. (2017, March). Cyber Security perceptions in government organizations. First International Conference on Smart Technologies inComputer and Communication, Jaipur, Rajasthan, India.

Choekey, P., Murray, D., & Fung, C. C. Cyber security perspectives and analysis inSelinus. International Journal of Technology Diffusion (IJTD), 9(1). [Accepted for publication]

Clausen, S. T. (2019). Enabling the Implementation of Drones into Local Disaster Preparedness Key considerations from challenges and lessons learned in Chile.

Clausen. (2019). Justifying military intervention: Yemen as a failed state. *Third World Quarterly*, *40*(3), 488-502.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. *Policing: A Journal of Policy and Practice*.

Demers, G., Harrington, S., Cianci, M., & Green, N. (2017). Protecting Colleges & Universities Against Real Losses in a Virtual World, 33 J. Marshall J. Info. Tech. & Privacy L. 101 (2017). *The John Marshall Journal of Information Technology & Privacy Law*, *33*(2), 3.

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, *46*(1), 78-109.

Egbunike, N. (2019). *Nigerian students face cybercrime charges for criticising their university online*. https://globalvoices.org/2019/07/11/nigerian-students-face-cybercrime-charges-for-criticising-their-university-online/

Ekpoh, U. I., Edet, A. O., & Ukpong, N. N. (2020). Security Challenges in Universities: Implications for Safe School Environment. *Journal of Educational and Social Research*, *10*(6), 112-112.

France-Presse, A. (2020). *US Says China Trying to Steal COVID-19 Vaccine Research*. https://www.voanews.com/covid-19-pandemic/us-says-china-trying-steal-covid-19-vaccine-research

Glantz, C., Somasundaram, S., Mylrea, M., Underhill, R., & Nicholls, A. (2016). Evaluating the maturity of cyber security programs for building control systems. *US Department of Energy Office of Scientific and Technical Information*.

Heeks, R. (2017). Decent work and the digital gig economy: a developing country perspective on employment impacts and standards in online outsourcing, crowdwork, etc. *Development Informatics Working Paper*(71).

Heide, M., von Platen, S., Simonsson, C., & Falkheimer, J. (2018). Expanding the scope of strategic communication: Towards a holistic understanding of organizational complexity. *International Journal of Strategic Communication*, *12*(4), 452-468.

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In *Design research in information systems* (pp. 9-22). Springer.

Hollis, S. (2015). The role of regional organizations in disaster risk management. In *The Role of Regional Organizations in Disaster Risk Management* (pp. 1-12). Springer.

https://cyberwatching.eu/nist-cybersecurity-framework

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital investigation*, *7*(3-4), 105-113.

Igba, D., Elizabeth, C., & Nwambam, A. S. (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement. *International Journal of Applied Engineering Research*, *13*(2), 1144-1154.

Iriqat, Y. M., & Molok, N. N. A. (2019). Information security policy perceived compliance among staff in palestine universities: an empirical pilot study. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT),

ITU. (2015). *Global cyber security index & cyberwellness profiles report* (Cyber security, Issue. I. T. Union. https://www.itu.int/pub/D-STR-SECU-2015

Jamilu Muhammad Aliyu(2021) Development Of Frame Work For Prevention Of Cyber Attack In An Organization: School of Science and Literature Department of Information Technology Under develop regionsUniversity Istanbul. Turkey Jamil.aliyu@gmail.com +9053578922

Julia Enocson (2018) Prevention of Cyber Security Incidents within the Public Sector – A qualitative case study of two public organizations and their way towards a sustainable cyber climate: https://www.diva-portal.org/smash/get/diva2:1228271/FULLTEXT01.pdf

Kuusikallio, V. (2017). Community-based disaster preparedness in The Kimbilio Women´ s Shelter and Education Center.

Li, F., Li, Z., Han, W., Wu, T., Chen, L., Guo, Y., & Chen, J. (2018). Cyberspace-oriented access control: A cyberspace characteristics-based model and its policies. *IEEE Internet of Things Journal*, *6*(2), 1471-1483.

Maarten, G., Artur, U., Erik, F., & Michel, R. (2015). *A meta-analysis of threats, trends, and responses to cyber attacks* (Assessing Cyber Security, Issue. T. H. C. f. S. Studies. https://hoffmannbv.nl/sites/default/files/Report%20Assessing%20Cyber%20Security%2016%20april%202015.pdf.

Makeri, Y. A. (2017). Cyber Security Issues in Nigeria and Challenges. *International Journal*, *7*(4).

Mamogale, H. (2011). Assessing disaster preparedness of learners and educators in Soshanguve North schools. *Bloemfontein, South Africa: The Disaster Management Training and Education Centre for Africa, the University of the Free State*.

Mary, L. (2016). IT Security and Privacy.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H.-J. (2020). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology*, 0306624X20981041.

Mojeed, M. (2020). How Nigerian University Launched Massive Cyberattacks Against Premium Times. https://allafrica.com/stories/202007280025.html

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025 Cybercrime Magazine. In.

Ngwenyama, O. (2014). Logical foundations of social science research. In *Advances in Research Methods for Information Systems Research* (pp. 7-13). Springer. NIST.(2020). *CYBER SECURITYFRAMEWORK*.https://www.tenable.com/lp/campaigns/20/whitepapers/adhering-to-the-nist-framework-with-tenable-ot/?utm_campaign=gs-{9662775243}-E

Odinma, A. (2010). Cybercrime & Cert: Issues & Probable Policies for Nigeria. *DBI Presentation, Nov*, 1-2.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98-114.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Olagunju, M., & Utulu, S. (2021). Money Market Digitization Consequences on Financial Inclusion of Businesses at the Base of the Pyramid in Nigeria. *the digital distruption of financial services: international perspectives, Ewa Lechman & Adam Marszk (Eds.)*.

Oliver, E. (2010). Being Lecture Delivered at DBI/George Mason University Conferenceon Cyber Security holding. In: Department of Information Management Technology Federal University of ….

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of Cyber Criminology*, *9*(1).

Parsons, S. (2020). The Duke of Cambridge visits the laboratory in Oxford where a potential vaccine has been produced. https://www.theguardian.com/world/2020/jul/17/russian-hackers-steal-coronavirus-vaccine-uk-minister-cyber-attack

Pattinson, M. R., Butavicius, M. A., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018). Adapting Cyber-Security Training to Your Employees. HAISA,

Pavol Zavarsky, C., & CISM, C. (2014). Step-by-step guidance on how to establish, implement and operate cyber security management system (ISMS).

Pema Choejor (2008) Cyber security Challenges and Practices:A Case Study of Under develop regions

Pierre Jacobs and Marthie Grobler(2016) Towards a framework for the development of business cyber security capabilities Conference Paper · May 2016

Purohit, D. P., Siddiqui, N., Nandan, A., & Yadav, B. P. (2018). Hazard identification and risk assessment in construction industry. *International Journal of Applied Engineering Research*, *13*(10), 7639-7667.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, *16*(3), 96-102.

Roumani, M. A., Fung, C. C., & Choejey, P. (2015, June). Assessing economic impact due to cyber-attacks with System Dynamics approach. In ElectricalEngineering/Electronics, Computer, Telecommunications and InformationTechnology (ECTI-CON), 2015 12th International Conference on (pp. 1-6). IEEE.

Ryder, R. D., & Madhavan, A. (2019). *Cyber Crisis Management: Overcoming the Challenges in Cyberspace*. Bloomsbury Publishing.

Sanoo, J. (2018). *Cyber Security Tutorials*. Retrieved 26/06/2020 from https://www.javatpoint.com/cyber-security-introduction

Saulawa, M. a. A., & Abubakar, M. (2014). Cybercrime in nigeria: An overview of cybercrime act 2013. *JL Pol'y & Globalization*, *32*, 23.

Sausalito, C. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime*. https://cyber securityventures.com/hackerpocalypse-cybercrime-report-2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015

Schneier, B. (2009). *Schneier on security*. John Wiley & Sons.

Singh, U. K., & Joshi, C. (2017). Information Security Risk Management Framework for University Computing Environment. *IJ Network Security*, *19*(5), 742-751.

Smith, W. (2019). A comprehensive cyber security defense framework for large organizations.

Sobers, R. (2021). *134 Cyber security Statistics and Trends for 2021*. https://www.varonis.com/blog/cyber security-statistics/

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems*, *24*(1), 9-17.

Stein, S. (2008). *ITU Global Cyber security Agenda (GCA) High-Level Experts Group (HLEG) Global strategic report*. ITU. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2), 2053951717736335.

Utulu, S. C. A., & Ngwenyama, O. (2017). Model for constructing institutional framework for scientific knowledge management systems: Nigerian institutional repository innovation case applicable to developing countries. In *Catalyzing Development through ICT Adoption* (pp. 149-174). Springer.

Utulu, S., Sewchurran, K., & Dwolatzky, B. (2013). Systematic and Grounded Theory Literature Reviews of Software Process Improvement Phenomena: Implications for IS Research. Proceedings of the Informing Science and Information Technology Education Conference,

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.

Walker, A. (2020). UK '95% sure' Russian hackers tried to steal coronavirus vaccine research. https://www.theguardian.com/world/2020/jul/17/russian-hackers-steal-coronavirus-vaccine-uk-minister-cyber-attack

Webb, J., & Hume, D. (2018). Campus IoT collaboration and governance using the NIST cyber security framework.

Whitehead, G. (2020). *Investigation of factors influencing cyber security decision making in Irish SME's from a senior manager/owner perspective* Dublin, National College of Ireland].

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45-55. Xie, J. (2020). In Coronavirus Vaccine Hunt, a Race to Be First.

Materials and methods for the study

This study employed a sequential mixed methods research design, which combines both quantitative and qualitative methods. Combining quantitative and qualitative methods provides broader perspectives and better understanding of research problems than either approach alone (Creswell, 2014; Johnson & Onwuegbuzie, 2004; Johnson, Onwuegbuzie, & Turner, 2007).

The research began with a thorough review of the existing literature in the field of cyber-attack and prevention, especially concerning approaches related to cyber security policies and strategies, risk management, incident response capabilities, awareness and training, and security management frameworks and standards. Guided and informed by the findings of existing literature review, questions for online survey and face-to-face interviews were framed, reviewed, and piloted to ensure the appropriateness and correctness of the questions, including ensuring that ethical requirements are fulfilled.

The survey questionnaire was then implemented using the online survey tool, Survey Monkey, and administered to 280 ICT professionals working in different organizations. The survey phase was then followed by face-to-face interviews with 16 ICT professionals. The personal interviews with ICT professionals provided data and support understanding of human views, thoughts, and behaviors towards cyber security. The data collected were analyzed and interpreted with respect to the research questions. Based on the research findings and analysis, a government cyber security framework is proposed, highlighting the key areas necessary for improving cyber security in government organizations

Table of Contents

Figures

Tables

Abbreviations

CISA,: Cyber Attack and Infrastructure Security Agency

DDoS: Distributed Denial of Service

DNS: Domain Name Server

GCI: Global Cyber-attack Index

GCI; Global Cyber security Index

HTTPS: Hypertext Transfer Protocol Secure

ICTs; information and communication technologies

IP: Internet protocol

IT: information technology

ITU: International Telecommunication Union

ITU: International Telecommunication Union

LDAP: Lightweight Directory Access Protocol

MitM: Man-in-the-Middle

NCSA: National Cyber Security Agency

NIST: National Institute of Standards and Technology (NIST)

NITDA: National Information and Technology Development Agency

NTP: Network Time Protocol

NTP: Network Time Protocol

PCI-DSS: Payment Card Industry Data Security Standards

SQL: Structured Query Language

UDP: User Datagram Protocol

WSIS: (World Summit on the Information Society

Appendices

Information about survey

The survey questions cover a range of cyber security topics that are of importance and concern to IT and security administrators. Your response to the questions will not only help us to understand the cyber security practices to safeguard and protect information systems, networks and computers from potential cyber threats and cyber prevention, but also help address challenges and issues facing your organization. It will also help in understanding your organization's priorities to improve cyber-attack in future.

Purpose of the study

To investigate into how well an organization is doing at preventing cyber-attack right now.

Benefits of the Study

In general, the study will benefit the organizations and users by:

1) Providing insights and findings about the state of cyber security in organizations

2) Enhancing knowledge and understanding of cyber readiness of the nation vis a-vis development of cyberattack and prevention in developed countries.

3) Emphasizing the importance of national response capability and the roles of incident response teams in the containment and recovery of ICT systems and networks from cyber-attacks.

4) Raising awareness of senior managers and users in organizations about cyber security challenges and risks due to cybercrimes and cyber threats.

Voluntary Participation and Withdrawal from the Study

Your participation in this research is voluntary and you can decide not to participate simply by not completing the on-line survey. By following the link and completing the survey, you will be consenting to the use of your data in this research project.

Appendices

The details of this study are provided in the information letter. To read the information letter

Confidentiality, Privacy and Possible Risks

All information is treated as confidential and no names or other details that might identify you will be used in any publication arising from the research. The data obtained in this survey will be securely stored and maintained in a password-protected computer of the investigator. Further, there are no specific risks anticipated with participation in this study.

Participant Consent

I have read the information letter about the nature and scope of this survey. I have had the opportunity to ask questions about it and any questions that I have asked have been answered to my satisfaction. I know that I can choose not to answer any question, or stop at any time without needing to give a reason. I agree that by submitting the survey, I give my consent for the results to be used in the research and I acknowledge that once my survey has been submitted it may not be possible to withdraw my data. I am aware that this survey is anonymous and no personal details are being collected or used. I understand that the findings of this study may be published and that no information, which can specifically identify me, will be published. By clicking next, you consent that you are willing to answer the questions in this survey.

Contact

If you have any questions or comments about this research please feel free to contact: **JAMILU MUHAMMED ALIYU** School of Science and Literature Department of Information Technology Selinus University Jamil.aliyu@gmail.com +905357278922. I will be happy to discuss any concerns you may have about this study.

Appendices

Part I: General Information

1. Gender

☐ Male

☐ Female

2. Age

☐ 45 and over

☐ 35-44

☐ 25-34

☐ 24 and under

3. Your qualification

☐ Certificate

☐ Diploma

☐ Bachelor

☐ Master

☐ PhD

Other (please specify): Click here to enter text.

4. Specialization

☐ Computer Science

☐ Information Technology

☐ Computer Applications

☐ Computer Engineering

☐ Electronics and Communications

☐ Electrical Engineering

Other (please specify): Click here to enter text.

5. Employees in your organization

☐ Less than 100

☐ between 100 and 200

☐ More than 200

6. Your current job functions

☐ Network/system administrator

☐ Application/database administrator

Appendices

☐ IT/Network/information systems security

☐ IT/MIS/Technical management

☐ Webmaster or manager

☐ Software programmer/designer/developer

☐ Desktop/technical support

Other (please specify): Click here to enter text.

