12693154

Ransomware Attacks and its effects on South Africa

Research Proposal

Contents

[Introduction – Project Title 1](#_Toc179222487)

[Significance of the Research & Research Question 1](#_Toc179222488)

[Objectives 2](#_Toc179222489)

[Key Literature 2](#_Toc179222490)

[Methodology / Research Design 2](#_Toc179222491)

[Ethical Considerations 3](#_Toc179222492)

[Timeline 3](#_Toc179222493)

[Conclusion 3](#_Toc179222494)

[References 4](#_Toc179222495)

# Introduction – Project Title

The world of information technology has continually expanded and continues to expand at a rapid pace. With this expansion, comes the rising threat of hackers and malicious users in the world of information technology who will use vulnerabilities they have found to exploit users for their own gain. One of the attacks malicious users have taken advantage of is Ransomware attacks, which can cripple individual users and companies halting their business practices. Ransomware is an attack that holds individual users and companies’ data and technology hostage by encrypting the data on their devices and demand a ransom to be paid for the data to be decrypted. Laws and governance have been put in place around the world to assist with attacks taking place, however, these laws are not perfect and many businesses are still targeted with these attacks. One of the countries that is still significantly targeted with cyber-attacks is South Africa. This research proposal aims to investigate with the use of research articles, journals and statistics publicly available to research and understand the effects of ransomware attacks and the financial impacts of these attacks on individuals and businesses. Therefore, this project is titled “Ransomware Attacks and its financial effects on South Africa”.

# Significance of the Research & Research Question

The rise of ransomware is a current affair that the country is facing with several major attacks taking place in recent years in South Africa. By investigating the financial damage of these attacks, businesses and users can prepare themselves to mitigate such attacks to prevent their businesses from coming to stand still. Businesses and users can also start to invest into counter measures to ensure if such an attack takes place, there are backups in place to ensure everything continues to function as normal. The significance of this research would also aid South Africa specifically to be educated on the dangers of these attacks as one of the main reasons for South Africa being such a big target is the lack of education surrounding the topic of cyber-attacks and cyber security. This research will also aid the cybercrimes unit of South Africa and cybercrime units worldwide to pick up trends with the attacks potentially aiding law enforcement in bring cybercrime syndicates to justice and assisting those affected by ransomware more effectively. Taking into account the significance of the research and the damage that ransomware can have on a country, the following research question can be extracted and researched: What is the Financial Impact of Ransomware attacks in South Africa? (Lemos, 2024)

# Objectives

This research proposal aims to accomplish the following objectives:

* Identify the threat that is Ransomware. Identifying and analysing the threat that is ransomware will aid in understand the dangers that can come from ransomware.
* Show the impact of the threat in South Africa. There are multiple incidences of ransomware crippling businesses in South Africa stopping all of their business practices causing a sufficient financial loss to the businesses.
* Show the lack of education in South Africa towards the threat. South Africa is a prime target for cyber-attacks because South Africans lack the education towards cyber-attacks and cybersecurity. By bring this awareness forward, companies can take proactive steps educating staff and businesses to protect themselves from these attacks.
* Show the financial impact of the threat in South Africa. This research proposal aims to show the financial impact of these attacks and the cost to business and individuals these attacks can cause.
* Propose a solution. This research proposal aims in the end to provide a solution for the threat assisting businesses and users to effectively mitigating these attacks and the steps to take when facing such an attack.

# Key Literature

As noted in the article written by Van Niekerk in 2017, there has been a rise in cyber attacks and data breaches in recent years, and it can be noted that companies have not taken the approach they need to mitigate these attacks and a lack of education is still prevalent in countries today. It is noted that countries including the United Kingdom, Australia and Kenya all suffer from a lack of protection implementation for cyber security. It was then highlighted that South Africa is now at a very critical point with regards to cyber-attacks. (Van Niekerk, 2017)

Mabunda highlights that even though South Africa is behind in the implementation of protection to mitigate cyber-attacks, South Africa still has taken steps towards the future by implementing the cybercrimes act of South Africa. This act governs most cyber activities that take place in South Africa, however, to date the tribunal that governs the cybercrimes act has not been formed. Meaning that there are no proper regulations governing the act in place allowing for a lot of leniencies in court. However, having no tribunal in place also means that the act as it stated is law, which has caused a lot of issues for South Africa in recent years. (Mabunda, 2017)

There has been a recent incident in South Africa where the South African Blood Testing Services was hit with a ransom attack not only impact the service financially but also placing lives in danger by rendering the National Health Laboratory of South Africa unable to process millions of blood tests. This kind of action poses a great threat to human life and to the financial side of the Blood Testing Service. Many healthcare professionals faced a delay in getting results for their patients and many laboratories were shutting their IT systems down to try and circumvent the attack. Although the police are on the hunt for the perpetrators, it is suspected that the cybercrime group known as the BlackSuit Ransomware Gang were the ones responsible for the attack. (CLULEY, 2024)

