ISRG Journal of Economics, Business & Management (ISRGJEBM)

ISRG PUBLISHERS

Abbreviated Key Title: Isrg J Econ Bus Manag

ISSN: 2584-0916 (Online)

Journal homepage: https://isrgpublishers.com/isrgjebm/

Volume – IV Issue - V (September-October) 2026

Frequency: Bimonthly

CYBERSECURITY RISKS AND THEIR IMPLICATIONS FOR FINANCIAL INFORMATION INTEGRITY IN NIGERIAN FIRMS.

Maxwell Smith OGBOTOR Ph.D[1*], IZEDIKE Wealth[2]

[1, 2] Department of Accounting, Faculty of management Science Delta State University, Abraka Delta State, Nigeria.

| **Received:** 10.09.2026 | **Accepted:** 17.09.2026 | **Published:** 20.09.2026

***Corresponding author:** Maxwell Smith OGBOTOR Ph.D

Abstract

This study examined the effect of cybersecurity risks on the integrity of financial information in Nigerian firms. The study specifically focused on four major cybersecurity risks: malware attacks, social engineering attacks, insider threats, and ransomware attacks, and their effects on the accuracy, reliability, completeness, and consistency of financial information. A quantitative survey research design was adopted for the study. Data were collected through structured questionnaires administered to respondents in selected Nigerian firms. The data collected were analyzed using descriptive statistics and multiple regression analysis at a 5% level of significance. The findings revealed that malware attacks, social engineering attacks, insider threats, and ransomware attacks have significant negative effects on financial information integrity. The regression analysis showed that the four cybersecurity risk factors collectively explained 47.2% of the variation in financial information integrity, while the overall regression model was statistically significant. The study concludes that cybersecurity risks constitute a significant threat to the integrity of financial information in Nigerian firms. It therefore recommends that firms strengthen cybersecurity controls, regularly update security systems, provide continuous cybersecurity awareness and training for employees, implement effective access controls, maintain regular data backups, and conduct periodic security assessments to protect financial information from cyber threats.

Keywords: *Cybersecurity, Risks, Integrity, Insider, Ransomware, Firm.*

1. INTRODUCTION

Over the past two decades, the rapid expansion of digital technologies has transformed how modern organizations operate, communicate, and manage financial information. Nigerian firms, like their counterparts across the world, have embraced digital systems to enhance business efficiency, reduce operational costs, and improve financial transparency (Aderibigbe & Ojo, 2021). The increasing reliance on digital platforms ranging from electronic accounting systems and enterprise resource planning (ERP) software to online banking, cloud computing, and automated financial reporting has undeniably improved business processes. However, this digital transformation has also introduced a new and

DOI: 10.5281/zenodo.22852901

growing challenge: the rise of cybersecurity risks that directly threaten the confidentiality, reliability, and overall integrity of financial information (Okon & Effiong, 2020). Cybersecurity risks refer to potential threats that exploit vulnerabilities within an organization's information systems, thereby compromising data, disrupting operations, or enabling unauthorized access (Adewuyi, 2022). These risks include malware attacks, ransomware, phishing schemes, insider threats, denial-of-service attacks, password breaches, identity theft, and manipulation of financial records. As Nigerian firms move deeper into technologically advanced operations, they become increasingly exposed to the dangers associated with cybercrime, which has grown in sophistication and frequency nationwide (Ovat & Idemudia, 2023). The financial sector, manufacturing firms, telecommunications companies, and even small businesses have witnessed a spike in cyber-related attacks aimed primarily at tampering with financial information.

Financial information integrity refers to the accuracy, reliability, completeness, and consistency of financial data used by firms for decision-making, reporting, auditing, and strategic planning (Obi & Nwankwo, 2020). It is a critical component of corporate governance, investor confidence, and sustainable business performance. When financial data is distorted, manipulated, or accessed by unauthorized individuals, organizations face significant consequences, including financial losses, reputational damage, legal sanctions, and operational disruptions. For this reason, protecting the integrity of financial information has become a central concern for stakeholders across Nigeria's business ecosystem (Ahmed & Yusuf, 2021; Apete & Orimuo, 2026). Nigeria has experienced substantial growth in cybercrime activities, driven partly by improved internet penetration, technological adoption, and the increasing monetization of cyber-attacks (Ibrahim & Abdullahi, 2022). Reports from the Nigeria Inter-Bank Settlement System (NIBSS) indicate a year-on-year increase in fraud attempts, particularly through electronic channels such as mobile banking, web payments, and automated systems (NIBSS, 2021). While banks remain the primary targets, non-financial firms are also affected due to their reliance on digital financial records, cloud-based accounting tools, and online transaction platforms. The interconnectivity of business systems means that even the smallest security breach can compromise sensitive financial data and create ripple effects throughout the organization (Eke & Onukwufor, 2023; Aroghene 2023). In many Nigerian firms, cybersecurity systems have not evolved at the same pace as technological adoption. Several organizations lack adequate firewalls, intrusion detection systems, encryption protocols, continuous monitoring tools, or skilled cybersecurity personnel (Oluwafemi & Balogun, 2021). This gap makes them susceptible to data breaches, cyber espionage, and financial manipulation. Scholars argue that weaknesses in cybersecurity governance, poor policy compliance, underinvestment in digital defense, and limited awareness among employees contribute to the increasing vulnerability of Nigerian firms (Nwachukwu & Igbokwe, 2022; Imene, 2023). Consequently, financial information stored within these digital systems becomes an easy target for attackers. The human element also plays a significant role in cybersecurity risks. Employees often unintentionally expose firms to cyber threats through weak passwords, unsafe browsing habits, sharing confidential data, or falling victim to phishing attacks (Adekunle & Jimoh, 2021). Insider threats whether deliberate or accidental have become one of the most pressing concerns for firms because internal users often possess access privileges that can easily be exploited to distort financial information or leak sensitive data (Okeke & Abata, 2020; Ogbotor & Nwabudo, 2025). This makes it even more challenging to safeguard financial information integrity in a digital environment.