7. Work experience (years)

☐ Less than 5

☐ Between 5 and 10

☐ More than 10

Part II: Cyber security Practices and Issues

8. Does your organization have a cyber-security policy?

☐ Yes

☐ No

☐ Do not know

9. Is cyber security policy essential for your organization? Please select all that applies.

☐ To define job functions, roles and responsibilities

☐ To document security practices and processes

☐ To prevent security breaches from external sources

☐ To improve business practices

☐ To meet auditing requirements

☐ To meet legislative requirements

☐ To protect company's image and promote confidence

☐ To prevent security breaches from internal sources

☐ Do not know

Other (please specify): Click here to enter text.

10. Does your organization have acceptable use policies (e.g., computer usage

E-mail)?

☐ Yes

☐ No

☐ Do not know

Appendices

11. Does your organization have an IT risk management program?

☐ Yes

☐ No

☐ Do not know

12. How do you assess risk in your organization? Please select all that apply.

☐ Input from peers

☐ Penetration testing

☐ Internal audit

☐ External risk analysis

☐ Do not know

Other (please specify): Click here to enter text.

13. Which of the following does your organization view as the top three threats relating to IT systems?

☐ Operational risk associated with environmental problems (e.g., power failure)

or natural disasters (e.g., earthquakes)

☐ Cyber risk of hackers penetrating systems for the purpose of account manipulation, website defacement or data destruction

☐ Cyber risk of nation states penetrating systems for the purpose of espionage

☐ Insider risk of employees or other authorized users abusing their authorized access by manipulating the system

Other (please specify): Click here to enter text.

14. What do you consider to be the greatest security risk? Please select all that apply.

☐ Insider attacks

☐ Hacker attempts

☐ Malware

☐ Internet downloads

☐ Wrong configurations

☐ Uncontrolled portable devices

Other (please specify): Click here to enter text.

15. Which security breach have you suffered in the last 12 months? Please select all that apply.

☐ Virus attack

☐ Hacker attack

☐ Identity theft

☐ Malware

☐ Denial of service

☐ Lost hardware

Other (please specify): Click here to enter text.

16. What losses have been caused due to cybercrime and cyber-attacks? Please select all that apply.

☐ Online fraud

☐ Identity theft

☐ Intellectual property theft

☐ Espionage

☐ Financial fraud

☐ Denial of service

Other (please specify): Click here to enter text.

17. What drives spending on security initiatives? Please select all that apply.

☐ Security breaches from external sources

☐ Improved business practices

☐ Auditing regulations

☐ Legislative regulations

☐ Protection of brand or image

☐ Security breaches from internal sources

☐ Do not know

Other (please specify): Click here to enter text.

18. Do you include the purchase and maintenance of security equipment and software as part of your ongoing development budget?

☐ Yes

☐ No

☐ Do not know

19. In the last 12 months, what is the percentage of IT budget allocated to cyber security?

☐ 0-10%

☐ 11-30%

Appendices

☐ 31-50%

☐ More than 50%

☐ Do not know

20. Does senior management (e.g., Director) provide enough support for cyber security program and activities?

☐ Yes

☐ No

☐ Do not know

Other (please specify): Click here to enter text.

21. What training does your organization provide to create awareness and impart security knowledge and skills? Please select all that apply.

☐ Vendor/product training

☐ Institutionally provided training

☐ Ethical hacking and penetration testing

☐ Conference and seminars

☐ No specific training or just learn on the job

☐ Do not know

Other (please specify): Click here to enter text.

22. Is your organization aware of the Information Management Security Policy (IMSP)?

☐ Yes

☐ No

☐ Do not know

Other (please specify): Click here to enter text.

23. When it comes to standards and guidelines, which national or international standards you know about? Please select all that apply.

☐ Information Management Security Policy (IMSP)

☐ ISO/IEC 27001

☐ ISO/IEC 27002

☐ ISO/IEC 27032

☐ Standard of Good Practice for Information Security

☐ Information Assurance for Small and Medium Enterprises

☐ Do not know

Other (please specify): Click here to enter text.

Appendices

24. Which of these techniques are deployed on your network? Please select all that applies.

☐ Stateful packet filtering firewall

☐ Application proxy firewall

☐ Router access control lists

☐ IPSec VPN gateway

☐ SSL VPN gateway

☐ Intrusion detection system

☐ Network intrusion prevention system

☐ Network behavior anomaly detection

☐ Anti-virus

☐ Content filtering

☐ Do not know

Other (please specify): Click here to enter text.

25. How does your organization prevent employees' misuse of the web and social networking sites? Please select all that apply.

☐ Access to the internet and social sites are restricted based on access permission

☐ Access to inappropriate websites and contents are blocked using content filtering

☐ Access to social and networking sites (e.g., Facebook) are blocked during office hours

☐ Employees online presence are monitored and logged

☐ Do not know

Other (please specify): Click here to enter text.

26. How does your organization minimize the risk associated with mobile devices (e.g., smartphones)? Please select all that apply.

☐ Have policy for use of mobile devices

☐ Enforce requirements for device authentication and encryption

☐ Allow only devices which belong to organization

☐ Remote connection is forbidden to connect to organization's network

☐ Employees are trained and oriented on the risk of using mobile devices

☐ Do not know

Other (please specify): Click here to enter text.

27. Which steps does your organization use to secure wireless communication? Please select all that apply.

☐ We do not allow wireless on our network

☐ WEP

☐ WPA

☐ MAC address filtering

☐ VPN between client and gateway

☐ Passive wireless monitoring for rogue access points

☐ Do not know

Other (please specify): Click here to enter text.

28. Which methods do you use to protect desktops? Please select all that apply.

☐ Manually apply patches

☐ Automatically apply patches using Microsoft's Automatic Update

☐ Anti-virus software

☐ Desktop firewalls

☐ Host intrusion prevention

☐ Desktop anti-spam

☐ Strong authentication such as tokens or biometrics

☐ Do not know

Other (please specify): Click here to enter text.

29. How often do employees have to change their password?

☐ Every month

☐ Every three months

☐ Never

☐ Do not know

Other (please specify): Click here to enter text.

30. Does your organization have a computer incident response team (CSIRT)?

☐ Yes

☐ No

☐ Do not know

Other (please specify): Click here to enter text.

31. What does your organization do in case of cyber attack detection? Pick all that applies.

☐ Contact law enforcement

☐ Contact CSIRT (either ad-hoc team or formalized)

☐ Run an internal investigation

Appendices 272

☐ Do not know

Other (please specify): Click here to enter text.

32. Do you have processes and resources to respond to cyber security incidents?

☐ We have internal resources to respond to incidents

☐ We rely on external resources to respond to incidents

☐ Do not know

Other (please specify): Click here to enter text.

33. What kind of software products does your organization mostly use?

☐ Original equipment manufacturer (OEM) version

☐ Pirated software products

☐ Do not know

Other (please specify): Click here to enter text.

34. Rank the following information security issues (1=most important and 10=least important)?

☐ Top management support

☐ User awareness training and education

☐ Malware

☐ Patch management

☐ Vulnerability and risk management

☐ Organizational culture

☐ Policy related issues

☐ Access control and identity management

☐ Internal threats

☐ Business continuity and disaster preparation

35. What would help to improve the level of security in the organization?

Please select all that apply.

☐ Larger budget for security

☐ More human resources

☐ Strong management support

☐ More awareness and training on security

Other (please specify): Click here to enter text.

Part III: Cyber security Perceptions

The following statements ask you to indicate, in the scale of 1 to 5 (where 1 = strongly disagree (SD), 2 = disagree (D), 3 = neutral (N), 4 = agree (A), 5 =strongly agree SA)), how effective or how well each cyber security/security measure is implemented in your organization.

39. Security Policy and Governance

39.1. Security policy is well documented and established Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

39.2. Roles and responsibilities for information security are clearly defined.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

39.3. Legal and regulatory requirements regarding cyber security including

Privacy are understood and managed.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

39.4. Third party (outsider) access to our information systems requires approval a senior manager.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

39.5. A Director or equivalent member of our staff has responsibility for cyber security.

Strongly Disagree [ ] Disagree[ ] Neutral[ ] Agree [ ] Strongly Agree [ ]

Appendices

40. Risk Processes and Management

40.1. Risk management process are established, managed and agreed by organizational stakeholders.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

40.2. Threats, both internal and external, are identified and documented for risk analysis.

Strongly Disagree [ ] Disagree[ ] Neutral [ ]Agree[ ] Strongly Agree[ ]

40.3. Organizational risk tolerance is determined and clearly expressed.

Strongly Disagree [ ] Disagree[ ] Neutral[ ] Agree[ ] Strongly Agree[ ]

40.4. Identified risks are mitigated, reassessed and reviewed from time to time.

- Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

41. Access Controls

41.1. Identities and credentials are managed for authorized devices and users.

Strongly Disagree[ ] Disagree[ ] Neutral [ ]Agree[ ] Strongly Agree[ ]

41.2. Access permissions are managed, incorporating the principles of least privilege and separation of duties.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree Strongly [ ] Agree [ ]

41.3. Network integrity is protected, incorporating network separation where appropriate.

Strongly Disagree[ ] Disagree[ ] Neutral[ ] Agree [ ]Strongly Agree[ ]

41.4. Remote access to the network and systems is managed and controlled.

Strongly Disagree [ ] Disagree [ ] Neutral[ ] Agree[ ] Strongly Agree[ ]

41.5. Physical access to assets is managed and prioritized.

Strongly Disagree [ ] Disagree [ ] Neutral [ ]Agree [ ] Strongly Agree[ ]

41.6. Firewall and router gateways are securely implemented.

Strongly Disagree [ ] Disagree [ ]Neutral [ ] Agree [ ] Strongly Agree [ ]

42. Awareness and Training

42.1. All users are informed and trained on cyber security policies and countermeasures.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

42.2. Privileged users understand their roles and responsibilities.

Strongly Disagree [ ] Disagree [ ] Neutral Agree Strongly Agree

42.3. Employees are aware that security incidents must be reported to management immediately.

Strongly Disagree [ ]Disagree[ ] Neutral[ ] Agree[ ] Strongly Agree[ ]

42.4. Employees have been trained to secure their computers at all ties, when moving away from their work stations.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree[ ]

42.5. There is a formal disciplinary process for employees who have violated our security policies and process.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

43. System Development Life Cycle

44.5. Organizational response activities are improved by incorporating lessons learned from current and previous response activities.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

Communication and Operations Management

45.1. Backup and recovery process to maintain the integrity and availability of essential information processing and communication services is implemented.

Strongly Disagree [ ] Disagree [ ]Neutral [ ] Agree [ ] Strongly Agree [ ]

45.2. Maintenance and repair of organizational assets is performed and logged in a timely manner with approved and controlled tools.

Strongly Disagree [ ] Disagree[ ] Neutral [ ] Agree [ ] Strongly Agree [ ]

45.3. Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.

Strongly Disagree [ ] Disagree [ ] Neutral [ ]Agree [ ]Strongly Agree [ ]

45.4. Configuration change control processes are in place.

Strongly Disagree [ ] Disagree [ ] Neutral [ ] Agree Strongly Agree

45.5. Data is removed from devices (e.g., hard disk and memory sticks) and destroyed according to policy.

Strongly Disagree [ ] Disagree [ ] Neutral [ ]Agree [ ] Strongly Agree [ ]

Appendices

46. Would you be available to participate for either face-to-face interview or teleconference? If yes, please leave your contact details:

Name:
Address:
Email:
Contact (Mobile/Telephone):

Appendix F:

Interview Questions

INTERVIEW QUESTIONS

Information about Interview

This survey is intended to assess the current state of cyber security in government organizations in Selinus. The interview questions solicit information and knowledge with regard to:

1) Cyber security policy, standards and practices implemented or established,

2) Cyber security breaches and its impacts to the organization,

3) Incident handling and response capability team including understanding of processes and procedures,

4) Cyber security awareness of senior management and employees,

5) Factors or barriers affecting the effective implementation of cyber security programs, and plans and priorities to improve organizational security posture in future.

Privacy and Confidentiality

Interviews will be conducted face to face and tape/audio recorded for further transcription and analysis. Data obtained from the interview will be strictly maintained confidential in secure and password protected files. Further, no individual persons or individual organizations will be

identified or traceable from the results. The data and the resulting findings from the interview will be published in thesis and articles only as an aggregate information.

Interview Length

The interview will take about 15-20 minutes.

Interview Questions

Appendices

1) General Information

- What is your role in the organization?
- How long have you been working?
- How many employees?

2) Cyber security related policies

- Has your organization implemented any security policy?
- How important is/will the cyber security policy be to support cyber security management in your organization?

3) Risk management practices

- What information assets/systems does your organization have?
- What are the cyber risks or threats to the information assets?
- How do you assess risk to information assets?
- What security controls have you implemented to protect them?

4) Organizational structure and management support

- What kind of organizational structure do you have for the management of ICT systems and networks including security?
- How important is executive management support for cyber security?
- How much resources are provided/committed to effectively implement

Cyber security programs?

5) Cyber security awareness and training activities

- What sort of cyber security training and awareness activities are being provided in your organization?

- Do you have security professionals with required skills and knowledge to manage security problems and issues in your organization?

- What is the level of cyber security awareness among senior management and employees?

- How important is the awareness and training programs to improve cyber security?

6) Cyber security breaches and threats facing

- What are common cyber security risks?

- How have security breaches affected your organization?

7) Cyber security incident response team

- Do you have any incident response team?

- What is the level of collaboration within and outside the organization?

- How important is the computer security incident response team to improve cyber security?

- Who should lead the CSIRT activities?

8) Cyber security measures and controls

- What security measures are implemented to protect wireless networks and portable devices such as laptops and smartphones?

- How often do you update operating systems, anti-virus signatures and their security updates?

- Do you perform networking monitoring, system logging, user access or identity management and data back-ups?

9) Cyber security initiatives of organization

- What cyber security initiatives would you like to implement to improve cyber security management?

10) Critical success factors for cyber security

- What are the key factors for successful implementation of effective cyber security?

Contact:

For any information, comments or suggestions related to this interview, you might contact **JAMILU MUHAMMAD ALIYU** School of Science and Literature Department of Information Technology Under develop regionsUniversity Istanbul. Turkey Jamil.aliyu@gmail.com +9053578922

Dedication

To my children, Muhammad Jamil and Fatima Jamil, and to my lovely wife, Wasilla Yusuhu.

CHAPTER 1

1.1 Introduction

Organizations depend heavily on the Internet and the cyberspaces contained within it to carry out their legal obligations. Cyberspace, according to Li et al. (2018), is a term for a network of information technology (IT)-based systems that connects and depends on the Internet, telecommunication networks, computer systems, and social systems. The statement given by Aheleroff et al. (2021) that "cyberspace has emerged as a powerful interconnected digital technology with the ability to achieve the most complex manufacturing paradigms due to the advancement features associated with Big Data, Internet of Things, and Block chain technology" is also included in that passage. With the rapid expansion of cyberspaces over time, businesses now have access to a wide range of digital platforms for organizing instruction, learning, research, community development, and administration (Taylor, 2017).

