Plan Overview

*A Data Management Plan created using DMPTool*

**DMP ID:** [https://doi.org/10.48321/D1252C4963](https://doi.org/10.48321/D1252C4963)

**Title:** EXPLORING CYBERSECURITY ATTACKS IN SOUTH AFRICA’S FINANCE SECTOR

**Creator:** Siphokuhle Nhlapo - **ORCID:** [0009-0003-7999-8781](https://orcid.org/0009-0003-7999-8781)

**Affiliation:** The Independent Institute of Education (iie.ac.za)

**Funder:** N/a

**Template:** Digital Curation Centre

**Project abstract:**

The rapid rise of digital financial services such as online payments, cell phone banking, and online banking etc. has led to South Africa’s financial sector being an optimal target for cybercriminals. With the exponential rise of cyber security attacks globally, South Africa finds themselves part and parcel of this threat, and this poses a risk to the country’s financial systems, economic prosperity, and citizen trust.

Understanding the nature, scope, and impact of these cyber threats is essential for developing effective cybersecurity strategies and mitigating risks.

The purpose of this study is to provide an overview of previous attacks in South Africa’s finance sector and the measures needed to prevent future attacks and alleviate any risks.

**Start date:** 02-25-2024

**End date:** 11-04-2024

**Last modified:** 06-10-2024

**Copyright information:**

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customize it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan’s text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal.
Secondary data will be collected to undertake research. According to (Silva Martins et al. 2008), secondary data simply refers to datasets not gathered by the author. Secondary data is used as a data collection method for this research due to:

- Vast range of accessible sources (articles, government publications, books, etc.).
- Simplifying the process of comparing and contrasting past and existing data with my own research for validity.
- Potential to enhance phenomenon-driven research, in this context, for example, it can be used to study previous cybersecurity attacks in South Africa's finance sector.

The use of secondary data in this research is essential in challenging current security measures. Secondary data often includes detailed reports on the effectiveness of existing security measures. By reviewing case studies, incident reports, and analyses conducted by cybersecurity experts and institutions, one can identify the strengths and weaknesses of current security protocols. This data can provide insights into how well current measures are working and where they might be failing, thus enabling a critical evaluation.

Secondary data also provides access to a wide range of solutions that have been tried and tested in different contexts. This includes best practices, technological innovations, and strategic recommendations from industry leaders and academic research. By analyzing successful case studies and expert recommendations, I can compile a comprehensive list of strategies to improve cybersecurity in the finance sector.

Data will be collected using purposive sampling. Purposive sampling focuses on selecting cases that are the most relevant and informative to the research objectives. It aids in:

- Identifying Cases: the selection of cases based on the type of financial institution (banks, insurance companies, credit unions, etc.).
- Ensures Variety: I will be looking at institutions of different sizes, sectors, and incident histories (reputation).
- An example of this is studying and comparing contrasting cases, such as cases of cybersecurity breaches, against cases of successful cybersecurity implementation.

Content and thematic analysis are qualitative research methods that can be used effectively to explore cybersecurity attacks in South Africa's finance sector.

Content analysis can be used for:

- Data Collection: Gather relevant documents, such as incident reports, news articles, policy papers, and expert analysis on cybersecurity attacks in South Africa's finance sector.
- Frequency Analysis: Determine the frequency of different types of attacks, common vulnerabilities, and other key variables. For instance, content analysis can reveal how often certain types of attacks occur and which vulnerabilities are most frequently exploited.
- Trend Identification: Analyse changes over time to identify emerging trends in cybersecurity threats. This can help in understanding how the threat landscape has evolved and predicting future challenges.

Thematic analysis can be used for:

- Searching for Themes: Group the initial codes into broader themes that capture the key aspects of cybersecurity attacks. For example, themes might include "phishing tactics," "organisational vulnerabilities," "incident response strategies," and "regulatory challenges."
Defining and Naming Themes: Define each theme clearly and develop a coherent narrative that explains what each theme encompasses. Provide descriptive names that capture the essence of each theme.

These methods apply to the research paper as it:

- Investigating the History of Cyber-attacks: Use content analysis to categorize and quantify past cyber-attacks. Thematic analysis can help in understanding the broader context and impact of these attacks on the finance sector.
- Challenging Current Security Measures: Identify themes related to the strengths and weaknesses of existing security protocols. Content analysis can highlight specific areas where current measures are failing.
- Providing Solutions: Thematic analysis can uncover best practices and successful strategies from the data. Content analysis can quantify the prevalence of these solutions and their effectiveness.

Due to the use of secondary data in this paper, the data sources and information will be considered as the population. This data will be captured and stored on my local device, but relevant information will be displayed in my paper. The content will be from seminal and non-seminal sources, providing a full view of threat intelligence and threat modelling.

Secondary data is not widely considered as a major risk to research ethics, however, ethical standards still need to be adhered to whilst considering and acknowledging limitations.

The following ethics and limitations will be considered in the research:

- Access to Data: Restricted access to sensitive data owned by financial institutions may constrain the depth of the research.
- Transparency: Maintain transparency in research methods, procedures, and findings to promote accountability and trustworthiness.
- Bias and subjectivity: preconceptions from researchers about the country’s digital landscape may affect the research process.
- Proper interpretation of secondary data, ensuring it's meaning and purpose is not misconstrued.

I will seek verification and access from the relevant sources as well as correctly citing and referencing them.

It will be stored on my local device and backed up on a 1TB hard drive, cloud storage service (Google Drive)

I will ensure that only I may access the paper during editing by limiting permissions and sending "read-only" files when providing drafts.

All data

N/A

Through relevant channels created by the institution.

No
Myself, the researcher

EBSCO Host, Google Scholar, and the IIE Library for article collection. Microsoft PowerPoint for presentations. Microsoft Word for the creation of the final document.
The proposed purpose of this study is to provide a comprehensive overview of previous cybersecurity attacks in South Africa’s finance sector. This involves analysing the types, frequency, and impact of past cyber-attacks on financial institutions in the region. By examining detailed case studies and incident reports, the study aims to identify common vulnerabilities and attack vectors that have been exploited by cybercriminals.

Furthermore, the study seeks to evaluate the effectiveness of current security measures implemented by financial institutions and regulatory bodies. Through a critical assessment of existing protocols and response strategies, the research will highlight areas where current defenses are robust and where they fall short.

In addition to the retrospective analysis, the study aims to propose proactive measures to prevent future cyber-attacks. This includes recommending best practices for enhancing cybersecurity infrastructure, improving incident response capabilities, and fostering a culture of security awareness within organizations.

The study will also address strategies for risk mitigation, emphasizing the importance of continuous monitoring, regular security assessments, and the adoption of advanced technologies such as artificial intelligence and machine learning for threat detection and prevention.

Ultimately, this research aims to provide valuable insights and actionable recommendations for stakeholders in South Africa’s finance sector, including policymakers, financial institutions, and cybersecurity professionals, to enhance their preparedness and resilience against the evolving landscape of cyber threats.

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Anticipated release date</th>
<th>Initial access level</th>
<th>Intended repository(ies)</th>
<th>Anticipated file size</th>
<th>License</th>
<th>Metadata standard(s)</th>
<th>May contain sensitive data?</th>
<th>May contain PII?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anticipated Contribution</td>
<td>Text</td>
<td>Unspecified</td>
<td>Open</td>
<td>None specified</td>
<td>None specified</td>
<td>None specified</td>
<td>None specified</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>