Given the growing sophistication of cyber criminals and the widening digital footprint of Nigerian firms, ensuring financial information integrity has become both a managerial and technological challenge. Scholars argue that financial data integrity cannot be achieved without a strong cybersecurity architecture that incorporates technological tools, human awareness, organizational policies, and regulatory compliance (Ezenwa & Nwosu, 2024). Regulatory bodies in Nigeria including the Central Bank of Nigeria (CBN), the National Information Technology Development Agency (NITDA), and the Securities and Exchange Commission (SEC) have developed several guidelines aimed at strengthening cybersecurity frameworks for organizations (NITDA, 2020; CBN, 2022). These policies emphasize data protection, risk assessment, incident reporting, and system security. However, compliance remains inconsistent across firms due to cost barriers, inadequate training, and limited enforcement (Chukwuma & Ezenwa, 2023; Ogbotor, 2025; Imene & Ikenga, 2024). As a result, many organizations continue to face challenges in maintaining a strong cybersecurity posture capable of protecting their financial information from emerging cyber threats.

Despite the growing research on cybersecurity and financial management globally, limited empirical studies have specifically examined how cybersecurity risks affect the integrity of financial information within Nigerian firms. Many existing Nigerian studies focus on cybercrime generally, electronic fraud, employee awareness, or banking security, but fewer examine the direct relationship between cybersecurity threats and the reliability of financial information across industries (Adejumo & Fapohunda, 2023). This study investigates the implications of cybersecurity risks on financial information integrity within Nigerian firms. It provide evidence-based insights into how cyber threats impact financial records, the nature of vulnerabilities present in Nigerian businesses, and the measures necessary to safeguard financial data in an increasingly digital economy.

Objectives of the Study

The main objective of the study is to examine the effect of cybersecurity risks on the integrity of financial information in Nigerian firms. The specific objectives is to:

i. determine the extent to which malware attacks influence the integrity of financial information in Nigerian firms.

ii. examine how social engineering attacks affect the integrity of financial information in Nigerian firms.

iii. assess how insider threats influence the integrity of financial information in Nigerian firms.

iv. evaluate the effect of ransomware attacks on the integrity of financial information in Nigerian firms.

Research Questions

The study raised the following research questions:

1. How does malware attacks influence the integrity of financial information in Nigerian firms?

2. How does social engineering influence the integrity of financial information in Nigerian firms?

DOI: 10.5281/zenodo.22852901

3. How does insider threats influence the integrity of financial information in Nigerian firms?
4. How does ransomware attacks influence the integrity of financial information in Nigerian firms?

Research Hypotheses

The following hypotheses are formulated in their null forms:

H_{01}: Malware attacks have no significant influence on the integrity of financial information in Nigerian firms.

H_{02}: Social engineering attacks have no significant effect on the integrity of financial information in Nigerian firms.

H_{03}: Insider threats have no significant influence on the integrity of financial information in Nigerian firms.

H_{04}: Ransomware attacks have no significant effect on the integrity of financial information in Nigerian firms.

2. LITERATURE REVIEW

2.1 Conceptual Review

Cybersecurity

Cybersecurity is a multidisciplinary concept that refers to the set of technologies, processes, practices, and controls designed to protect computer systems, networks, programs, and data from unauthorized access, attack, damage, or disruption. In today's digital-driven economy, cybersecurity has become a fundamental requirement for organizations, particularly those that rely heavily on electronic data processing and digital financial systems. It ensures that sensitive organizational information, especially financial data, is safeguarded from both internal and external threats that could compromise its confidentiality, integrity, and availability (Davis, 1989; Ezenwa & Nwosu, 2024). Cybersecurity also involves both preventive and responsive measures. Preventive measures are designed to stop cyberattacks before they occur, while responsive measures focus on mitigating damage after a breach has taken place. Preventive mechanisms include firewalls, antivirus software, encryption techniques, intrusion detection systems, and secure authentication protocols. Responsive mechanisms, on the other hand, include incident response planning, disaster recovery systems, and forensic analysis tools (Ezenwa & Nwosu, 2024). These combined measures ensure that organizations can maintain operational continuity even in the event of cyber incidents. In addition to technological safeguards, cybersecurity also encompasses human and organizational factors. Research has shown that many cybersecurity breaches occur not as a result of system failure, but due to human error or manipulation (Adekunle & Jimoh, 2021; Ogbotor, 2025). From an organizational perspective, cybersecurity is closely linked to risk management. Every organization that uses digital systems faces potential cyber risks, and cybersecurity provides the framework for identifying, assessing, and mitigating these risks. According to Nwachukwu and Igbokwe (2022), effective cybersecurity governance ensures that organizations adopt structured policies and procedures to minimize exposure to cyber threats while maintaining operational efficiency. This is particularly important in sectors such as banking, finance, and telecommunications, where large volumes of sensitive financial data are processed daily.