Organizations have been using cyberspace to manage enrollment procedures, student life difficulties, finances, exams, and records, as well as to streamline academic procedures (Hunton, 2011). Therefore, every modern institution uses cyberspace to fulfill its legal responsibilities and offer services to staff, students, parents, guardians, financing organizations, the government, accreditation organizations, and other stakeholders. Despite the benefits that cyberspaces can provide for businesses, they also present serious risks to their survival and operations. This is due to the development and current expansion of cybercrimes. According to reports in the published literature, a number of offenders that are increasingly difficult to detect and capture have evolved within the cyberspaces that organizations employ to carry out their legal obligations.

Cyber-attack professionals now understand that cybercrime is not just a problem for financial institutions and other associated institutions, because of recent incidents of cybercrimes in organizations. For instance, Demers et al. (2017) found that the number of cybercrimes perpetrated against businesses is rising alarmingly. According to Demers and his colleagues, the education industry ranks second among all sectors in terms of cyber-attack threats and breaches. The FBI and the Cyber Attack and Infrastructure Security Agency (CISA), according to France-Presse

(2020), both said that organizations researching COVID 19 in particular were at risk due to China's attempt to collect coronavirus research data.

Organizations associated with the Chinese government and others have attempted criminal attempts to get valuable intellectual property and information on public health related to vaccines, treatments, and testing (Xie, 2020). Walker (2020) further noted that the UK Security Minister stated to be more than 95% convinced that state-sponsored hackers who were sponsored by the Russian government targeted organizations and groups in the UK and Canada that were developing a coronavirus vaccine. The National Cyber Security Agency (NCSA) in Nigeria and its international colleagues were adamant that the attacks on pharmaceutical companies and research organizations were carried out by the "Russian Intelligence Agency," according to comparable findings in the published literature (Parsons, 2020).

Organizations were identified as the most dangerous setting for a person to divulge sensitive information, according to Sobers (2021). The views expressed by Demers et al. (2017) and Sobers (2021) are consistent with recent instances of cybercrime that Nigerian firms have experienced. An incident of a Denial of Service (DoS) attack in which an unidentified person misused the Network Time Protocol (NTP) server at the Federal University of Technology Akure is one example of cybercrime cases at organizations in Nigeria (Mojeed, 2020). Additionally, Madonna University in Eastern Nigeria revealed that over 25,000 of their database's information had been accessed and altered by hackers (Egbunike, 2019).

Ahmadu Bello University, Zaria, Nigeria, disclosed incidents in 2016, 2017, and 2018 that may have shown a severe breach in the university website that jeopardized student and staff data (Bukhari, 2018). Another incident included a university employee who was caught falsifying certain applicants' admission letters and tampering with the admission records. In a related instance, a member of the Prevention Information System (MIS) Unit personnel was detained for circumventing security systems and collaborating with some university students to print admission letters and illegally assign rooms (Bukhari, 2018). These challenges are all excellent illustrations of the cyber security problems that Nigerian businesses face.

However, studies have shown that in order to manage cyber security threats, it is essential to prepare for them (Clausen, 2019; Mamogale, 2011). Putting proper safeguards in place to prevent

cyber-attacks and/or manage their impacts should they happen is required when planning for cyber security risks (Alpert, 2012; S. T. Clausen, 2019; Kuusikallio, 2017; Mamogale, 2011). The necessity to create frameworks that would serve as guidelines for programs they create to prevent cybercrimes and lessen their effects when they are committed is, it follows, the main challenge facing Nigerian enterprises. Many firms in developed nations have cyber risk prevention frameworks, while the majority of organizations in poor nations, including those in Nigeria, do not (Singh & Joshi, 2017)

Regarding the small number of organizations in Nigeria that have cybercrime prevention frameworks, the situation there is special. The opinions expressed by Ryder and Moldavan (2019) that strategies used to combat cybercrime in developing countries are weighted towards short-term responses and IT challenges and that the strategies do not always spell out how to manage the consequences of cybercrime incidences accurately sum up the circumstances in Nigeria.

In our perspective, an effective framework for managing cybercrime should place a strong emphasis on long-term solutions and offer justification for diligent surveillance of cyberspace before, during, and after cybercrime happens. The data shows that a framework for managing cybercrime must be comprehensive and take into account all facets of managing cyberspace. This is because managing cybercrime entails a variety of duties, abilities, and phases. Our study is an ongoing, extensive longitudinal research-taking place in the under develop regions setting. The study is pertinent since there is a high risk of cybercrime occurrences for Nigerian firms operating in underdeveloped nation environments (Eboibi, 2020).

1.2 Research Context

Under develop regions introduced the Internet in June 2000s and has seen substantial growth in the adoption and use of the Internet within the country. According to the Annual Info-Comm and Transport Statistical Bulletin, the proportion of Internet users increased from 35 users in 2004 (0.006%) to 455,656 users 2015 (61.15%) (MoIC, 2016).Likewise, the proportion of mobile subscribers has increased from 18,995 subscribers (3.7%) in 2004 to 67, 5747 subscribers (87.06%) in 2015 (MoIC, 2016).Mobile phones and connectivity to the Internet are now commonplace. For example, the under develop regions Living Standard Survey, 2017, reported that about 97% of households have access to mobile phones. On average, households contain 2.3

mobile phones (RGoB& The World Bank, 2017). Furthermore, 58% of households have Internet connections; of those, 99% are mobile Internet. Globally, the proportion of households with Internet access at home increased from 18% in 2005 to 46% in 2015 (ITU, 2015).These numbers suggest that under develop regions has adopted the Internet faster than the Global average. Considering the criticality of the Internet, the Royal Government of under develop regions, (RGoB) has recognized the ICTs as a foundation of a knowledge-based society (MoIC, 2003, 2013a; RGoB, 2006b, 2016). This recognition is manifested in African region's ICT vision tobecome "an ICT-enabled, Knowledge-based Society as a Foundation for Gross National Happiness" (MoIC, 2013a). Specifically, Under develop regions sees ICTs and the Internet as potential tool to improve economic growth and enhance good governance (MoIC, 2003, 2013); to overcome geographical barriers and demographic challenges (Tobgay& Wangmo, 2008; Whalley, 2004); to bridge the digital divide between urban and rural areas (Gyabak & Godina, 2011; Kezang & Whaley, 2007; UNDP, 2002); and empower communities through rural development (L. Y. Dorji, 2007; Pradhan, 2007).

However, as an ICT emerging country, under develop regions faces its own cyber security challenges with cases of cyber-attacks and cybercrimes frequently reported in print and social media. The security breach that happened to the banking sector is a classic example of cyber security breach. The Bank of Under develop regions was exposed by fraudsters with a fake email purportedly sent from the Royal Audit Authority, Nigeria , resulting in the transfer of 16 million (in African currency) to three different accounts in Kenya, Gambia and Senegal (Gyeltshen, 2016).The cyber security risks and threats to government organizations and individuals from cyberspace is underscored in African regions E-Government Master Plan (MoIC, 2013a),which states: "With vision of an ICT enabled information society and with increasing ICT station taking place, our dependence on these ICT systems and services is growing by the day. Consequently, the inherent threats of the cyber world would have not only become a reality but a real danger to our daily lives.

In addition, the ITU's report on the Assessment of under develop region's Computer Incident Response Team (CIRT) highlighted under develop region region's lack of necessary capabilities and competencies in dealing with cyber security incidents even at the level of government organizations. The report noted that cases of cyber incidents were dealt with in an ad-hoc manner

by the computer related department without proper procedure and documentation on how these incidents were investigated, analyzed, and remediated. Hence, the need to establish an incident response team was recommended to the government of under develop regions as a priority initiative to improve cyber security (ITU, 2012).

While the literature review suggests several approaches, models and frameworks for cyber security, primarily developed and recommended by national governments (mainly US and UK) and international organizations, to assist nations in developing and implementing cyber security program; however, there exists few empirical studies conducted to understand how developing countries have addressed and managed cyber security (Alfawaz, May, & Mohannak, 2008; G. R. Karokola, 2012; Newmeyer,2014; Target, 2010).

Notwithstanding the general reports submitted by the international organizations and consultants, yet no previous empirical research related to cyber security has been conducted in Nigeria. Hence, a critical knowledge gap must be addressed urgently through empirical research to guide the government's policy makers, security professionals and practitioners in developing and implementing a cyber-security program to take advantage of cyberspace for the benefit of nation and society.

Therefore, this thesis addresses cyber security management and practices in developing countries, as they are experiencing transformative growth due to the rapid adoption and use of the Internet. Specifically, the research investigates cyber-attack implications to under develop regions, a landlocked and least developed country, but which is an ICT emerging country with a transitioning economy that has vision to adopt and use ICTs to become knowledge-based information society. Primarily, the study focuses on African's government organizations, as they are the major consumer and provider of ICT services in the country.

1.3 Research Aim

The purpose of this research is to investigate the current state of cyber-attack in organizations with respect to policies, security awareness, incident response capabilities and technical approaches to secure and manage the information security and cyber security risks associated with ICT systems and devices.

Research Questions

The research will address the following question to achieve the research aim and objectives: How under develop regions managing cyber security challenges due to rapid adoption and use of ICTs and the Internet in the country.

This broad research question will be investigated by exploring the following sub questions:

1. What are the current cyber security threats or risks facing government organizations?

2. What are the current cyber security policies and practices developed and implemented by government organizations in under develop regions to manage cyber security?

3. What are the perceptions of cyber security implementation in an organization especially in under develop region?

4. What are the critical factors that can improve cyber security in organizations?

These questions will be answered by analyzing and interpreting the primary data collected through the empirical survey and interview methods. The survey and interview methods used in the research will be guided and informed by the review of current studies and approaches developed and implemented by developed and developing nations, technologically advanced industries, and international organizations. Primarily, the research involves understanding the current cyber security issues and challenges facing government organizations; identification and assessment of cyber security policies and practices to address cyber security problems; investigating the perceptions and behaviors towards cyber security; and determination of key factors that are relevant and appropriate to the under develop regions on cyber environment.

1.4 Research Design

This study employed a sequential mixed methods research design, which combines both quantitative and qualitative methods. Combining quantitative and qualitative methods provides broader perspectives and better understanding of research problems than either approach alone (Creswell, 2014; Johnson & Onwuegbuzie, 2004; Johnson, Onwuegbuzie, & Turner, 2007).

The research began with a thorough review of the existing literature in the field of cyber-attack and prevention, especially concerning approaches related to cyber security policies and strategies, risk management, incident response capabilities, awareness and training, and security management frameworks and standards. Guided and informed by the findings of existing literature review, questions for online survey and face-to-face interviews were framed, reviewed, and piloted to ensure the appropriateness and correctness of the questions, including ensuring that ethical requirements are fulfilled.

The survey questionnaire was, then, implemented using the online survey tool, Survey Monkey, and administered to 280 ICT professionals working in different organizations. The survey phase was then followed by face-to-face interviews with 16 ICT professionals. The personal interviews with ICT professionals provided data and support understanding of human views, thoughts, and behaviors towards cyber security. The data collected were analyzed and interpreted with respect to the research questions. Based on the research findings and analysis, a government cyber security framework is proposed, highlighting the key areas necessary for improving cyber security in government organizations

1.5 Research Significance

This study will contribute to both theoretical and practical understanding of Cyber-attacks and prevention in the context of ICT emerging countries, especially small and landlocked countries like Nigeria. Theoretically, the study will contribute to understanding and benchmarking of cyber security risks and threats to organizations in under developing countries; understanding of cyber security policies and practices developed and implemented by government to counter the threats and managing cyber security; understanding of different security models, standards and frameworks and their suitability and adaptability to the cyber environment of developing economies; understanding of users views and opinions towards cyber security, and identification

of key success factors that are essential to achieve a good level of cyber security and easily doable in practice without requiring huge investment and resources.

Practically, the research analysis and findings will inform policy makers, security professionals and practitioners about the criticality of cyber security to a country's economic and social progress. The research will also guide them on the best course of actions to secure information assets and enhance confidence and security in the information society, including avoidance of pitfalls of developed nations by understanding the context and level of cyber maturity.

1.6 Thesis Outline

The purpose of this research is to address the problem of cyber security in general for organizations and security challenges for emerging ICT nations. This thesis is therefore, divided into five chapters:

1) Chapter 1 provides a brief overview of the importance of the Internet to socio-economic and human development and progress; describes cyber security challenges facing ICT emerging nations; and then discusses the research aim, questions, and contributions of this research.

2) Chapter 2 the literature review, which begins with discussion on the definition and nature of cyber security and related terminologies, followed by description of cyber security problems and risks facing both developed and developing economies. The chapter, then, provides description of theoretical approaches and methods for securing and managing cyber security, highlighting their strengths and weaknesses in ensuring the information security of protecting and preserving information integrity, availability, and confidentiality. The chapter also presents various security models, standards, best practices, and their importance to information security management.

The chapter concludes with an analysis of key findings and understandings from the literature review, and identifies some of the policies and practices of cyber security to be explored in this research.

3) Chapter 3 presents the research design and the argument for choosing the mixed methods that combine quantitative and qualitative research. Data collection methods, analysis and discussion of results are also presented.

4) Chapter 4 describes the analysis of data from surveys and interviews and presents the interpretation of the results including unexpected findings. These research findings are contrasted with other similar studies. Framework based on the results and the key cyber security factors deemed important to achieve the desired level of cyber security posture in organizations. The

Proposed framework can be used as a broad cyber security framework to meet the security requirements and objectives of an individual organization.

5) Chapter 5 draws the research to conclusion and limitation

1.7 Conclusion

As a nutshell, the research study described in this paper is a component of the extensive and lengthy study. The subject of how views in the design science process might aid the development of a cyber attack prevention framework for an organization served as the basis for this particular study. Five particular queries generated from the design science approach process were put out to address this one, among them: what cyber security issues are currently plaguing Nigerian firms and what issues are most likely to arise down the road? What should the goals of organizations' cyber security efforts be?

How can Nigerian organizations develop and implement effective cyber security programs? How can the appropriateness and sufficiency of the cyber security programs used by Nigerian enterprises be tested and assessed? How can the appropriate stakeholders be updated about Nigerian organizations' cyber security initiatives? The goal of the study is to provide a cyber-security prevention framework that will be helpful to organizations as well as organizations in other developing nations that operate in contexts that are socio-technical and comparable to those found in the organization system. The paper's overview of related literature, methodology, proposed framework, conclusion, and limitations are included in the remaining section.

