Conducting Risk Analysis and Vulnerability Assessment in the Core Fund System Management at National Social Security Fund

Ahmadi Khamis

Master's Student, College of Business Education, Tanzania

Respeckius Casmir

Lecturer, College of Business Education, Tanzania

Abstract:

The study sought to analyse security risks and assess security vulnerabilities in the NSSF Core Fund System. The study employed descriptive survey design while the study population was 314 staff working at head office of NSSF. In addition to that, purposive and sampling techniques were used to select 89 who were members of sample size. In addition to that questionnaire and interview were used to solicit data from the respondents while data were analysed using descriptive and content analysis. The study found that security risks and vulnerabilities associated with the core fund system included cyber-attacks, disclosure of sensitive data and hardware failure, others said viruses, internal security threats and internal accidental threats. In the similar case, some said system administration errors. The study also indicated that existence of information security risks had been in different period of time depending on the type of such information security risks. The study concluded that enhancing information security in the Core Fund System utilized by the National Social Security Fund (NSSF) is crucial for safeguarding the data of both the staff and customers. This can be achieved by regularly updating the records of customers and staff members to ensure their information remains reliable. The increasing reliance on computers, mobile devices, and digitalization of business operations necessitates a knowledgeable manager who understands the vulnerabilities and threats to data and information assets. Such a manager can then develop strategies to mitigate risks and protect the organization’s data and assets. The study recommended that it is important for organizations to continue providing training to their staff regarding security policies and guidelines for information systems. This will help raise awareness about security risks and allow for the evaluation of vulnerabilities in the NSSF Core Fund System. As a result, it is necessary to establish standards and guidelines that promote the adoption of best practices in information security, ultimately achieving a satisfactory and sufficient level of security.

Keywords: risk, analysis, vulnerabilities, core fund system, management, NSSF.

Introduction

It is widely accepted worldwide that managing risk is a crucial concern for organizations aiming to enhance their performance (Tang, 2018). Conversely, social security funds play a crucial role in a nation's welfare system, offering financial assistance and benefits to its populace. Nevertheless, these funds face numerous security risks and vulnerabilities. A significant breach in 2017 involving the United Kingdom's...
National Health Service impacted around 26 million individuals, exposing personal data like social security numbers and medical records (Michael, 2017).

The social security funds in Tanzania, designed to provide financial support and stability to individuals and families in times of need, are facing significant security risks and vulnerabilities within their core fund system. These risks and vulnerabilities pose a substantial threat to the integrity and functionality of the social security funds, potentially compromising the financial well-being of beneficiaries and undermining public trust in the system (Rathaus, 2019). For example, unauthorized access whereas the core fund system is susceptible to unauthorized access by malicious actors, including hackers and cybercriminals. Such breaches could result in unauthorized modifications, theft of sensitive information, or disruption of fund operations. Also data data breaches whereas inadequate data protection measures expose personal and financial information of beneficiaries to potential breaches. This could lead to identity theft, fraud, and financial loss for individuals reliant on social security funds (Osiro, 2017). In addition to that, the presence of vulnerabilities within the system may enable fraudulent activities, such as the creation of fictitious beneficiaries, false claims, or manipulation of benefit calculations. This can drain resources from the fund and reduce the available support for genuine beneficiaries (Karokola, & Yngström, 2019).

Methods

This study used descriptive design. Descriptive studies aim to provide a description or definition of a subject by creating a profile of a group of problems, individuals, or events. This is achieved through data collection and the tabulation of frequencies related to research variables or their interactions (Cooper & Schindler, 2013). The sample size of the study was 89 respondents. The determination of this study’s sample size was based on Slovin’s formula, taking into account a confidence level of 91% and a margin of error of 9% (1-0.09). The formula can be expressed as follows:

\[ n = \frac{N}{(1+Ne)^2} \]  

Where: \( n \) = is number of sample (required)  
\( N \) = Total population (314) and  
\( e \) = Error tolerance (level) or margin of error (0.09)

Using above formula, the sample size is calculated as indicated below;  
\[ 314/ (1+314(0.09)^2) = 314/3.5434 = 88.6154 \]

Therefore, the sample size for this study was 89 respondents.

Table 1. Sample size distribution

<table>
<thead>
<tr>
<th>Respondents</th>
<th>Population</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>11</td>
<td>3</td>
<td>3.4</td>
</tr>
<tr>
<td>Operational staff</td>
<td>303</td>
<td>86</td>
<td>96.6</td>
</tr>
<tr>
<td>Total</td>
<td>314</td>
<td>89</td>
<td>100</td>
</tr>
</tbody>
</table>

Source: Field Data, 2023

Furthermore, purposive and sampling techniques were used to select 89 who were members of sample size. In addition to that questionnaire and interview were used to solicit data from the respondents while data were analysed using descriptive and content analysis.
Results

This part shows the demographic information of the respondents involved in the study. It provides general information about the respondents who took part in this research, such as their gender, age, level of education and work experience.