Types of Cybersecurity in Firms

Cybersecurity in modern organizations is not a single, uniform practice but a combination of different protective measures designed to secure various components of information systems. Each type of cybersecurity addresses a specific layer of protection within an organization's digital infrastructure. In firms that rely heavily on digital financial systems, such as accounting software, enterprise resource planning (ERP) systems, and online banking platforms, these cybersecurity types work together to ensure the safety of financial information and maintain data integrity (Adewuyi, 2022). One of the most fundamental types is network security, which focuses on protecting the internal and external networks of an organization from unauthorized access, misuse, or attacks. Network security tools include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and virtual private networks (VPNs). These tools help regulate traffic flow and ensure that only authorized users can access sensitive systems (Okon & Effiong, 2020; Apete & Ogeh, 2026).

Another category is application security, which is concerned with securing software applications used within organizations. Financial applications such as accounting software, payroll systems, and banking platforms are common targets for cybercriminals due to the sensitive nature of the data they process. Application security involves identifying and fixing vulnerabilities in software codes, implementing secure coding practices, and regularly updating applications to prevent exploitation (Eze & Nwosu, 2022). Also, information security is a type of cybersecurity that focuses directly on protecting data, regardless of whether it is in storage, processing, or transit. This type of security ensures that financial information remains confidential, accurate, and unaltered. Techniques such as encryption, access control, authentication mechanisms, and data masking are commonly used to protect sensitive financial data from unauthorized access (Oluwafemi & Balogun, 2021; Aroghene et al., 2025). Another significant type is cloud security. cloud security focuses on protecting data stored and processed in cloud computing environments. Many modern firms in Nigeria now rely on cloud-based systems for financial data storage and business operations. While cloud computing offers flexibility and cost efficiency, it also introduces new vulnerabilities if not properly secured. Despite these differences, it is clear that all types of cybersecurity are interconnected and collectively contribute to the protection of financial information integrity. A weakness in one area, such as endpoint security, can expose the entire system to threats such as malware attacks or ransomware infections. Therefore, firms are expected to adopt a holistic cybersecurity approach that integrates all security types into a unified defense strategy (Ezenwa & Nwosu, 2024).

Cybersecurity Threats and Financial Data Vulnerability

Cybersecurity risks have become one of the most significant threats to financial information integrity in contemporary organizations. Cybersecurity threats refer to malicious activities, actions, or events that are designed to disrupt, damage, or gain unauthorized access to information systems and digital resources. In organizational environments, these threats pose significant risks to the confidentiality, integrity, and availability of financial information. These threats include malware attacks, ransomware, insider threats and social engineering

Malware consist of viruses, worms, and spyware designed to infiltrate computer systems and disrupt normal operations. In

DOI: 10.5281/zenodo.22852901

financial systems, malware can corrupt accounting records, delete transaction histories, or secretly transmit sensitive financial data to unauthorized users. In financial systems, malware can corrupt accounting records, delete transaction histories, or secretly transmit sensitive financial data to unauthorized users. Once a system is infected, the integrity of financial records becomes questionable, as data may be altered without detection (Afolabi & Oladimeji, 2022).

Ransomware is a type of malicious software that encrypts an organization's data and demands payment before access is restored. In financial environments, ransomware can completely lock accounting systems, preventing access to financial records and disrupting business operations. This not only affects data availability but also raises concerns about the integrity of financial information, especially if data is altered or lost during recovery attempts (Ajepe, Agbi & Mustapha, 2021).

Insider threats represent a serious cybersecurity risk to financial information. These threats occur when employees, contractors, or authorized users intentionally or unintentionally misuse their access to organizational systems. Insider threats involve data manipulation, theft of financial records, unauthorized transactions, or negligence in handling sensitive information. Since insiders already have legitimate access to systems, their actions are often harder to detect and can cause more damage than external attacks (Okeke & Abata, 2020).

Social engineering attacks target individuals within an organization rather than technical systems. These attacks rely on psychological manipulation to trick employees into revealing confidential financial information such as passwords, bank details, or access credentials. Techniques such as phishing emails, impersonation, and deceptive communication are commonly used. Because these attacks exploit human behavior, they are often difficult to detect and prevent, making them a significant risk to financial data integrity (Adejumo & Fapohunda, 2023; Aroghene & Obiekea, 2025).