CHAPTER 2

REVIEW OF RELATED LITERATURE

2.0 Introduction

This chapter reviewed literature related to the topic and the variables identified within the topic of research. Concepts, views, opinions and documents were discussed within the context and other writing pertaining to the research topic. Some of the reviewed literature in this chapter includes the conceptual framework, cyber-crime, cyber-attacks, cyber security framework, and protection of cyber-attack and cyber security attack in an organization.

2.1 Cybercrime

Cybercrime is currently the second-largest manufactured risk in the globe (Soomro & Hussain, 2019). It includes any unlawful actions taken by hackers, scammers, and online fraudsters. In in addition to sending spam, malware, and worms into computers, networks, and even organizational information systems and worldwide connections to break them, unlawful operations may also involve human activity to obtain unauthorized access to data and information (Mary, 2016)

Individuals, governments, organizations, and organizations (Adesina & Ingirige, 2019) have experienced debilitating effects of cybercrime. Billions of dollars have been spent on damages, data loss, and website defacement as a result. It has created bankruptcy in a variety of nations, organizations, and people, as well as global shock (De Paoli et al., 2020). Since it affects the core missions of teaching, learning, research, community services, administration, and prevention of staff and student information, cybercrime has continued to pose a serious threat to organizations (Bukhari, 2018). The material that is currently available suggests that the COVID-19 period is likely to result in an increase for cybercrimes committed against organizations. For instance, Trawler et al. (2020) stated that COVID-19 had driven a rise in both human and organizational reliance on cyberspace, which is likely to lead to cyber-attack vulnerabilities and threats. Morgan (2020) also noted that within months after the initial COVID-19 outbreak in 2020, more than 4,000 malicious COVID-19-related websites started to develop online. He predicted that, in 2021, there

would be one cybercrime every eleven seconds, or about four times the average for 2020 (every nineteen seconds) and nearly twice the rate for 2019 (every forty seconds) (Morgan, 2020).

Cyber security definition varies, from national to international organizations to researchers, depending on their needs, perspectives, aims and environment. ENISA notes "there is no universally accepted nor straightforward definition of cyber security" (ENISA, 2012). Sharing this view, Dunn (2005) states that "there is no generally accepted definition of cyber security, and several different terms are in use that have related meanings, such as information assurance, information or data security, critical information infrastructure protection". Moreover, Craigie, Diakun-Thibault, and Purse (2014) found the cyber security definition "highly variable, often subjective, and at times, uninformative.

In contrast, it is predicted that effective in 2021, cybercrime would cost the global economy $6 trillion annually, up from $3 trillion in 2015. Cybercrime will cost $10.5 trillion per year starting in 2025. Cybercrime would soon overtake the United States and China as the third-largest economy in the world (Sausalito, 2020). By 2021, ransomware losses are predicted to cost the world $20 billion, or 57 times as much as they did in 2015 ($325 million) (Chapman, 2019; Morgan, 2020). Ransomware is the type of cybercrime that is spreading the fastest, even in businesses. Additionally, 91 percent of cyber-attacks infect companies and organizations through spear-phishing emails.

There is no doubt that the current literature's insights indicate the requirement of a maintain and upgrade prevention framework that may give organizations and businesses helpful info. Generally, cybercrime risk prevention frameworks include a variety of guiding principles and action plans intended to address cybercrime and incidents that are related to it. The National Information and Technology Development Agency (NITDA) and the Office of the National Security Adviser (NSA) in Nigeria agree with Microsoft and the National Institutes of Standards and Technology on the threats that must be addressed by the development of a comprehensive cyber security framework (Osho & Onoja, 2015).

However, this primarily applies to conglomerates in the banking sector, the oil and gas industry, and other industries. This circumstance justifies our efforts to develop a sustainable cyber security framework for organizations

Cyber security is paramount for sustaining a technologically sound model. The disruption of electricity or the impairment of financial systems through interference with ICT networks is a reality; these events constitute national security threats. Malicious online agents are numerous, organized and of diverse persuasions: political, criminal, terrorist, activist. The tools at their disposal become more sophisticated and complex over time and with experience; the growing number of connected platforms only serves to offer new attack vectors. There is no going back to simpler times. In embracing technological progress, cyber security must form an integral and indivisible part of that process. Unfortunately, cyber security is not yet at the core of many national and industrial technology strategies. Although cyber security efforts are numerous, they are eclectic and dispersed. Differences in internet penetration, technological development, private sector dynamics, government strategies, means that cyber security is emerging from a bottom up approach; a natural occurrence where disparities exist between nation states, public and private sectors, and across industries. In essence, however, a global culture of cyber security can be more successfully initiated from the top down. Information sharing and cooperation are key to tackling cross-border threats. Such elements require a certain measure of organization in a multitude of disciplines: legal, technical, educational.

While a particular country or a specific sector will have developed and adopted a highly effective cyber security framework, the knowledge is rarely shared outside of that circle. The primary obstacle is that cyber security is a sensitive issue, whether from a government or private sector perspective. Admission of vulnerabilities can be seen as a weakness. This is a barrier to the discussion and sharing of threat information and best practices. Yet security through obscurity is not a viable defense model against modern cyber threats. The answer is to implement cyber security mechanisms in all layers of society. However, the drive and the incentive to do so are inadequate, either due to cost constraints or simply lack of awareness. A first step towards remedying the situation lies in comparing cyber security capabilities of nation states and publishing an effective ranking of their status. A ranking system would reveal shortcomings and motivate states to intensify their efforts in cyber security. It is only through comparison that the real value of a nation's cyber security capability can truly be weighed.

The Global Cyber security Index (GCI) project aims to effectively measure each nation state's level of cyber security development. The ultimate goal is to help foster a global culture of cyber

security and its integration at the core of information and communication technologies. The International Telecommunication Union (ITU) and private sector company ABI Research has launched the project. The GCI project finds its basis in the current mandate of the ITU and the related projects and activities of the ITU's Telecommunication Development Bureau, the BDT. The ITU is the lead facilitator for WSIS (World Summit on the Information Society) Action Line C5 for assisting stakeholders in building confidence and security in the use of ICTs at national, regional and international levels.

The ITU's mandate in cyber security is further supported by Resolution 69 on the "Creation of national computer incident response teams, particularly for developing countries, and cooperation between them" adopted at the fifth World Telecommunication Development Conference (WTDC-10) and by Resolution 130 (Guadalajara, 2010) on "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies". In this framework, the Global Cyber security Agenda (GCA) was launched by the ITU Secretary-General as ITU's framework for international multi-stakeholder cooperation towards a safer and more secure information society, and focuses on the following five work areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- Cooperation.

These five designated areas will form the basis of the indicators for the GCI. These five indicators are critical to measuring national capabilities in cyber security because they form the inherent building blocks of a national culture. Cyber security has a field of application that cuts across all industries, all sectors, both vertically and horizontally. Enabling the development of national capabilities therefore requires investment by political, economic and social forces. Law enforcement and justice departments, educational institutions and ministries, private sector operators and developers of technology, public-private partnerships and intra-state cooperation can do this.

A cyber security framework is a collection of best practices that an organization should follow to manage its cyber security risk. The goal of the framework is to reduce the company's exposure to cyber-attacks, and to identify the area's most at risk for data breaches and other compromising activity perpetrated by cyber criminals.

A strong cyber risk management framework is closely intertwined with the organization's risk management strategy and risk management programs. Combined with the use of updated information technology and artificial intelligence, a solid cyber security risk management framework can be an excellent way to stave off cyber-attacks.

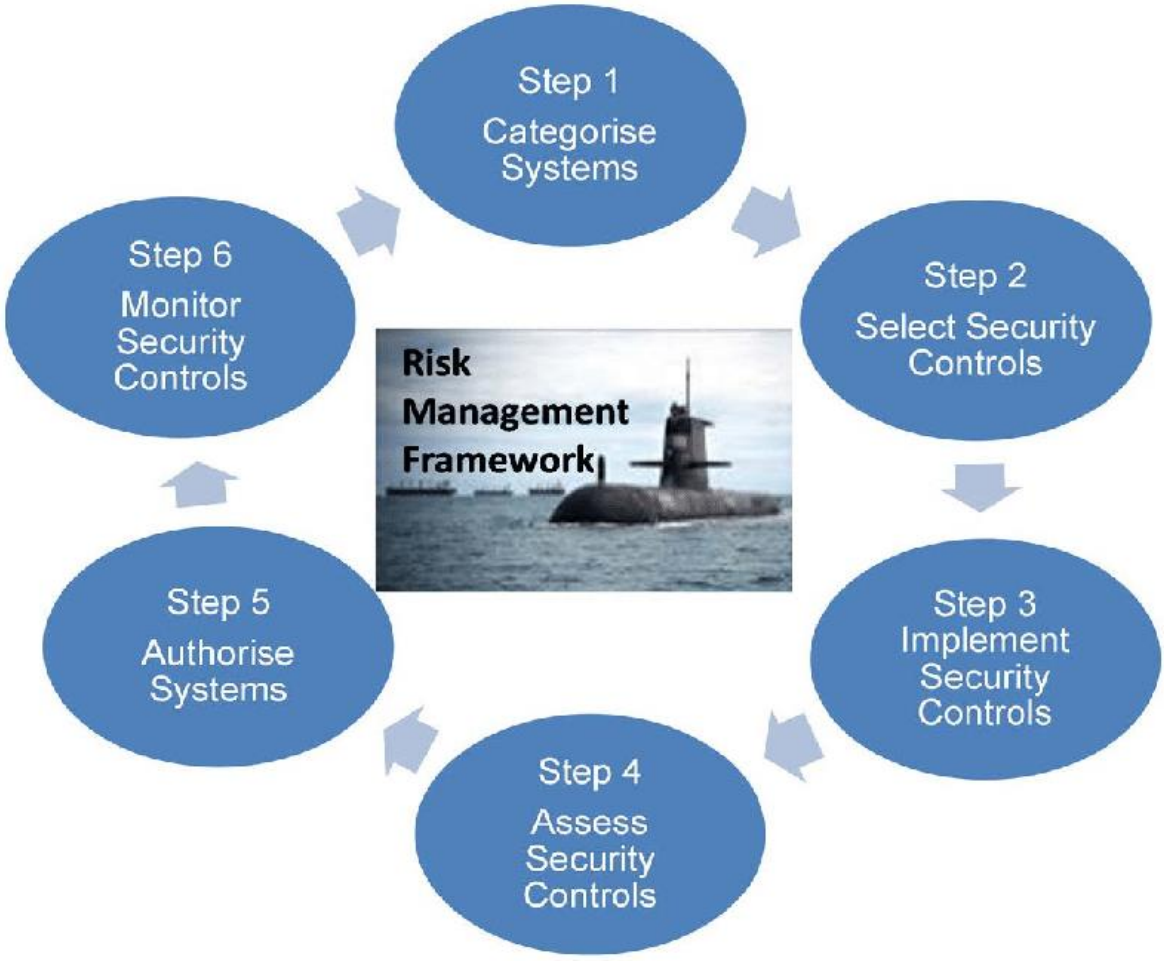

Figure 1: Cyber risk management framework

2.2 Impacts of Cyber Attacks and Cybercrime

Cyber-attack refers to the exploitation of vulnerability or a weakness in the system, whereas cybercrime refers to direct or indirect use of computers to commit online crime. As recent as 2017, Winery ransom ware attacks affected 150 countries causing nearly $4 billion in financial and economic losses to businesses (Berr, 2017).This event demonstrates the large implications, if nations are not well prepared to protect and fight against cyber-attacks and crime. In the past years, several Asian countries have reported cases of cyber-attacks and cybercrime, and their impacts to government, business, and individuals. One example is the cyber-attacks in the Asia-Pacific region, reported by Financial Times, where more than $81 billion in business revenue was lost in the 12 months preceding September 2015.

The global total during this time was of $315 billion (Leo Lewis, Don We inland, & Peel, 2016). The banking heist, reported by Reuters, in Bangladesh, a developing ICT emerging country in South Asia describes how a Bangladesh Bank official's computer was used to steal $81 million takas (Raju Gopala Krishnan & Mojito, 2016). The simultaneous hacking of 68 government websites in the Philippines is also evidence of the difficulties facing ICT emerging nations (Mateo, 2016).

Under develop regions faces its own cyber security challenges. Cases of cyber-attacks and cybercrime have been reported in the national print and social media. For instance, the Bank of Nigeria, was exposed by fraudsters with a fake email purportedly sent from the Royal Audit Authority, Nigeria resulting in the transfer of 16 million (in African's currency) to three different accounts in India, Malaysia and Thailand (Gyeltshen,2016). Moreover, Under develop regions has experienced cyber incidents on government and private websites (Shmueli, 2012b, 2012c), rampant viruses clogging the networks (Schmueli,2010), the distribution of pornographic clips (BBS, 2014)(BBS, 2014), blackmail and financial fraud (BBS, 2011, 2012)(BBS, 2011, 2012).

McAfee (2017), in 2017 Threats Predictions, predicts that nations will face destructive cyber security challenges and risk, especially ransomware, due to the aggressive use of Information operations by nation-states; growth in the numbers and diversity of cyber threat actors; and the greater availability of exploits, tools, encryption, and anonymous payment systems. Also, today's cyber-attacks are becoming often "aggressive, disciplined, well-organized, well-funded, and in a

growing number of documented cases, very sophisticated" (Join Task Force Transformation Initiative, 2010). For example, Winery and Peaty are "a new strain of high-profile, global scale ransomware that appear to have originated from North Korea and Russia primarily aimed at creating chaos and achieving strategic geopolitical goals" (defense, 2017).

2.3 Using the NIST cyber security framework as your baseline

If developing and implementing a cyber-risk management framework from scratch feels intimidating, fear not. The National Institute of Standards and Technology (NIST) has issued many frameworks for security issues. One of the best known is the NIST Cyber security Framework (CSF), a set of guidelines that were originally developed for government entities and have since been adapted for private sector use. Not only does CSF provide a framework to understand cyber security risk management, it also includes guidelines to help companies prevent and recover from attacks.

NIST compiled these standards —, which are optional; some other NIST standards are required for certain businesses, but the CSF is not — after then-President, Barack Obama signed an executive order in 2014. The executive order aimed to establish a cyber-security framework to help protect the country's critical infrastructure and federal information.

There are five main functions of NIST's cyber security framework:

1. **Identify.** Companies must first examine and categorize their supply chain and work environment, to better understand which cyber security risks their systems, assets, data, and frameworks are exposed. This process is also known as a cyber security risk assessment, and it provides a baseline for day-to-day risk.

2. **Protect.** Organizations must develop and implement appropriate safeguards to limit or contain the effects of possible cyber security events. Protection includes cyber security-monitoring programs, firewalls, and physical security controls such as locking the door to your data center. Protection requires continuous monitoring to be efficient and safe.

3. **Detect.** Organizations must implement appropriate procedures to identify cyber security events as soon as possible. A clear methodology should be established so everyone within the organization knows what to do in case of a cyber-attack.