Demographic Characteristics

Table 2. Demographic Information of the Respondents

<table>
<thead>
<tr>
<th>Character</th>
<th>Category</th>
<th>Frequency</th>
<th>Percent (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Age</strong></td>
<td>18 – 25 years</td>
<td>07</td>
<td>8.0</td>
</tr>
<tr>
<td></td>
<td>26 – 35 years</td>
<td>26</td>
<td>29.0</td>
</tr>
<tr>
<td></td>
<td>36 – 45 years</td>
<td>39</td>
<td>44.0</td>
</tr>
<tr>
<td></td>
<td>46+ years</td>
<td>17</td>
<td>19.0</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
<td>64</td>
<td>78.0</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>25</td>
<td>22.0</td>
</tr>
<tr>
<td><strong>Level of education</strong></td>
<td>Certificate</td>
<td>06</td>
<td>6.8</td>
</tr>
<tr>
<td></td>
<td>Diploma</td>
<td>20</td>
<td>22.5</td>
</tr>
<tr>
<td></td>
<td>Degree</td>
<td>45</td>
<td>50.6</td>
</tr>
<tr>
<td></td>
<td>Postgraduate</td>
<td>18</td>
<td>20.2</td>
</tr>
<tr>
<td><strong>Working experience</strong></td>
<td>1-5 years</td>
<td>19</td>
<td>21.3</td>
</tr>
<tr>
<td></td>
<td>6-10 years</td>
<td>59</td>
<td>66.3</td>
</tr>
<tr>
<td></td>
<td>Above 11 years</td>
<td>11</td>
<td>12.4</td>
</tr>
</tbody>
</table>

Source: Field Data (2023)

Table 2 indicated that 7 respondents, accounting for 8% of the total, fell within the age range of 18 to 25 years. Similarly, 26 respondents, equivalent to 22.2%, were between the ages of 26 and 35. Furthermore, 39 respondents, comprising 44% of the total, were aged between 34 and 45, while 17 respondents, representing 20%, were 46 years old or older. The findings indicate that 80% of participants were below the age of 45. The study specifically included individuals who were mature and of sufficient age to provide meaningful responses to the questionnaires distributed. Also according to the results, 64 respondents (72%) were male, while 25 respondents (28%) were female. This ratio indicates that the majority of respondents were of the male gender, which dominates the research in terms of representing the interests of both genders in the population. Meanwhile, the findings revealed that 06 participants, accounting for 6.7%, possess a certificate as their highest educational qualification. Additionally, 20 participants, representing 22.5%, hold a diploma.

The majority of respondents, 45 in total, which corresponds to 50.6%, have a bachelor's degree. Furthermore, 18 respondents, equivalent to 20.2%, possess a postgraduate degree. These results demonstrate that the data collected for this study came from a diverse group of participants with varying levels of education, providing reliable and valuable information for the researcher. Also the results indicate that out of the total respondents, 03 individuals, which accounts for 6.6%, had job experience ranging from 1 to 3 years in their current roles. Additionally, 09 respondents, or 20%, had work experience between 4 and 6 years, while 22 participants, equivalent to 48.8%, had experience spanning 7 to 10 years. Furthermore, 11 respondents, making up 24.5%, possessed experience exceeding 10 years. This suggests that the majority of the study's participants have sufficient experience to comprehend the performance of the procurement unit because they were able to comprehend questions about
Security Risks and Vulnerabilities Associated with the Core Fund System

This section presents security risks and vulnerabilities associated with the core fund system. The study revealed that about 6(8.2%) said cyber-attacks while 26% said disclosure of sensitive data and 15.1% said hardware failure. On the other hand, the study indicated that about 0.5% said viruses, 9.6% said internal security threats and 16.4% said internal accidental threats. In addition to that, the study revealed that about 34.1% said system administration errors. From that point of view, it can be said that respondents had different views regarding to the information security risks associated with the core fund system at NSSF. While some said cyber-attacks, disclosure of sensitive data and hardware failure, others said viruses, internal security threats and internal accidental threats. In the similar case, some said system administration errors.

Figure 1. Identified information security risks
Source: Field Data (2023)

Duration of Information Security Risks

In this category of question, respondents were asked to state duration in which information security risks have existed at NSSF. In that regard, the study findings are therefore presented in Figure 2.

Figure 2. Duration of information security risks
Source: Field Data (2023)
It was established that, about 8.2% said cyber-attacks is more current while 26% said disclosure of sensitive data had been existing for a long time and 15.1% said hardware failure had been existing and occurring frequently and 20.5% said viruses had been existing and occurring frequently. Also the study revealed that 9.6% said internal security threats had not been occurring frequently while 16.4% aid insider accidental threats had not been existing frequently and the rest with 4.1% said system administration errors had been existing or occurring frequently. To sum up, it can be said that the existence of information security risks had been in different period of time depending on the type of such information security risks.