These risks directly undermine the integrity of financial information and can result in financial losses and reputational damage (Ajepe, Agbi & Mustapha, 2021). In the Nigerian business environment, maintaining financial information integrity is particularly challenging due to the increasing rate of cybercrime and limited cybersecurity infrastructure in many firms. Organizations often struggle with inadequate internal controls, limited cybersecurity awareness among employees, and insufficient investment in security technologies. These challenges increase the likelihood of financial data manipulation or loss (Adegboye, Adelekan & Salami, 2021). Furthermore, regulatory frameworks such as the Nigeria Data Protection Regulation (NDPR) emphasize the importance of protecting personal and financial data from unauthorized access and misuse. Compliance with such regulations helps firms strengthen their data governance structures and improve the integrity of financial information.

2.2 Theoretical Review

Systems Theory

Systems Theory was propounded by Ludwig von Bertalanffy in 1968 through his seminal work titled General System Theory: Foundations, Development, Applications. He argued that systems should be understood as wholes made up of interdependent parts rather than isolated components, because the interaction among parts produces outcomes that cannot be explained individually (Von Bertalanffy, 1968). The central idea of Systems Theory is that every organization or phenomenon is a system composed of interrelated and interdependent subsystems that work together to achieve a common goal. These systems continuously interact with their environment by receiving inputs, processing them, and producing outputs, while also receiving feedback for adjustment and improvement. This interaction makes systems dynamic rather than static, meaning that a change in one part of the system affects the entire structure (Von Bertalanffy, 1968; Skyttner, 2005). In relation to organizational settings, Systems Theory views a firm as an integrated structure made up of various subsystems such as finance, operations, human resources, and information systems. Each subsystem contributes to overall organizational performance. Therefore, any disruption in one subsystem can affect the entire organization. This perspective is particularly relevant to financial systems, where data integrity depends on the smooth interaction between technology, employees, and internal controls.

Furthermore, Systems Theory helps explain that financial information integrity cannot be protected in isolation. Instead, it depends on the interaction between technological controls, human behavior, and organizational policies. A weakness in any part of the system such as employee negligence or weak cybersecurity infrastructure can compromise the entire financial reporting system. Therefore, Systems Theory provides a strong conceptual foundation for this study as it explains how interconnected organizational components collectively influence financial information integrity in the presence of cybersecurity threats.

Fraud Triangle Theory

Fraud Triangle Theory was propounded by Donald R. Cressey in 1953 in his classical work titled Other People's Money: A Study in the Social Psychology of Embezzlement. He concluded that fraud does not occur randomly but is driven by three interrelated factors: pressure, opportunity, and rationalization. The first element, pressure, refers to the motivation or incentive that pushes an individual to commit fraud. This pressure may arise from financial difficulties, personal obligations, or organizational performance expectations. The second element, opportunity, occurs when an individual perceives a weakness in the system that allows fraud to be committed without immediate detection. Weak internal controls, poor supervision, and inadequate cybersecurity systems create such opportunities. The third element, rationalization, refers to the mental process through which individuals justify their unethical behavior, often convincing themselves that the act is acceptable under the circumstances. Fraud Triangle Theory is widely applied in accounting, auditing, and information systems security because it helps explain why individuals engage in fraudulent activities within organizations. It highlights that fraud is not only a result of personal character but also a consequence of organizational weaknesses that create enabling environments for unethical behavior. In the Nigerian business environment, the relevance of Fraud Triangle Theory is particularly evident due to weak internal control systems, limited cybersecurity awareness, and increasing reliance on digital financial systems. These conditions create significant opportunities for fraud and cyber-related financial manipulation. As a result, organizations become vulnerable to data breaches that directly affect the integrity of financial information.

Information Security Management Theory

Information Security Management Theory is rooted in the works of Rossouw von Solms and Basie von Solms (2008), who advanced

DOI: 10.5281/zenodo.22852901

the concept of structured information security governance in their publication Information Security Governance: A Model Based on the Balanced Scorecard. The theory emphasizes that information security is not merely a technical function but a strategic management responsibility that must be integrated into organizational governance, risk management, and operational processes. The core idea of the theory is that organizations must implement a systematic and continuous approach to protecting information assets through policies, procedures, technologies, and human behavioral controls. Information Security Management Theory further stresses that cybersecurity should be treated as an ongoing process rather than a one-time implementation. This involves continuous risk assessment, monitoring of threats, enforcement of security policies, and regular updates of security infrastructure. The theory also supports the use of governance frameworks that assign responsibility and accountability for information protection at all levels of the organization.

The theory provides a structured explanation of how organizations can manage cybersecurity risks such as malware attacks, ransomware attacks, insider threats, and social engineering attacks. These risks directly threaten the integrity of financial information systems in Nigerian firms. The theory explains that without a well-structured security management system, financial data becomes highly vulnerable to unauthorized access, manipulation, and destruction. For example, malware and ransomware attacks can be mitigated through strong security policies, regular system updates, and effective incident response strategies. Insider threats can be controlled through access management systems, segregation of duties, and continuous monitoring. Social engineering attacks can be reduced through employee training and awareness programs. All these measures fall within the scope of information security management practices.