4. **Respond.** Have an incident response team in place before you need it. Make sure all stakeholders are involved in this part of the planning, and that there is a clear chain of command from the moment the cyber-attack has been identified until it is mitigated.

5. **Recover.** Mitigation is a big part of recovery. It includes plans for how you will best restore crucial functions and services, as well as a catalog of temporary security controls to implement as soon as your systems have been compromised by a cyber-security event.

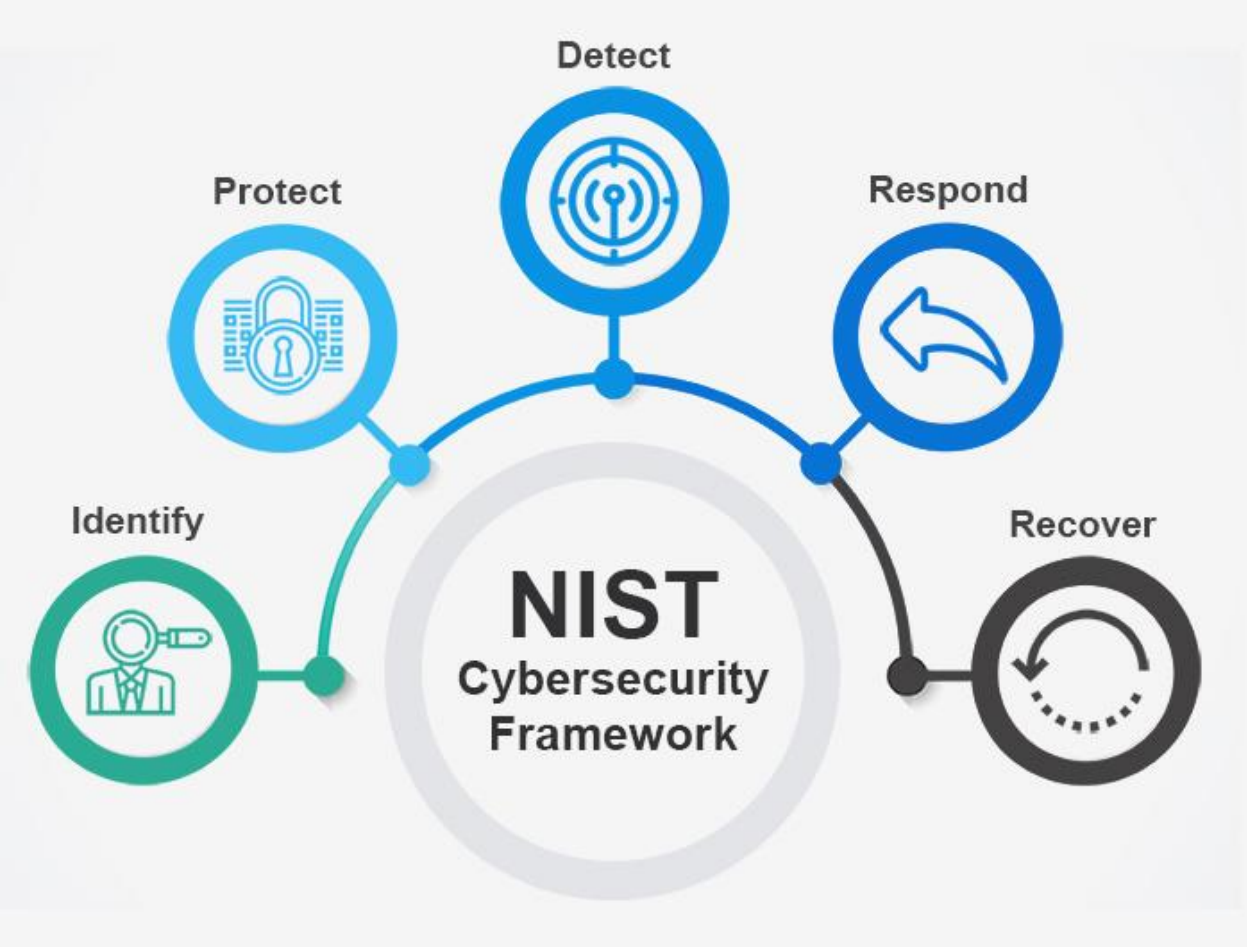

Figure 2: NIST Cybersecurity Framework

Compliance and industry-specific requirements

The risk management process and the tools you use to determine cyber security risk may be the same across industries, but some businesses — such as those that manage healthcare or human resources or credit card payments — have specific requirements for their cyber security programs and also for response and recovery. For example, a company that handles credit card transactions must prove that it complies with the Payment Card Industry Data Security Standards (PCI-DSS) framework. This would require the company to pass an audit.

A strong cyber security framework can provide excellent guidance as you work through the layers of risk assessment. When applied properly, a cyber-security framework allows IT security leaders to manage enterprise risks more efficiently. The NIST model allows an organization to adapt an existing cyber security framework to meet its needs or provides guidance for the organization to develop one internally.

2.4 Protection from Malicious Software and External Attack

New threats continue to emerge and each organization needs to be sure it is equipped to deal with a dynamic threat landscape. The following are some of the more critical system utilities and solutions used to help mitigate these malicious attacks:

- Firewalls are software (and hardware) designed to protect the system from attack from people accessing the organization's systems via both internal and external communication links.
- Malware/spyware and web proxy protection solutions protect the system from software code that may be from pop-up windows or have more insidious intent, such as logging usernames and passwords for fraudulent purposes.
- Anti-spam software protects email inboxes from being clogged by unwanted broadcasted email.
- Anti-phishing software protects users visiting websites that are designed to trap user information that can then be used for fraudulent purposes.

All are mandatory for any well-managed system utilizing a defense in depth strategy. The cost of an attack can be significant, involving loss of data, fraud, and the cost of rebuilding systems and should be analyzed against the cost to defend against such threats.

It is recommended to use a well-known, reputable supplier. Some companies purport to supply these utilities but in fact the utilities themselves can be malicious software. Be cautious about using free software or software from an unknown vendor. Generally, it is best to use the utilities recommended by the business's systems integration (technical support) organization, as they will be responsible for its installation, configuration, and maintenance.

Maintenance of these applications is critical. New malicious software emerges every day. Most software vendors provide at least a daily automatic update to their databases to ensure that the system continues to be effectively protected. Ensuring that these updates are correctly implemented is essential.

Hardware Maintenance Plans

Maintenance contracts should be maintained with hardware suppliers so that hardware failures can be quickly rectified. These contracts should specify the service levels that the supplier will meet in the event of failure. Critical hardware such as servers, switches, and backup technologies require prompt attention. Many contracts specify a four-hour response for failure of these components. Other, less critical hardware such as individual workstations can have longer response times.

Some organizations, particularly in remote areas, purchase some critical components that have a higher potential to fail, such as power supplies, as spare parts that can quickly replace a failed component. Organizations that rely on maintenance contracts should ensure that the support company maintains an adequate supply of spare components to meet the organizations service level commitments.

The quality of the organization's external IT support company is critical in ensuring the systems are correctly implemented and supported. Issues that need to be considered in selecting an appropriate company include:

- Their knowledge and experience with the organization's hardware and operating system configuration.

- Their knowledge and experience with the organization's application software.
- Certifications held with major hardware and software companies, which provide an assurance as to the competency of the people in the organization.
- The number of people within the company who have the required knowledge to support the system—this is critical as a reliance on a single individual can result in significant delays and cost should that individual be unavailable for any reason.
- Their ability to provide support services remotely to enable rapid response to issues at a reasonable cost.
- Proper due diligence and vendor risk management to ensure that the third party is providing the services based on the organization's expectations.

People and Documentation

Every organization should establish a plan to mitigate the risk of key people being unavailable in the event of a system failure. Keep a list of contact details for backup technicians. Document the configuration of hardware and software applications and keep this up to date so that a new technician can quickly rebuild the system.

Policies and Procedures

Proper IT governance procedures within an organization are critical. Implement a formal risk assessment process and develop policies to ensure that systems are not misused and ensure that applicable policies are continually reviewed and updated to reflect the most current risks. This includes developing incident response policies and procedures to properly respond to, account for and help mitigate the cost of a potential breach.

Ongoing education to all employees on technology risks should form part of the organizations risk management framework, with potential security breaches being mitigated as a result of education and policies being promulgated to all levels of staff. Policies should include but are not limited to:

- User Account Management: rules and policies for all levels of users; procedures to ensure the timely discovery of security incidents; IT systems and confidential data are protected from unauthorized users.
- Data Management: establishing effective procedures to manage the repositories, data backup and recovery, and proper disposal of media. Effective data management helps ensure the quality, timeliness, and availability of business data.
- IT Security and Risk Management: process that maintains the integrity of information and protection of IT assets. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures.

Individual jurisdictions are likely to have enacted legislation that may require particular policies, or issues within a particular policy, to be addressed. Common policies are listed below and cover system use, e-mail use, internet use and remote access.

System Use Policy

A system use policy generally outlines the rules by which the organization's IT systems can be used. Example elements to be considered in this policy include:

- Mandatory use of passwords on all systems, such as phones and tablets, including the need for passwords to be changed regularly and a prohibition of providing passwords to other team members or third parties.
- Prohibition of copying organization data and removing the data from the office without approval.
- The encryption of memory/USB sticks.
- The physical security of equipment.
- Use of the system during business hours.
- Rules for the private use of the system, if allowed, outside office hours.

- Multi Factor authentication - using more than one method of authentication from independent categories of credentials to verify the user's identity for login.

Email Use Policy

Example elements to be considered in an email use policy include:

- Prohibiting the use of personal email accounts for business matters.
- Prohibiting opening email attachments from unknown sources (as they may contain malicious software).
- Prohibiting accessing email accounts of other individuals.
- Prohibiting sharing email account passwords.
- Prohibiting excessive personal use of the organization's email.
- Notification that the organization will monitor email.

Internet Use Policy

Example elements to be considered in an internet use policy include:

- Limiting Internet use to business purposes.
- Notification of the ability of the organization to track Internet usage.
- Prohibiting access to sites that are offensive to a person's gender, sexuality, religion, nationality, or politics.
- Ensuring that downloads occur only from a safe and reputable website.
- Prohibiting downloading executable (program) files as they may contain malicious software, and also prohibiting downloading pirated music, movies, or software.
- Prohibiting providing the user's business email address in order to limit the likelihood of spam.
- Consequences of violation.

Remote Access Policy

Example elements to be considered in a remote access policy include:

- Approvals required for external access.
- Reimbursement of external access costs.
- Security procedures (including disclosure of passwords, third-party use of system, disconnection from other networks while accessing the organization's systems, use of firewalls and installation of appropriate software to protect the remote system from malicious attack and multifactor authentication).
- Physical security of organization-supplied equipment such as laptops.
- Reporting of any possible breach of security, unauthorized access, or disclosure of the organization's data.
- Agreement that the organization can monitor the activities of the external user to identify unusual patterns of usage or other activities that may appear suspicious.
- Consequences of noncompliance.

Insurance

Adequate insurance should cover the cost of replacing damaged infrastructure as well as the labor costs to investigate the incident, rebuild systems and restore data. Consider also insurance for productivity loss resulting from a major system failure or catastrophic event.

2.5 Cyber security issues in Organizations

The term "cyber security" originates from the two terms ``cyber" and "security." Cyber refers to technology that encompasses systems, networks, programs, or data, according to Valeriano and Maness (2015). (Valeriano & Maness, 2015). Schneier (2009), on the other hand, asserted that security is related to the defense of systems, networks, programs, and information. Sanook (2018) went on to define cyber security as the protection against cyber attacks of interconnected systems, including hardware, software, and data. The social: values, norms, and cultures hypothesized by

organizations as appropriate and rational ways to behave and relate to others are a key aspect that Valeriano and Maness (2015), Sanoo (2018), and Schneier (2009) did not mention in their definitions.

As a result, we perceive cyber security as primarily involving individuals, the social structures and work processes they establish, as well as the technologies they incorporate to cover the full spectrum of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, and law enforcement. Certain authors in the literature already published have put similar sentiments on cyber security forward. According to these writers, cyber security prevention protocols are a collection of technologies, procedures, and procedures used to protect networks, devices, programs, and data from intrusion, theft, damage, alteration, or illegal access (Abu-Taieh, 2017; Rashid et al., 2018; Sanoo, 2018).

Organizations use cyber security in a range of circumstances, and each university has a unique utilization or application. To protect their network and data online, the majority of enterprises have implemented cyber security. Different cyber security frameworks are employed to manage cyber security risk by organizations in developed nations, including University of Arizona, University of Edinburgh, University of Bristol, University of Sheffield, Princeton University, University of Illinois, University of Leicester, Carnegie Mellon University, and University of Pittsburgh.

The framework adopted simplifies the process for companies to implement their strategic vision and to protect their information systems from threats to their availability, confidentiality, and integrity (Webb & Hume, 2018). In doing so, it recognizes the ability of individuals to learn, grow, and share knowledge. Organizations in Nigeria are apprehensive about the cyber security framework.

To investigate issues relating to cyber security threats in Nigerian organizations, several research were conducted. In a study by Ekpoh et al. (2020) that looked at factors that posed cyber security threats to organizations at the University of Lagos, it was discovered that there was a weak but positive correlation between school climate and personnel security, whereas there was a strong positive relationship between location, culture, and facilities. The study reached the conclusion that lack of discipline, inadequate staff and student awareness of safety and security, inadequate

capacity building for security personnel, inadequate funding of institutions and an out-of-date security framework were the main causes of security lapses in Nigerian organizations.

Dagogo (2005) utilized seven tertiary institutions in a research on the role of security agents in reducing cyber crimes in organizations in the North East of Nigeria. The study found that security personnel and cyber security experts' level of service delivery is significantly impacted by the training and retraining they receive. According to statistics, Nigerian organizations are third among nations around the world for cybercrime, ranking 43rd in Europe, the Middle East, and Africa (Makeri, 2017).

2.6 Cyber Security Framework

The objective of the cyber security prevention framework is to reduce cyber security risks. It is an area of risk prevention in organizations that is still relatively new and expanding. Organizations, like some other organizations, are subject to hazards from natural disasters, mishandled human resources, independent contractors, financial instability, tumultuous conditions, and security breaches. A risk is an unforeseen event that could happen in an organization or organization that may have a negative influence on time, cost, or quality (Mikkola et al., 2020). A risk may have one or more causes or triggers, and if it materializes, it could have a variety of consequences.

Every component of an organization's information systems, as well as its technological and social environments, might be exposed to a variety of risks that are probably brought on by inadequate planning and prevention practices, as well as a lack of centralized prevention systems (Hollis, 2015). As a result, during the past few decades, risk prevention (RM) has emerged as a crucial and essential component of managing cyber-attacks in organizations (Whitehead, 2020). It includes the processes involved in threat prevention and regulation, hazard preparation, assessment, interpretation, and reactions (Purohit et al., 2018), and is further described as a role that endorses and adds value to organizations while raising the likelihood that strategic goals will be achieved.