# Methodology / Research Design

This research proposal needs to make use of the right methodologies and research design in order to produce an effective research proposal. Considering this, a mixture of the qualitative research method and quantitative research method would work very well for this proposal. Qualitative research involves the collection of non-numerical data such as videos, texts and audio to gather insights towards a problem and generate research ideas. (Bhat, 2024) Quantitative research involves the collection of statistics and raw data to make predictions and test relationships between results. The quantitative research will be essential when analysing the financial losses due to ransomware attacks. (Fleetwood, 2024) These methodologies need to be incorporated with descriptive research design. This focuses on providing detail and accurate descriptions of events that have taken place. This research design can answer questions such as “who”, “what”, “where”, “when” and how but will never answer the why question. This research design will assist in making the final research proposal valid and significant in contributing towards the final research paper. (Singh, 2024)

# Ethical Considerations

While doing the research paper, it is important to understand the ethical issues that can arise from researching this topic. Firstly, any information collected should be anonymous. This is to protect any user or business from having their reputation ruined and to protect any sensitive information that may be shared or exposed while researching the ransomware attacks that have taken place in South Africa. From the other perspective, it is important for research paper to consider that there could be the potential of glamorizing cyber-attacks and cyber-crimes making it enticing for criminals to actually use ransomware attacks to commit cyber-crimes. Therefore, presentation of the results of the research paper needs to be taken into consideration and must be presented in such a manner to try avoid enticing cyber criminals towards ransomware attacks as well as protecting the identity of those affected as much as possible to avoid ruining their reputation any further. (Denison, 2024)

# Timeline

From the publishing of this research proposal, one week will be taken to read through various articles and papers, identifying trends and potential common factors that happen with the ransomware attacks. This can include looking for common targets, common kinds of attacks and common variables. Once this analysis of various articles is complete, the final research paper will be drafted and completed in another week. This leads to a two-week timeline to complete the paper.

# Conclusion

Considering the danger that is imposed by ransomware attacks on users and businesses, it is important to remember to highlight the dangers surrounding these attacks, educate users on how to protect yourself from these attacks and to ensure that sufficient mitigations are in place to make sure that a company does not get crippled when such an attack takes place. However, in order to understand what is required, a depth analysis on the financial impact of ransomware in South Africa needs to be assessed to ensure that sufficient knowledge is gathered to assess the impact and provide the best possible solution.

# References

Bhat, A. (2024) *Qualitative research: Definition, types, methods and examples*, *QuestionPro*. Available at: https://www.questionpro.com/blog/qualitative-research-methods/ (Accessed: 07 October 2024).

CLULEY, G. (2024) *Ransomware attack on blood-testing service puts lives in danger in South Africa*, *Hot for Security*. Available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/ransomware-attack-on-blood-testing-service-puts-lives-in-danger-in-south-africa/ (Accessed: 07 October 2024).

Denison, G. (2024) *Ethical research: Best practices for responsible studies*, *Prolific*. Available at: https://www.prolific.com/resources/ethical-considerations-in-research-best-practices-and-examples (Accessed: 07 October 2024).

Farhat, D. and Awan, M.S. (2021) ‘A brief survey on ransomware with the perspective of internet security threat reports’, *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, 24, pp. 1–6. doi:10.1109/isdfs52919.2021.9486348.

Fleetwood, D. (2024) *Quantitative research: What it is, practices & methods*, *QuestionPro*. Available at: https://www.questionpro.com/blog/quantitative-research/ (Accessed: 07 October 2024).

Lemos, R. (2024) *South Africa Lab still reeling from Ransomware attack*, *South Africa Lab Still Reeling from Ransomware Attack*. Available at: https://www.darkreading.com/cyberattacks-data-breaches/south-africa-healthcare-lab-still-reeling-from-ransomware-attack (Accessed: 07 October 2024).

Mabunda, S. (2017) ‘Cyber extortion, ransomware and the south african cybercrimes and Cybersecurity bill’, *Statute Law Review*, 40(2), pp. 143–154. doi:10.1093/slr/hmx028.

Singh, S. (2024) *What is descriptive research? definition, methods, types and examples*, *Researcher.Life*. Available at: https://researcher.life/blog/article/what-is-descriptive-research-definition-methods-types-and-examples/ (Accessed: 07 October 2024).

Van Niekerk, B. (2017) ‘An analysis of cyber-incidents in South Africa’, *The African Journal of Information and Communication (AJIC)* [Preprint], (20). doi:10.23962/10539/23573.