2.3 Empirical Review

Global Studies

One significant study was conducted by Smith, Jones, and Clark (2022) in the United States, which examined the impact of cyberattacks on corporate financial reporting accuracy. The study adopted a quantitative research design using survey data from 120 medium and large-scale firms. Findings revealed that organizations experiencing frequent malware and ransomware attacks reported higher instances of financial data distortion and reporting delays. The study concluded that cybersecurity breaches significantly reduce the reliability of financial information systems, thereby affecting decision-making processes. Brown and Williams (2021) investigated cybersecurity vulnerabilities and financial data integrity in European financial institutions. Using panel data analysis, the study found that insider threats were among the most damaging risks to financial integrity due to their internal access privileges. The study emphasized that weak internal controls significantly increase the likelihood of financial data manipulation. It recommended stronger governance frameworks and continuous employee monitoring to reduce insider-related risks. Kim and Park (2023) examined the relationship between ransomware attacks and financial system disruption in South Korean corporations. The study employed case study analysis and found that ransomware incidents not only disrupt operational continuity but also compromise the integrity of financial records during recovery processes. The study highlighted that organizations often experience partial data loss or corruption even after ransom payments are made, thereby affecting the credibility of financial reports. Furthermore, Garcia and Lopez (2020) in Spain conducted a study on social engineering attacks and organizational data security. Their research revealed that phishing and impersonation attacks remain one of the most successful methods used by cybercriminals to gain access to financial systems. The study showed that employee awareness levels significantly influence the success or failure of such attacks. Organizations with low cybersecurity awareness experienced higher rates of financial data breaches.

Johnson et al. (2021) in Canada explored the role of cybersecurity governance in protecting financial information integrity. The study used regression analysis to assess the relationship between cybersecurity investment and data protection outcomes. Findings indicated that firms with stronger cybersecurity governance frameworks experienced significantly fewer data integrity breaches compared to firms with weak or poorly implemented security policies. Ahmed and Khan (2022) in the United Kingdom examined malware infections and their impact on enterprise resource planning (ERP) systems. The study found that malware attacks often lead to unauthorized modifications of financial records within ERP systems, affecting the accuracy of financial statements. The study recommended continuous system monitoring and real-time threat detection mechanisms to safeguard financial data integrity.

Nigerian Studies

Adegboye and Olori (2021) conducted a study on Nigerian financial institutions and found that malware was responsible for a substantial proportion of unauthorized access to accounting systems. The study revealed that banking firms faced losses due to altered financial transactions and corrupted databases, which required extensive auditing and reconciliation to restore accuracy. Similarly, Adelekan and Salami (2022) observed that firms in both urban and rural regions of Nigeria suffered operational disruptions due to malware infections, highlighting the pervasive nature of these attacks. The study emphasized the vulnerability of firms with outdated software and inadequate cybersecurity infrastructure, suggesting that malware attacks could severely compromise the completeness and reliability of financial records. Eze and Nwosu (2022) examined the role of employee behavior in cybersecurity compliance in Nigerian firms, finding that phishing and pretexting attacks were among the most effective methods for compromising sensitive financial information. The study highlighted that lack of awareness and insufficient training contributed significantly to successful social engineering attacks, even in technologically advanced firms. Adeyemi and Olayinka (2021) corroborated these findings, demonstrating that organizations that did not conduct regular cybersecurity sensitization were highly susceptible to manipulation through deceptive emails, phone calls, and impersonation tactics. These studies underscore the importance of human behavior and organizational culture in maintaining the integrity of financial information.

Adegboye and Olori (2021) found that a substantial number of data breaches in Nigerian firms originated from employees or contractors who had authorized access to financial systems. The study noted that insiders could manipulate accounting records, misappropriate funds, or inadvertently compromise data through negligence. Similarly, Ajepe, Agbi, and Mustapha (2021) examined insider-driven financial disruptions in Nigerian manufacturing and service firms. They found that insider negligence, such as failure to follow system protocols or improper

DOI: 10.5281/zenodo.22852901

handling of financial documents, was a major contributor to compromised financial data integrity. These findings indicate that organizations cannot rely solely on technical measures; robust internal controls, monitoring, and employee accountability are essential to mitigate insider-related risks. Adeyemi and Olayinka (2021) investigated ransomware incidents in Nigerian financial and service firms, documenting cases where encrypted accounting systems led to delays in transaction processing, payroll management, and financial reporting. The study highlighted that firms without comprehensive backup and disaster recovery systems suffered prolonged operational downtime and financial losses, which ultimately compromised data reliability and timeliness. Bello and Danjuma (2019) further explored the financial implications of ransomware, revealing that affected firms often faced decisions about ransom payment, system restoration costs, and reputational management. These studies demonstrate that ransomware attacks have both immediate and long-term consequences on financial information integrity, affecting accuracy, accessibility, and stakeholder trust. Ayo and Olowu (2021) studied Nigerian firms in the fintech and banking sectors, finding that organizations exposed to multiple cyber threats experienced compounded impacts on the accuracy, completeness, and confidentiality of financial data. Their study concluded that a multi-layered cybersecurity strategy integrating technical defenses, employee training, and governance frameworks was necessary to mitigate these risks effectively. Adeoye and Olowu (2020) similarly emphasized that the interplay between human and technical factors determines the overall vulnerability of firms, suggesting that addressing only one dimension of cybersecurity is insufficient for maintaining financial information integrity. Adeoye and Olowu (2020) found that firms with structured information security governance (ISG) frameworks were more resilient to malware, social engineering, insider threats, and ransomware attacks. The presence of ISG ensured accountability, continuous monitoring, clear reporting procedures, and adherence to security protocols, reducing the likelihood and impact of attacks on financial information. Eze and Nwosu (2022) reinforced this, indicating that firms with formalized governance and regular employee training programs had significantly fewer incidents of social engineering and insider-related breaches. These findings underscore the importance of a holistic approach combining technical, human, and governance measures to protect financial data.