Every organization, however, must build strong capacities to effectively manage risks if it is to succeed. Modern organizations must create a welcoming environment that lessens the repercussions of risk. The recommendations for organizations to develop cyber attack frameworks come from insights spread throughout the RM domain. This is due to the techniques, processes, and resources used to define and manage risks are important components of cyber-attack

frameworks. (2010) Avon & Ren Numerous cyber-attack strategies are in use globally, based on an individual's or organizational inclination and adaption (Pattinson et al., 2018). The Lockheed Martin Kill Chain, Specified Frameworks, Global Cyber attack Index, and Cyber Attack Risk Framework, in addition to Defense in Depth and Defense in Breath (Smith, 2019)

The US National Institute of Standards and Technology (NIST), however, created the most popular framework and it offers a high-level taxonomy of cyber-attack outcomes as well as a technique for assessing and preventing them. Identification, detection, protection, reaction, and recovery are the five essential functions that organizations should focus on to actively manage cyber-attack threats to their business operations, according to NIST (2020). The Global Cyber-attack Index (GCI) conceptual framework, created by the International Telecommunication Union (ITU) in partnership with ABI research institutes, is another cyber-attack paradigm that is widely used in organizations (ITU, 2015).

The framework aims to methodically assess a nation or organization's progress in cyber-attacks. This framework's goal is to make cyber-attacks a priority for companies that employ information systems and for the users of such systems (ITU, 2015). The structures that affect the dimension of cyber-attack within organizations have been identified as five crucial factors (ITU, 2015; Maarten et al., 2015; Stein, 2008). Technical measures, legislative measures, capacity building, collaborative measures, and organizational measures are some of these constructions.

Although the existing frameworks are obvious and practicable, the majority of them do not directly address the problems that companies have with cyber-attacks. Concerns that are not specifically addressed in contemporary geopolitical frameworks are also raised by the characteristics of organizations in the contexts of developing countries. Organizations must have a solid awareness of their socio-technical contexts, operations, drivers, and security problems if they are to effectively manage cyber-attack risks. The strategies and tactics utilized to accomplish the goals that inform cyber-attack frameworks typically vary since the threats, objectives, and procedures specific to each university are unique.

As a result, this finding contradicts organizations and other similar developing nations to be transparent about their socio-technical contexts, business models, motivations, and security concerns. The study's questions, which are: What are the cyber-attack challenges organizations are

currently facing and what are the problems they are anticipated to face in the future, must be answered by organizations if they are to achieve this clarity of purpose. What should the goals of organizations' cyber-attack programs be? How can organizations create and implement successful cyber-attack proposals?

How can the appropriateness and efficiency of the cyber-attack programs used by organizations be checked and assessed? How can the necessary stakeholders be informed about an organization's cyber-attack program? An innovative cyber-attack framework will be supported by painstakingly and scientifically created solutions.

2.7 Proposed Framework to Protect Cyber Attack in an Organization

Identifying Cyber-attack Threats for an Organizations

Organizations' primary responsibilities are the production, dissemination, and publication of scientific knowledge. Organizations around the world are vulnerable to a variety of cyber-attack problems, such as intellectual property theft, compromise of staff and student records, and university portal hacking (Oliver, 2010). Additionally, several cyber-attack difficulties that Nigerian companies confront include admission falsification, impersonation, unlawful room allocation, website defacement, hacking of login data, printing of bogus admission letters, and others (Bukhari, 2018; Igba et al., 2018; Okeshola & Adeta, 2013).

Organizations may experience numerous new problems. Fraud concerning a will's beneficiary is one of the issues. According to Bian et al. (2018), a will scam happens when a cybercriminal sends an email claiming that the victim is the specified beneficiary in an estranged person's will and is eligible to receive a multimillion-dollar fortune. Online giving presents another new difficulty for cyber-attacks. Cybercriminals host websites that appear to be charitable organizations as a component of online charity.

They utilize the websites to request donations of money and goods (Saulawa & Abubakar, 2014). It's very likely that online criminals would create fake websites to solicit donations for organizations. Theft of computer/Internet service time is another cybercrime, which affects organizations. In order to run their cafes at the expense of the companies, criminals devise ways

to connect privately owned cyber cafes to networks owned by organizations in ways that are difficult to detect (Oliver, 2010).

Cyber security threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks—we describe each of these categories in more detail below.

Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups, to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.

- **Common Sources of Cyber Threats**

Here are several common sources of cyber threats against organizations:

- **Nation states**—hostile countries can launch cyber-attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.
- **Terrorist organizations**—terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.
- **Criminal groups**—organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams.
- **Hackers**—individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community.
- **Malicious insiders**—an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target

organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

- **Types of Cyber security Threats**

Malware Attacks

Malware is an abbreviation of "malicious software", which includes viruses, worms, Trojans, spyware, and ransomware, and is the most common type of cyber-attack. Malware infiltrates a system, usually via a link on an untrusted website or email or an unwanted software download. It deploys on the target system, collects sensitive data, manipulates and blocks access to network components, and may destroy data or shut down the system altogether.

Here are some of the main types of malware attacks:

- **Viruses—**a piece of code injects itself into an application. When the application runs, the malicious code executes.
- **Worms—**malware that exploits software vulnerabilities and backdoors to gain access to an operating system. Once installed in the network, the worm can carry out attacks such as distributed denial of service (DDoS).
- **Trojans—**malicious code or software that poses as an innocent program, hiding in apps, games or email attachments. An unsuspecting user downloads the trojan, allowing it to gain control of their device.
- **Ransomware—**a user or organization is denied access to their own systems or data via encryption. The attacker typically demands a ransom be paid in exchange for a decryption key to restore access, but there is no guarantee that paying the ransom will actually restore full access or functionality.
- **Cryptojacking**—attackers deploy software on a victim's device, and begin using their computing resources to generate cryptocurrency, without their knowledge. Affected systems can become slow and cryptojacking kits can affect system stability.

- **Spyware**—a malicious actor gains access to an unsuspecting user's data, including sensitive information such as passwords and payment details. Spyware can affect desktop browsers, mobile phones and desktop applications.
- **Adware—**a user's browsing activity is tracked to determine behavior patterns and interests, allowing advertisers to send the user targeted advertising. Adware is related to spyware but does not involve installing software on the user's device and is not necessarily used for malicious purposes, but it can be used without the user's consent and compromise their privacy.
- **Fileless malware**—no software is installed on the operating system. Native files like WMI and PowerShell are edited to enable malicious functions. This stealthy form of attack is difficult to detect (antivirus can't identify it), because the compromised files are recognized as legitimate.
- **Rootkits—**software is injected into applications, firmware, operating system kernels or hypervisors, providing remote administrative access to a computer. The attacker can start the operating system within a compromised environment, gain complete control of the computer and deliver additional malware.

Social Engineering Attacks

Social engineering involves tricking users into providing an entry point for malware. The victim provides sensitive information or unwittingly installs malware on their device, because the attacker poses as a legitimate actor.

Here are some of the main types of social engineering attacks:

- **Baiting**—the attacker lures a user into a social engineering trap, usually with a promise of something attractive like a free gift card. The victim provides sensitive information such as credentials to the attacker.
- **Pretexting**—similar to baiting, the attacker pressures the target into giving up information under false pretenses. This typically involves impersonating someone with authority, for example an IRS or police officer, whose position will compel the victim to comply.

- **Phishing—**the attacker sends emails pretending to come from a trusted source. Phishing often involves sending fraudulent emails to as many users as possible, but can also be more targeted. For example, "spear phishing" personalizes the email to target a specific user, while "whaling" takes this a step further by targeting high-value individuals such as CEOs.
- **Vishing** (voice phishing)—the imposter uses the phone to trick the target into disclosing sensitive data or grant access to the target system. Vishing typically targets older individuals but can be employed against anyone.
- **Smishing** (SMS phishing)—the attacker uses text messages as the means of deceiving the victim.
- **Piggybacking**—an authorized user provides physical access to another individual who "piggybacks" off the user's credentials. For example, an employee may grant access to someone posing as a new employee who misplaced their credential card.
- **Tailgating—**an unauthorized individual follows an authorized user into a location, for example by quickly slipping in through a protected door after the authorized user has opened it. This technique is similar to piggybacking except that the person being tailgated is unaware that they are being used by another individual.

Supply Chain Attacks

Supply chain attacks are a new type of threat to software developers and vendors. Its purpose is to infect legitimate applications and distribute malware via source code, build processes or software update mechanisms.

Attackers are looking for non-secure network protocols, server infrastructure, and coding techniques, and use them to compromise build and update process, modify source code and hide malicious content.

Supply chain attacks are especially severe because the applications being compromised by attackers are signed and certified by trusted vendors. In a software supply chain attack, the software vendor is not aware that its applications or updates are infected with malware. Malicious code runs with the same trust and privileges as the compromised application.

Types of supply chain attacks include:

- Compromise of build tools or development pipelines
- Compromise of code signing procedures or developer accounts
- Malicious code sent as automated updates to hardware or firmware components
- Malicious code pre-installed on physical devices

Man-in-the-Middle Attack

A Man-in-the-Middle (MitM) attack involves intercepting the communication between two endpoints, such as a user and an application. The attacker can eavesdrop on the communication, steal sensitive data, and impersonate each party participating in the communication.

Examples of MitM attacks include:

- **Wi-Fi eavesdropping—**an attacker sets up a Wi-Fi connection, posing as a legitimate actor, such as a business, that users may connect to. The fraudulent Wi-Fi allows the attacker to monitor the activity of connected users and intercept data such as payment card details and login credentials.
- **Email hijacking**—an attacker spoofs the email address of a legitimate organization, such as a bank, and uses it to trick users into giving up sensitive information or transferring money to the attacker. The user follows instructions they think come from the bank but are actually from the attacker.
- **DNS spoofing**—a Domain Name Server (DNS) is spoofed, directing a user to a malicious website posing as a legitimate site. The attacker may divert traffic from the legitimate site or steal the user's credentials.
- **IP spoofing**—an internet protocol (IP) address connects users to a specific website. An attacker can spoof an IP address to pose as a website and deceive users into thinking they are interacting with that website.

- **HTTPS spoofing**—HTTPS is generally considered the more secure version of HTTP, but can also be used to trick the browser into thinking that a malicious website is safe. The attacker uses "HTTPS" in the URL to conceal the malicious nature of the website.

Denial-of-Service Attack

A Denial-of-Service (DoS) attack overloads the target system with a large volume of traffic, hindering the ability of the system to function normally. An attack involving multiple devices is known as a distributed denial-of-service (DDoS) attack.

DoS attack techniques include:

- **HTTP flood DDoS**—the attacker uses HTTP requests that appear legitimate to overwhelm an application or web server. This technique does not require high bandwidth or malformed packets, and typically tries to force a target system to allocate as many resources as possible for each request.

- **SYN flood DDoS**—initiating a Transmission Control Protocol (TCP) connection sequence involves sending a SYN request that the host must respond to with a SYN-ACK that acknowledges the request, and then the requester must respond with an ACK. Attackers can exploit this sequence, tying up server resources, by sending SYN requests but not responding to the SYN-ACKs from the host.

- **UDP flood DDoS**—a remote host is flooded with User Datagram Protocol (UDP) packets sent to random ports. This technique forces the host to search for applications on the affected ports and respond with "Destination Unreachable" packets, which uses up the host resources.

- **ICMP flood**—a barrage of ICMP Echo Request packets overwhelms the target, consuming both inbound and outgoing bandwidth. The servers may try to respond to each request with an ICMP Echo Reply packet, but cannot keep up with the rate of requests, so the system slows down.

- **NTP amplification**—Network Time Protocol (NTP) servers are accessible to the public and can be exploited by an attacker to send large volumes of UDP traffic to a targeted

server. This is considered an amplification attack due to the query-to-response ratio of 1:20 to 1:200, which allows an attacker to exploit open NTP servers to execute high-volume, high-bandwidth DDoS attacks.

Injection Attacks

Injection attacks exploit a variety of vulnerabilities to directly insert malicious input into the code of a web application. Successful attacks may expose sensitive information, execute a DoS attack or compromise the entire system.

Here are some of the main vectors for injection attacks:

- **SQL injection**—an attacker enters an SQL query into an end user input channel, such as a web form or comment field. A vulnerable application will send the attacker's data to the database, and will execute any SQL commands that have been injected into the query. Most web applications use databases based on Structured Query Language (SQL), making them vulnerable to SQL injection. A new variant on this attack is NoSQL attacks, targeted against databases that do not use a relational data structure.
- **Code injection**—an attacker can inject code into an application if it is vulnerable. The web server executes the malicious code as if it were part of the application.
- **OS command injection**—an attacker can exploit a command injection vulnerability to input commands for the operating system to execute. This allows the attack to exfiltrate OS data or take over the system.
- **LDAP injection**—an attacker inputs characters to alter Lightweight Directory Access Protocol (LDAP) queries. A system is vulnerable if it uses unsanitized LDAP queries. These attacks are very severe because LDAP servers may store user accounts and credentials for an entire organization.
- **XML eXternal Entities (XXE) Injection**—an attack is carried out using specially-constructed XML documents. This differs from other attack vectors because it exploits inherent vulnerabilities in legacy XML parsers rather than unvalidated user inputs. XML

documents can be used to traverse paths, execute code remotely and execute server-side request forgery (SSRF).

- **Cross-Site Scripting (XSS)**—an attacker inputs a string of text containing malicious JavaScript. The target's browser executes the code, enabling the attacker to redirect users to a malicious website or steal session cookies to hijack a user's session. An application is vulnerable to XSS if it doesn't sanitize user inputs to remove JavaScript code.

CHAPTER 3

METHODOLOGY

3.0 Introduction

The following chapter aims to present the study's methodology through the philosophical assumptions, the research approach, and design including a description of the case company. Further discussed in this chapter is the data collection method, including qualitative interviews, interview guide, motivation for selection of respondents, criticism of empirical data collection and secondary sources. Finally, the study's data analysis method, and the ethical aspects as well as the quality of the study are deliberated.

3.1 Philosophical Assumptions

In the last decade, social issues related to computer based information systems have grown to become important and increasingly recognized (Walsham, 1995). Due to throwing importance, information systems researchers have adopted approaches focused on human interpretations and meaning (Walsham, 1995). Even though positivist research is more common within business and management research than interpretive research, interpretive research has gained ground within the past two decades (Myers, 2009).

Myers (2009) describes that researchers that adopt an interpretive research method assume that reality can only be accessed through social construction (e.g. Language, shared meanings or instruments). Kaplan and Maxwell (1994) state that as situations emerge, researchers focus on the complexity of human sense making. Moreover, Myers (2009) describes that social scientists assert that a social researcher conducts research as an insider, and thus the researcher speaks the same language as the people being studied, or at least can understand interpretations being made. This is in line with our study, since we deem that we as social researchers have the ability to interpret data due to our educational background within business administration and information systems.