Discussion

Findings obtained through questionnaire indicated that there are different types of risks that exist. It is considered that cyber-attacks are deliberate actions by malicious individuals or groups to gain unauthorized access to computer systems, networks, or data with the intention of causing disruption, stealing sensitive information, or causing other harm. Cyber-attacks can take various forms, including hacking, phishing, malware attacks, ransomware, and denial-of-service (DoS) attacks. With reference to disclosure of sensitive data, this risk involves the unintentional or unauthorized disclosure of confidential or sensitive information. It can occur through data breaches, insider threats, social engineering, or inadequate security controls. The exposure of sensitive data can lead to financial loss, reputational damage, legal consequences, and violations of privacy regulations.

With reference to hardware failure, hardware failures can occur due to various reasons such as power surges, component malfunctions, natural disasters, or physical damage. When critical hardware components fail, it can disrupt business operations; result in data loss, or cause system downtime. Redundancy, regular backups, and disaster recovery plans can help mitigate the impact of hardware failures. With reference to the viruses, Viruses are malicious software programs designed to replicate them and infect computer systems. They can be spread through infected files, email attachments, or malicious websites. Viruses can cause damage to data, software, and hardware components, leading to system instability, data loss, and unauthorized access. Antivirus software, regular system updates, and user education can help defend against viruses. On the issue of internal security threats, these risks arise from within an organization and involve employees or insiders with authorized access to systems and data. Insider threats can be intentional, such as data theft by disgruntled employees, or unintentional, such as employees inadvertently exposing sensitive information. Implementing access controls, monitoring user activities, and conducting employee training and awareness programs can help mitigate internal security threats. On the issue of internal accidental threats, accidental threats refer to security incidents caused by unintentional actions or mistakes by employees. For example, an employee may accidentally delete important files, send sensitive information to the wrong recipient, or fall victim to a phishing attack. Training programs, data backup procedures, and implementing preventive measures like email filters and file permission controls can help mitigate accidental threats.

Moreover, existence of information security risks had been in different period of time depending on the type of such information security risks. It is considered that information security risks that exist over a long period can significantly affect organization. In that regard, if there is an accumulation of vulnerabilities and if an organization fails to regularly update and patch its systems, these vulnerabilities can accumulate, increasing the risk of successful cyber-attacks. Attackers may exploit outdated software versions, unpatched systems, or known vulnerabilities that were not addressed. In the similar case, risks that existed in the past may become more potent as attackers find innovative ways to exploit them. If an organization does not
continuously assess and adapt its security measures to address new threats, it can become increasingly vulnerable over time.

According to Mawala (2017), organizations that rely on outdated or legacy systems may struggle to keep up with emerging security requirements and fail to adequately protect their information assets. As technology evolves, organizations need to update their security measures and processes to ensure compatibility and resilience against new threats. Information security risks that persist over time increase the chances of data breaches and the compromise of sensitive information. Attackers may exploit known vulnerabilities or employ persistent attack techniques, gradually gathering information and compromising systems over an extended period. The longer an organization remains exposed to such risks, the higher the likelihood of a successful breach, leading to financial losses, reputational damage, legal consequences, and regulatory non-compliance. Also James (2018) revealed that, to mitigate the impact of long-standing information security risks, organizations should adopt a proactive and continuous approach to security. This includes regularly updating and patching systems, staying informed about emerging threats, investing in robust security measures, conducting risk assessments, training employees on security best practices, and complying with relevant regulations. By actively managing and addressing risks, organizations can minimize the potential negative consequences of long-term security vulnerabilities.

Conclusion

The results obtained from this study revealed that enhancing information security in the Core Fund System utilized by the National Social Security Fund (NSSF) is crucial for safeguarding the data of both the staff and customers. This can be achieved by regularly updating the records of customers and staff members to ensure their information remains reliable. The increasing reliance on computers, mobile devices, and digitalization of business operations necessitates a knowledgeable manager who understands the vulnerabilities and threats to data and information assets. Such a manager can then develop strategies to mitigate risks and protect the organization's data and assets. The study suggests that it is important for organizations to continue providing training to their staff regarding security policies and guidelines for information systems. This will help raise awareness about security risks and allow for the evaluation of vulnerabilities in the NSSF Core Fund System. As a result, it is necessary to establish standards and guidelines that promote the adoption of best practices in information security, ultimately achieving a satisfactory and sufficient level of security. The study indicates a lack of awareness among NSSF staff members regarding the analysis of security risks and assessment of vulnerabilities in the NSSF Core Fund System. Consequently, senior management should allocate additional resources to enhance staff awareness of information system security. They should also develop effective policies and guidelines to ensure accountability for both staff members and the protection of customer information.

References