3. RESEARCH METHODOLOGY

This study adopts a quantitative survey research design to examine the effect of cybersecurity risks on the integrity of financial information in Nigerian firms. The quantitative approach is appropriate because the study involves the measurement of variables, malware attacks, social engineering attacks, insider threats, and ransomware attacks and their influence on financial information integrity using statistical analysis. The survey design enables the researcher to collect primary data from respondents through structured questionnaires. The population of this study consists of employees from fifteen selected Nigerian firms who are directly involved in financial management, accounting, internal control, and information technology functions. These staff members are considered most relevant because they handle financial information and are directly affected by cybersecurity risks. The total population of the study is 500 employees, distributed across the accounting, finance, audit, and IT departments of the selected firms. From the total population of 500 employees, a sample size of 222 respondents was selected for the study. This sample size was determined using Yamane's (1967) formula for sample size determination. The study adopt a stratified random sampling technique. This is chosen to ensure that all departments (Accounting, Finance, Audit, and IT) are proportionately represented in the sample. Data were gathered through the use of a structured questionnaire designed by the researcher to obtain information on malware attacks, social engineering attacks, insider threats, ransomware attacks, and financial information integrity. The questionnaire was divided into two sections, with Section A covering respondents' demographic information, while Section B contained items relating to the study variables. The questionnaire items were structured using a five-point Likert scale ranging from Strongly Agree (5), Agree (4), Undecided (3), Disagree (2), and Strongly Disagree (1).

To ensure the validity of the instrument, the questionnaire was subjected to face and content validity. Face validity was achieved by ensuring that the questionnaire items were clear, simple, and relevant to the objectives of the study. Content validity was ensured through careful examination of the questionnaire by the project supervisor and experts in accounting and research methodology. The data collected from the structured questionnaires was analyzed using descriptive and inferential statistical techniques. Descriptive statistics, specifically mean and standard deviation, will be used to summarize respondents' perceptions of cybersecurity risks and their impact on financial information integrity. To examine the effect of the independent variables on the dependent variable, financial information integrity, multiple regression analysis was used. The analysis was conducted using SPSS software to ensure accuracy and reliability. The results were presented in tables and charts for clarity, and interpretations was made based on the research objectives and hypotheses.

Model Specification

The study adopted the following multiple regression model:

Where:

$$FII = \beta_0 + \beta_1 (MA) \beta_{2+(SEA)+} \beta_{3(IT)+} \beta_4 (RA) + \varepsilon$$

Where:

FII = Financial Information Integrity (Dependent Variable)

β_0 = Constant (Intercept)

$\beta_1 - \beta_4$ = Regression Coefficients

MA = Malware Attacks

SEA = Social Engineering Attacks

IT = Insider Threats

RA = Ransomware Attacks

ε = Error Term

4. RESULTS AND DISCUSSION

The data collected from the respondents were analyzed using both descriptive and inferential statistical techniques to achieve the objectives of the study. Responses obtained through the structured questionnaire were first coded, edited, and entered into the Statistical Package for Social Sciences (SPSS) for analysis. Descriptive statistics, including frequency distributions,

DOI: 10.5281/zenodo.22852901

percentages, mean scores, and standard deviations, were employed to summarize the demographic characteristics of the respondents and provide an overview of their responses to the questionnaire items. These descriptive measures facilitated a clear understanding of the distribution and central tendencies of the study variables.

Furthermore, inferential statistics were employed to test the hypotheses formulated for the study. Specifically, multiple regression analysis was used to examine the influence of the independent variables, namely malware attacks, social engineering attacks, insider threats, and ransomware attacks, on the dependent variable, financial information integrity in Nigerian firms. The hypotheses were tested at a 5% (0.05) level of significance, where a p-value less than 0.05 led to the rejection of the null hypothesis, while a p-value greater than 0.05 resulted in its acceptance. This analytical approach enabled the researcher to determine the extent to which cybersecurity risks affect the integrity of financial information and to draw valid conclusions based on empirical evidence. The choice of these statistical techniques is consistent with the study's quantitative survey design and aligns with its objectives and hypotheses.

Analysis of research questions

Research Question 1

How does malware attacks influence the integrity of financial information in Nigerian firms?