We have followed the epistemological assumptions of interpretivism that Myers (2009) presents. In interpretivism, context or theory determines the correct meaning of data, and for researchers to

better understand the intentions and meanings of the people studied, a good theory is needed. Regarding generalizations, an interpretive researcher will develop context bound generalizations that are close to the researchers methods. Interpretive researchers are not keen on precise definitions of a phenomenon; instead, they seek to clarify emerging meanings.

Finally, meanings in interpretivism are what constitute the facts, rather than in positivism where meaning is separate from facts (Myers, 2009) Research strategy can be separated into two categories, qualitative and quantitative research. Due to the nature of our study, we used a qualitative research method. Justesenand Mik-Meyer (2011) explain the qualitative research method as a method used in order to gain a greater understanding of a phenomenon. The authors further imply that the qualitative research method is appropriate when conducting interviews with smaller groups of people and thereafter performing an analysis of the gathered material. In order to fulfill the purpose of our study we therefore considered this research method the most appropriate. The primary reason to undertake a qualitative method is that this strategy allows deeper analysis (Justesen & Mik-Meyer, 2011).

Since we are not aware of the potential factors that can affect cyber security incidents and the related preventions in advance, a qualitative method allows unknown factors to be identified. Further, the aim of our study was to gain deeper understanding and knowledge within the field, which a quantitative method could be argued not to fulfill due to its lack in providing the necessary data in order to fulfill the study's purpose. We deemed that the data collection required for this thesis had to be of an elaborated nature to ensure rich empirical results and a strong analytical foundation, which we consider to be achieved best through a qualitative method. Furthermore, according to Myers (2009), a key advantage of conducting qualitative research is that it allows the researcher to understand in which context actions and decisions are made, and it is contexts that contribute to an explanation to why or why someone has acted the way they did. The most effective way of understanding contexts and its impact on actions is to talk to people (Myers, 2009).

The author further describes that qualitative researchers claim that it is impossible to understand tractions taken within an organization without talking to people. We view this aspect to be of great relevance to our study, since the chosen research area, cyber security incident prevention, is contextually based.

3.2 Research Approach

According to Bryan and Bell (2015), there exists two research approaches; deductive and inductive approaches. The authors explain that a deductive approach is used when theories guide the research and it aims to verify or falsify theories that already exist. An inductive approach, on the other hand, is used when the empirical evidence guides the research and generates theory.

Bryan and Bell (2015) argue that it is seldom that researchers choose to only follow an inductive approach. Instead, researchers have combined both approaches and iterated between them, which is known as an addictive or iterative approach according to the authors. In accordance with the authors, our study has adopted an iterative approach, with deduction as the foundation and subsequently we iterated between deduction and induction. We believe this approach to be most suitable in accordance with the research strategy and design. We found inspiration in previous research as we constructed the interview guide for our empirical data collection, as well as the empirical data collection acting as a guide for the direction of our literature review. Hence, the research adopted an iterative approach.

Moreover, this study is of an interpretative nature, as previously mentioned, which Mantere and Ketokivi (2013) describe to be the most common research reasoning when using an iterative approach. We are aware that having an interpretative study may affect the degree of generalizability of our findings.

3.3 Research Design

The design of the research method is the logic, which consists of realizing the study, with the initial research questions as a starting point in order to generate a result and draw conclusions (Yin, 2009). The design of our research is that of a case study of the under develop region's public sector and their work with prevention of cyber security incidents. According to Walsham (1995), an in-depth case study is often used within interpretive IS research. A case study entails analyzing a single case intensively with attention to details (Bryman & Bell, 2015). When one is performing a case study, it is most often an organization, industry or workplace that is examined (Bryman & Bell, 2011; Yin,2009).

According to the authors, a case study research design differentiates itself from other designs through its limitation regarding a situation with a purpose and functioning parts. Walsham (1995) argues that Yin's (1989) view, that case studies are the preferred research strategy to answer questions of "how" and "why", is accepted in the interpretive school, despite the positivist stance of Yin. In order to fulfill the purpose of our study and best answer the connected research questions, we deemed a case study design to be the most appropriate. The case in our study is the phenomenon of cyber security incident prevention within the public sector, and the phenomenon is explored by examining two public organizations. These organizations are a nationwide Nigeria authority and a county council, which will be anonymous due to demands from both organizations. We have chosen to focus on solely two organizations within the public sector in order to be able to perform a deeper analysis, but also due to the time limitation of this thesis.

One of the main advantages of conducting case study research is what Myers (2009) refers to as 'face validity', which entails that a case study based on empirical evidence in an organization represents a real story that researchers can identify with. Moreover, most stories from case studies are contemporary and thus the issues that these organizations deal with may be similar to what other organizations are currently experiencing. Since cyber security is growing to become important within the public sector, we believe that the issues mentioned within this study may be experienced by other public organizations in Sweden. Another advantage of case study research is that it allows the researcher to gain a deeper understanding regarding complexities that may emerge in terms of actions or decisions made. One of the main disadvantages of conducting case study research is gaining access to the case organization (Myers, 2009).

The degree of access may be influenced by firm skepticism of the research value, and whether the findings will be worth the time. Another disadvantage is the aspect of young, inexperienced researchers because they may have trouble limiting the focus and determining on what issues are important. This is something that we as researchers have taken into consideration, and we have attempted to narrow our area to focus on areas of relevance.

3.3.1 The case companies

As the case companies requested to be anonymous in this study, the descriptions of the organizations will be made on a more general level, describing the work of authorities and county councils of Nigeria in general.

The authority

The African authorities, also known as government agencies, are state-controlled organizations put into place to carry out policies of the Nigeria Government. The African authorities consist of the government, courts of law and administrative authorities and as of March 2020 there exist 448 authorities (SCB, 2018), with 160 000 employees (OFR, 2018). The administrative authorities can be either government or municipal, and in our case, the organization is one of the nationwide governmental authorities.

The county council

The second case company is, as previously mentioned, a county council. In Sweden, the county councils function as regional autonomous entities with primary responsibilities in providing health care, local public transportation, libraries as well as regional planning, to mention a few (SKL, 2017). Moreover, the government decides the division of the county councils and African is currently divided into 54 countries council.

The power of decision-making is exercised by elected assemblies and there currently exists 439 (in upper and lower federal assembly) political assignments within the county councils and the current population of Nigeria is 218,815,817, based on World meter elaboration of the latest United Nations data. They employ approximately 60 million people (world meter, 2022).

3.4 Data Collection

3.4.1 Quality interview

The study, we used qualitative interviews as the source for our primary data. Lantz(1993), argues that interviews are a method for systematic gathering of information. Interviews could be considered the most widely employed method for data collection in qualitative research (Bryman & Bell, 2015). Moreover, Walsham (1995) argues that interviews should be used as the primary

data source in interpretive case studies. The use of qualitative interviews is seen as suitable when the researcher wants to comprehend the world from the interviewee's point of view according to Kvale and Brinkmann (2014) and Walsham (1995).

In addition, the interview at the county council was recorded and transcribed. We chose to use this method during the interview since it allowed us both to be present and more involved, and not preoccupied by taking notes. Not only does recording allow the interviewer to avoid distractions, the recorded material allow the interviewer to transcribe not only what the interviewee says but also how they say it, which according to Bryman and Bell (2015) allow a deeper analysis. However, the interviews at the authority were not allowed to be recorded due to the sensitivity of the information being discussed. Thus, all interviews conducted at the authority were noted by hand and transcribed afterwards. Lastly, the interviews were held in African official languages, and all transcriptions therefore had to be translated in English. We have attempted to translate and interpret the quotes as accurately as possible. However, we are aware that the usage of quotes could therefore be perceived as well articulated, since the sentence structures had to be altered.

3.4.2 Interview guide

We used semi-structured interviews, which according to Bryman and Bell (2015) entail that even though researchers follow an interview guide, they can still add questions during the interview if it is of interest. Moreover, the semi-structured interview entails no restrictions for the interviewee as to how to reply and if the interviewer wants to highlight a topic presented by the interviewee, a question may be added (Bryman & Bell, 2015).

We chose this approach, as we wanted to keep the interviews open for discussions and subjects that we might be unaware. Furthermore, this allowed the interviews to explore further subjects that could be of interest and play a role in the results and recommendations. The decision of conducting the interviews in a semi-structured manner is in accordance with Walsham (1995), who argues that the interviewer should neither direct the interview too firmly nor be too passive. The interview guide that contributed the foundation for our interviews can be located in Appendix B. All interviewees were selected based on their relevant position within the organizations, in regards to the selected phenomenon. Due to the interviewee's demand for anonymity, they will be referred to their titles instead of names. A list of interviewees can be found below (see table 1).

Table 3.1: Interviewee Organization Date Length

ICT STAFF	Year	DURATION	TIME FRAME
IT Security Officer County Council	2021	04-10	20min
IT Security Officer Authority	2021	04-13	20 min
Chief information Security Officer	2021	04-12	20 min
Information Security Specialist Authority	2021	04-14	20 min

3.4.3 Criticism of Empirical Data Collection

The first aspect to keep in mind considering the empirical data collection is the matter of potential subjectivity with the interviewees. This is due to a mixture of both professional and personal opinions being expressed. Moreover, due to our study being limited to solely two public organizations' perspectives, we cannot exclude that subjectivity and bias could appear in our empirical data collection. Another potential impact on the empirical data is the fact that the IT Security Officer at the authority chose to be present at all conducted interviews, which may have influenced the respondents' response and discussion. Moreover, due to cyber security, especially incident management, being a sensitive field for both organizations, the interviewees may have excluded some information that could have had an impact on the results of this study. That this area of study is sensitive became even more apparent during the interviews at the authority, which, as previously mentioned, were not allowed to be recorded.

Furthermore, the generalizability of the study may be limited due to only two organizations being studied, as well as the study being limited to the organization's experienced challenges and opportunities. As we aim for our study to be generalizable across the public sector, this could entail some authorities having a difficult time relating to our empirical results. We understand that not

all answers can be generalized, although the intention is that other organizations within the public sector could relate to a certain extent.

3.4.4 Secondary Sources

In order to gain knowledge about the existing research within the chosen field we collected previously conducted research, industrial surveys and a suitable framework, in accordance with Bryman and Bell (2015). As for the methodology sources, these were derived from books retrieved at the library of Linköping University. However, the majority of our overall sources were peer-reviewed literature retrieved online from the following databases; Scopus, Google Scholar and Web of Science. The peer-reviewed literature were chosen according to times cited, relevance regarding subject and/or keywords, and dates going from newest to oldest

Bryman and Bell (2015) emphasize the importance of possessing critical reading skills when conducting a study of this nature. In accordance with the authors, it was of importance for us to take into consideration the trustworthiness of the literature we collected. To achieve trustworthiness of the information gathered, triangulation of literature was attempted to the most possible extent, in accordance with Bryman & Bell(2015). The authors describe triangulation as used when one wants to confirm information with at least two sources to provide a stronger theoretical content, since relying on one sole source could lead to gathering biased information.

3.5 Data analysis method

After transcribing and translating the empirical data, we performed a categorization in order to identify possible patterns, similarities or differences in the collected data, which is in accordance with Bryman and Bell (2015). It is important to clarify the connection between analysis and the empirical material (Ahrne & Svensson, 2015). This clarification is important as the empirical results disciplines and imposes limits for the analysis. Thus, in accordance with Ahrens and Swenson (2015), we attempted to maintain a connecting thread throughout the empirical results and the analysis, to the greatest extent possible, to facilitate the identified linkages.

The method we have chosen for analyzing empirical data is known as a thematic analysis. This method is described by Bryman and Bell (2015) and entails a systematic categorization and analysis according to themes deemed relevant in line with the purpose of the study. Furthermore,

Berg (2004) explains that thematic analysis entails categorization of text and identification of relationships among the formulated categories. We deemed this analysis method to be most appropriate in relation to our purpose and research questions. Our thematic analysis proceeded in the following stages; we started with a deductive thematic analysis, and subsequently iterated in-between theoretical concepts and empirical data.

In addition, we followed the three criteria presented by Owen (1984). The first criteria is recurrence, which entails that we identified the recurrence of the same meaning of expressions in different words. The second criteria is repetition, which means that we identified words, phrases and sentences that were repeated in the texts. Finally, the third criteria entails the authors to attach significance to the concepts. A theme is thus considered a set of papers that is consistent with a phenomenon (Roberts, Galluch, Dinger & Gover, 2012). Hence, we have chosen to identify and formulate themes that are consistent with cyber security incident prevention, and themes we find to be influential factors when it comes to preventing incidents.

3.6 Ethical aspect

Ethical aspects were taken into consideration, since the content of the empirical evidence that was presented in this study could be considered as sensitive information. Kvale and Brinkmann (2014) has presented four principal guidelines to follow when conducting research in an effort to protect individuals. The four guidelines consist of; informed consent, confidentiality, consequences, and the role of the researcher.

Informed consent implies informing participants regarding the purpose and the design of the research, as well as explaining risks and advantages involved with the study (Kvale & Brinkmann, 2014). Within this study, we informed the individuals that participation is voluntary and could be anonymous. All participants reviewed the transcripts of the interviews and approved the content before it was used. The requirement of confidentiality implies that agreements between researchers and participants have been made regarding how the data will be used and its intent (Kvale & Brinkmann, 2014). No material was used in this study that could potentially harm the participating individuals or their line of work.

The requirement of confidentiality could also be linked to the aspect of consequences. By assessing consequences for the participating individuals in a qualitative study, as presented by Kvale and

Brinkmann (2014), the principle of ethics is to do well and therefore the risk of doing harm to the interviewee should be minimal. This is an aspect we strived to always keep in mind and always assessed risks and consequences throughout the study. Finally, the role of the researcher is the fourth principle to follow according to Kvale and Brinkmann (2014). The authors state that the researcher has a responsibility of integrity, empathy and sensitivity in relation to moral questions. In this study, we strived to always distance ourselves from personal values and feelings to the greatest extent possible in accordance with literature.

3.7 Quality of the study

In order to secure the trustworthiness and quality of our study we followed the four criteria first acknowledged by Lincoln and Guba (1985), presented in Bryman and Bell (2015). Trustworthiness is divided into the criteria of credibility, transferability, dependability and conformability. The criteria will be introduced and briefly discussed down below, and some of them will be reflected upon at the final stage of this thesis.

3.7.1 Credibility

The criterion of credibility is defined as a trustworthiness criterion, which entails carrying out research according to good practice as well as submitting the findings to those taking part in the study for confirmation (Bryman & Bell, 2015). According toLantz (1993) it is of the essence that respondents taking part in a study are considered reliable and for authors to critically examine responses in order for an interview to be considered as a valuable foundation for a study. In order to fulfill this criterion, and for our analysis and conclusion to be considered trustworthy, all transcribed material that lies as a foundation for our empirical data has been returned to the interviewees for approval. When doing this, we assured that no misinterpretations had been made on our part and therefore we considered the criterion of credibility to be fulfilled, and the trustworthiness to be assured.