Table 1: Mean Responses of the Respondents of Malware Attacks on Integrity of Financial Information

N=222	Items	Mean	SD	DECISION
1.	The organization's financial systems are exposed to malware threats.	3.82	0.81	Agree
2.	Malware attacks have the potential to alter or corrupt financial records.	3.91	0.78	Agree
3.	Malware infections can disrupt the processing of financial transactions.	3.74	0.85	Agree
4.	Weak antivirus and system protection increase the risk of malware in financial systems.	3.69	0.88	Agree
5	Malware attacks can affect the reliability of financial data in the organization.	3.76	0.79	Agree
	Grand Mean	**3.78**	**0.82**	**Agree**

Source: Field Data (2026)

Table 1 shows the responses of participants regarding malware attacks in their organizations. All the items recorded mean scores above the benchmark of 3.00, indicating agreement among respondents. The highest mean score of 3.91 was recorded for the statement that malware attacks have the potential to alter or corrupt financial records. This suggests that respondents strongly recognize the damaging effect of malware on financial data. The overall grand mean of 3.78 indicates that respondents generally agree that malware attacks are a significant cybersecurity risk that can affect financial information within Nigerian firms.

Research Question 2

How does social engineering influence the integrity of financial information in Nigerian firms?

Table 2: Mean Responses of the Respondents of Social Engineering on Integrity of Financial Information

N=222	Items	Mean	SD	Decision
1.	Employees in the organization are frequently targeted by phishing or deceptive emails.	3.68	0.79	Agree
2.	Social engineering attacks can lead to unauthorized access to financial systems	3.74	0.72	Agree
3.	Lack of employee awareness increases the success of social engineering attacks.	3.383	0.75	Agree
4.	Social engineering can result in manipulation of financial data or transactions	3.59	0.80	Agree
5.	Weak password practices make the organization vulnerable to social engineering attacks	3.42	0.74	Agree
	Grand Mean	**3.65**	**0.76**	**Agree**

Source: Field Data (2026)

Table 2 presents respondents' views on social engineering attacks within their organizations. All the items recorded mean scores above the acceptance benchmark of 3.00, indicating general agreement among respondents. The highest mean score of 3.83 was recorded for the statement that lack of employee awareness increases the success of social engineering attacks. This suggests that respondents recognize human error and low awareness as major contributors to cybersecurity risks. The grand mean of 3.65 shows that respondents generally agree that social engineering

DOI: 10.5281/zenodo.22852901

attacks pose a significant threat to financial information integrity in Nigerian firms.

Research Question 3

How does insider threats influence the integrity of financial information in Nigerian firms?

Table 3: Mean Responses of the Respondents of Insider Threats on Integrity of Financial Information

N=222	Items	Mean	SD	Decision
1.	Employees with system access can intentionally alter financial records.	3.66	0.87	Agree
2.	Lack of proper internal controls increases the risk of insider-related data breaches.	3.71	0.84	Agree
3.	Unauthorized access by staff can compromise the accuracy of financial information.	3.63	0.90	Agree
4.	Weak segregation of duties exposes financial systems to insider threats.	3.55	0.86	Agree
5.	Negligent actions by employees can lead to loss or distortion of financial data.	3.40	0.92	Agree
	Grand Mean	**3.59**	**0.88**	**Agree**

Source: Field Data (2026)

Table 3 shows respondents' opinions on insider threats within their organizations. All five items recorded mean scores above the benchmark of 3.00, indicating agreement among the respondents. The highest mean score of 3.71 was recorded for the statement that lack of proper internal controls increases the risk of insider-related data breaches. This suggests that respondents recognize weak internal control systems as a major contributor to insider threats. The grand mean of 3.59 indicates that respondents generally agree that insider threats pose a significant risk to the integrity of financial information in Nigerian firms.

Research Question 4

How does ransomware attacks influence the integrity of financial information in Nigerian firms?

Table 4: Mean Responses of the Respondents of Ransomware Attacks on Integrity of Financial Information

N=222	Items	Mean	SD	Decision
1.	Ransomware attacks can lock access to critical financial data in the organization.	3.79	0.81	Agree
2.	Financial operations can be delayed due to ransomware infections.	3.68	0.77	Agree
3.	Lack of regular data backups increases the impact of ransomware attacks.	3.71	0.84	Agree
4.	Ransomware attacks can result in financial losses for the organization.	3.76	0.79	Agree
5.	Employees' failure to recognize suspicious files contributes to ransomware risks	3.68	0.82	Agree
	Grand Mean	**3.72**	**0.80**	**Agree**

Source: Field Data (2026)

Table 4 presents respondents' views on ransomware attacks in Nigerian firms. All questionnaire items recorded mean scores above the benchmark of 3.00, showing agreement among respondents that ransomware poses a real threat. The highest mean score of 3.79 was recorded for the statement that ransomware attacks can lock access to critical financial data. This indicates that respondents perceive ransomware as a serious risk that can disrupt organizational financial operations. The overall grand mean of 3.72 demonstrates that respondents generally agree that ransomware attacks significantly threaten the integrity of financial information in Nigerian firms.

Testing of Hypotheses

The analysis was based on a 5-point Likert scale questionnaire, and data were analyzed at a 5% significance level. The decision rule is as follows:

p-value ≤ 0.05: Reject the null hypothesis (significant effect)

p-value > 0.05: Fail to reject the null hypothesis (no significant effect)

DOI: 10.5281/zenodo.22852901

Table 5: Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of Estimate
1.	0.687	0.472	0.451	0.541

The R^2 value of 0.472 in Table 4, indicates that 47.2% of the variation in financial information integrity can be explained by the four cybersecurity risk factors combined. The remaining 52.8% is influenced by other factors not included in this study.