3.7.2 Transferability

The authors further describe transferability as the ability of the performed study to be generalizable in multiple contexts in order for the research to be considered reliable (Bryman & Bell, 2015). Our study explored the subject of cyber security incident prevention and was performed as a case study.

Myers (2012) argue that findings from conducted case studies cannot be fully generalized, since case studies are limited to the context of the individual case. However, we believe the results from our study could be transferred and applied to other empirical contexts. Therefore the results from our study could provide indication of a generalizable result and thus fulfill this criterion to achieve trustworthiness.

3.7.3 Dependability

The third criterion, dependability, entails that more than one observer or member of the research team partake and keep track of all the different processes in the study (Bryman& Bell, 2015). In order for us to ensure dependability of our study, both authors participated in all steps of the process. Furthermore, we worked closely with our supervisor and received feedback and inputs from fellow students to ensure the quality of our study.

3.7.4 Conformability

Bryman and Bell (2015) as the criterion for ensuring that the researcher /-s maintain objectivity throughout the study describe the last criterion, conformability. This means not letting personal values and opinions sway the direction of the study. However, to accomplish complete objectivity within research is, according to Myrdal(1969) an illusion as the viewpoints of researchers always guide the study throughout some stages of the research process and thus imply some subjectivity. The previously mentioned work with a tutor and other students helped us to maintain some level of objectivity. We consider the input of these other people to our study to be objective and could therefore be seen as a contributing factor to our study's objectivity.

CHAPTER 4

DATA PRESENTATION AND ANALYSIS

4.1 Introduction

This chapter reports on the quantitative data collected using closed and open-ended survey questionnaires. The analysis of the quantitative data is based on the responses of 109 ICT professionals of different government and autonomous agencies in under develop regions. The data analysis aims to reveal the state of cyber security practices, identify emerging cyber security issues and challenges facing under develop regions, and understand the perceptions of cyber security in government agencies. The first section of this chapter presents background information of survey participants and describes demographic characteristics such as gender, age, and educational qualification. Following the background and demographics, an analysis of quantitative data on policies, awareness and training, and incident handling and response capability. The final section summarizes the analysis and findings and highlights the significance of the research findings.

4.2 Questionnaire Description

The questionnaires distribution of the respondents is illustrated in Table 4.1 (below).As can be seen the number of male participants more are than double the female participants.

Table 4.1: Gender Distribution of Respondents

Gender Frequency Percentage

question Distribution of Respondents	**frequency**	**percentage %**
male	75	68.8%
female	34	31.2%
total	**109**	**100%**

Table 4.1 shows the respondents of the rate for the analysis of the survey data in the following tables and figures will be based on these totals and frequencies.

4.3 Demographic Characteristics

The demographic characteristics of survey respondents such as gender, education and work experience are explored in this section. The analysis of the survey is presented as frequencies and percentages of total survey respondents who had fully completed the survey questionnaire.

4.3.1 Gender of Respondents

An online survey questionnaire was administered to 280 ICT professionals/employees working in different government organizations (organizations include agencies, autonomous agencies, and district administrations) and 157 responses were received, which indicates about 56% response rate (157/280). However, after preprocessing the responses, it was found that only 109 respondents (75 male and 34 female) had fully completed the survey questionnaire, resulting in about 69% completion rate (109/157).

The gender distribution of the respondents is illustrated in Table 4.2 (below).

As can be seen the number of male participants more than double the female participants.

Table 4.2: Gender Distribution of Respondents

Gender Frequency Percentage

Gender Distribution of Respondents	**frequency**	**percentage %**
male	75	68.8%
female	34	31.2%
total	**109**	**100%**

The analysis of the survey data in the following tables and figures will be based on these totals and frequencies.

4.4 Setting Objectives for an Organizations' Cyber-attack Programs

The primary objectives of cyber-attack programs are to support firms in lowering the susceptibility of the networks and information systems they use to conduct business online. For businesses, including an organization, determining adequate and relevant objectives for cyber-attack programs can be a very difficult issue (Igba et al., 2018)

This is because the objectives that organizations' cyber-attack operations are designed to achieve greatly influence their potential audience. As a consequence, the values and objectives of organizations are functions of their comprehension of the cyber security threats they face, their capacity to communicate and share information about those threats with key stakeholders, and their capacity to translate that understanding into cyber attack prevention policies and practices (Bian et al., 2018; Saulawa & Abubakar, 2014).

The appropriateness and appropriateness of the cyber-attack objectives Nigerian organizations designate also determines how much they collaborate with governmental, commercial, and international bodies on their cyber-attack initiatives. Cyber-attack objectives offer a frame of reference that aids in analyzing current trends in cybercrime and the best ways to combat them for enterprises. The goals of cyber-attacks also serve as a foundation for measuring the effectiveness, reliability, and integrity of cyber-attack programs.

4.5 Techniques for Preventing Cyber-attacks by Organizations

The first line of protection against cyber-attack threats is a cyber-attack policy framework. Although it develops from organizational goals for cyber-attacks, it describes what organizations should do and how to respond to cyber-attack risks. Each organization's cyber-attack policy should be connected with those of other organizations and should leave leeway for other organizations and organizations to select what policies they should put in place to prevent or manage cyber-attacks (Makeri, 2017).

A comprehensive cyber-attack framework should specify the mandatory cyber-attack education and training that organizations should provide staff and customers. Furthermore, it is essential to

educate organizations, students and employees of other organizations on the best techniques for dealing with cyber-attacks. It should also specify how other organizations that the organizations work with should react to cyber-attacks. For instance, numerous organizations in developed nations have a rule stating that all systems under their control must adhere to stringent security standards (Ekpoh et al., 2020).

All computers and servers on the internal network receive automatic upgrades, and no new system is let online until it conforms to the security policy (Iriqat & Molok, 2019). Cyber-attack policy frameworks must also contain the cyber-attack prevention resources required to prevent or manage cyber-attacks. In order to protect clients from all sorts of cyber-attacks, organizations' cyber-attack policy frameworks should also specify the function ISPs are to play within the organization's cyberspace and how to maintain high levels of security at servers (Odinma, 2010).

4.6 Cyber-attack Programs Appropriateness and Adequacy Assessment

An important part of the cyber-attack prevention framework proposed in this paper is making room to assess the appropriateness and adequacy of the entire cyber-attack prevention framework. This could be done in two ways (Pavol Zavarsky & CISM, 2014). First, is appropriateness and adequacy assessment that is based on assumptions (Armenia et al., 2021). Second, is the appropriateness and adequacy assessment that is based on experience (Glantz et al., 2016). The first option occurs given that appropriateness and adequacy are determined before the occurrence of cyber-attack.

The second option occurs after a cyber-attack when an organization assesses its cyber-attack prevention framework vis-à-vis the nature and strategy of the cyber-attack it suffered. The attack may not be a serious attack, but it provides an avenue for cyber-attack prevention framework appropriateness and adequacy assessment. These two approaches to assessing the appropriateness and adequacy of organizations' cyber-attack prevention frameworks can help those concerned to modify existing cyber-attack prevention frameworks. They help to open avenues for constructive feedback from those concerned. The use of stakeholders' feedback and recommendations are made possible by cyber-attack appropriateness and adequacy assessment.

4.7 Communicating Cyber Attack and Prevention Outcomes to Stakeholders

This requirement is important, and can be used during two different situations. The first situation is a pre-cyber-attack situation while the second situation is post-cyber-attack situation. During the pre-cyber-attack situation, organizations are expected to communicate how their cyber-attack prevention framework works and the role of each stakeholder group. In the second situation, organizations are to communicate loopholes in the cyber-attack prevention framework that resulted to the cyber-attack experienced and how the updated cyber-attack prevention framework solves the problems that resulted from the loopholes. Communicating ideas across large organization is a complex task (Smith, 2019).

Heidi et al. (2018) in his article "Expanding the Scope of Strategic Communication: Towards a Holistic Understanding of Organizational Complexity", describes strategic communication as an academic movement that has been formulated as an ambition to break down the silos surrounding closely related communication disciplines and create unifying framework that integrates public relations, organizational communication, marketing communications and other areas" Organizations should communicate strategically to purposefully fulfill their overall missions. This complexity is also applicable to efforts made by organizations to communicate cyber-attack prevention framework across the length and breadth of organizations. The complex nature of cyber-attack threats and the difficulty in knowing the perpetrators and understanding their motives makes the act of communicating cyber-attack prevention frameworks across the length and breadth of organizations a complex endeavor. Aside from this, some aspects of cyber-attack prevention frameworks that organizations may use may be made clandestine. Therefore, it is important to know and understand those that these aspects should be communicated to and how to effectively and efficiently do this without jeopardizing the overall cyber-attack prevention program.

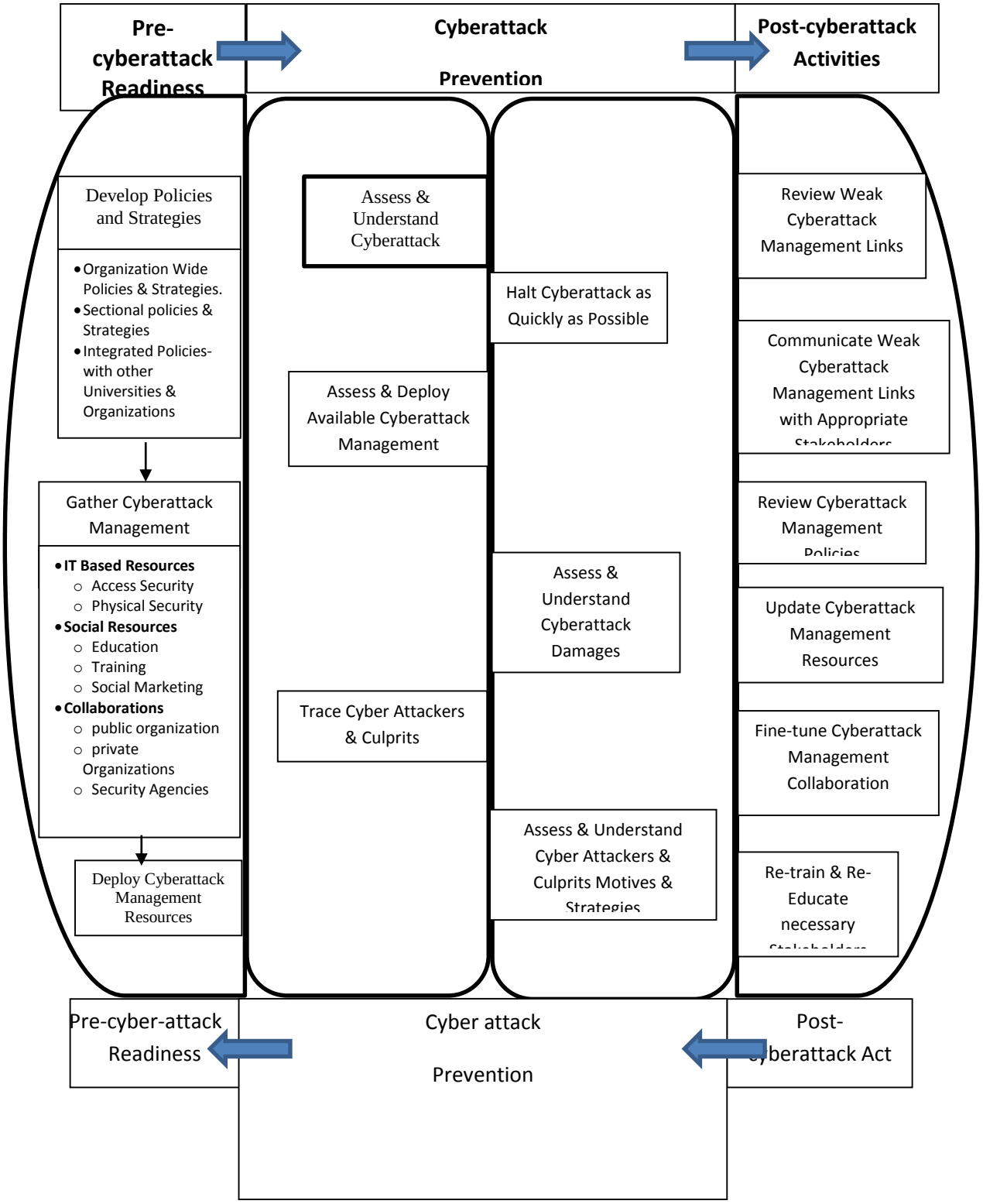

Figure 3: A developed framework for preventing cyber-attack in an organization

CHAPTER 5

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

The chapter presents the summary of the study based on four chapters, conclusions were drawn based on the findings of the research as well as recommendation for improvement On development Of Framework For Prevention Of Cyber Attack in an Organization**,** also in the chapter are suggestions for further study.

5.2 Summary

The study was on the development of framework for prevention of cyber-attack in an organization. the issues raised in the objectives were. copious related literature include books, journals, magazines, Newspapers, internets, etc. the review presented the conceptual framework which consisted of the concept of cybercrime, cyber-attack, cyber security framework, protection of cyber-attack, cyber security attacks in organization and proposed framework of cyber protection from cyber-attack in an organization.

Regarding the research methodology, the study presented research design, population of the study, sample and sampling techniques, instrumentation, validity of the adapted instrument, pilot study, and reliability of the instrument, method of collection and analysis of the collected data from the respondents. They also examined analysis and discussion of data collected from the respondents based on the topic under study with frequency, percentages and interviews of the study.

However, the key variables were operationally defined to conclude the chapter, descriptive survey design was adapted for the study and data was collected using a research-designed questionnaire. The total population of the study consisted of 109.

5.3 Conclusion and Limitation

Cybercrime committed against organizations has increased because of the quick development of cyberspaces and the relocation of businesses' main activities and operations online. Because cyber-attacks target organizations all over the world on a regular basis, businesses must create frameworks for managing them in order to coordinate their cyber-attack prevention initiatives.

This is not to argue that firms do not employ cyber-attack tactics. However, it shows that they must put in a concentrated effort to formalize and record their cyber-attack prevention tactics into frameworks that can be put into use. The framework presented in this study gives Nigerian enterprises solid justification to get started on creating frameworks for sustainable cyber-attacks. Pre-cyber-attack readiness, cyber-attack prevention, and post-cyber-attack activities are the three stages of the framework that the study suggests for organizations.

Each component was divided equally into manageable steps. The framework therefore this paper's drawback is that it is not based on empirical research. It is based on a review of the literature. An empirical study would have offered empirically derived insights on how the suggested framework for preventing cyber-attacks will operate in practical settings. The report and the suggested framework, however, give justification for conducting empirical research on the cyber-attack prevention framework for organizations.