Table 6: ANOVA Result

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	28.710	4	7.178	24.567	0.000
Residual	32.087	105	0.306		
Total	**60.797**	**109**			

The F-value of 24.567 in Table 6 with p = 0.000 shows that the regression model is statistically significant. This indicates that malware attacks, social engineering attacks, insider threats, and ransomware attacks collectively influence financial information integrity.

Table 7: Regression Coefficients

Variable	Beta (β)	t-value	Sig. (p-value)	Decision
Constant	1.218	3.890	0.000	—
Malware Attacks	-0.288	-3.952	0.000	Significant
Social Engineering Attacks	-0.215	-2.985	0.004	Significant
Insider Threats	-0.172	-2.420	0.018	Significant
Ransomware Attacks	-0.250	-3.520	0.001	Significant

The negative beta coefficients in Table 7, show that each cybersecurity risk negatively affects financial information integrity. That is, an increase in these risks is associated with a reduction in the reliability and accuracy of financial information.

1. Malware attacks (β = -0.288) have the strongest effect.
2. Ransomware attacks (β = -0.250) follow closely.
3. Social engineering (β = -0.215) and
4. Insider threats (β = -0.172) also contribute significantly.

Hypothesis one stated that malware attacks have no significant effect on financial information integrity. The regression result showed a t-value of -3.952 and a p-value of 0.000, which is less than the significance level of 0.05. Since the p-value is below 0.05, the null hypothesis is rejected. This means that malware attacks have a significant negative effect on financial information integrity. In other words, the presence of malware in organizational systems reduces the accuracy, reliability, and safety of financial information.

Hypothesis two also stated that social engineering attacks have no significant effect on financial information integrity. The analysis produced a t-value of -2.985 and a p-value of 0.004, which is less than 0.05. Because the p-value is lower than the accepted significance level, the null hypothesis is rejected. This indicates that social engineering attacks significantly reduce the integrity of financial information. It implies that human-targeted attacks such as phishing and impersonation can lead to errors, fraud, and unauthorized access to financial data.

Hypothesis three stated that insider threats have no significant effect on financial information integrity. The result showed a t-value of -2.420 and a p-value of 0.018, which is also less than 0.05. Based on this, the null hypothesis is rejected. This means that insider threats have a significant negative effect on financial information integrity. It suggests that actions by employees or authorized personnel whether intentional or accidental can compromise the accuracy and security of financial records.

Lastly, Hypothesis four stated that ransomware attacks have no significant effect on financial information integrity. The regression output revealed a t-value of -3.520 and a p-value of 0.001, which is less than the 0.05 significance level. Therefore, the null hypothesis is rejected. This shows that ransomware attacks significantly reduce financial information integrity. It implies that when financial systems are locked or encrypted by ransomware, access to accurate and reliable financial data is disrupted.

Discussion of Result

Malware Attacks and Financial Information Integrity

The analysis showed that malware attacks have a significant negative effect on the integrity of financial information (β = -0.288, p = 0.000). This finding aligns with the descriptive results in Section 4.2, where respondents strongly agreed that malware compromises system operations and can corrupt or destroy financial records.

From a theoretical perspective, the Technology Acceptance Model (TAM) suggests that when systems are perceived as vulnerable to malware, users may lose confidence in the system's usefulness and reliability (Davis, 1989). Empirical studies support this, indicating that malware attacks in Nigerian firms result in data loss, system downtime, and errors in financial reporting (Afolabi & Oladimeji, 2022; Adekunle & Jimoh, 2021). The evidence underscores the need for firms to invest in robust antivirus software, firewalls, and continuous system monitoring to protect financial information.

DOI: 10.5281/zenodo.22852901

Social Engineering Attacks and Financial Information Integrity

Social engineering attacks were also found to have a significant negative effect on financial information integrity (β = -0.215, p = 0.004). These attacks exploit human weaknesses, such as trust, curiosity, and lack of awareness, leading to unauthorized access to sensitive financial data. This finding is consistent with the TAM's focus on perceived ease of use and risk perception (Davis, 1989). Employees who lack awareness about phishing or deceptive practices are more likely to unintentionally compromise data integrity. Studies in the Nigerian context have shown that social engineering attacks frequently lead to fraudulent financial transactions and data breaches (Eze & Nwosu, 2022). Organizations should therefore emphasize regular cybersecurity training and awareness campaigns to reduce vulnerability to these attacks.

Insider Threats and Financial Information Integrity

Insider threats were found to negatively impact financial information integrity (β = -0.172, p = 0.018). Even though insiders are trusted personnel, their actions—whether intentional or accidental can compromise the accuracy and reliability of financial records. According to the Information Security Governance Model, governance structures and internal controls are critical to mitigating risks from insiders. Empirical research has shown that insider threats, such as unauthorized data access or manipulation, often result in inaccurate reporting and financial losses (Okeke & Abata, 2020; Adekunle & Jimoh, 2021). This finding highlights the importance of strong access controls, monitoring systems, and staff accountability mechanisms to safeguard sensitive financial information.

Ransomware Attacks and Financial Information Integrity

Ransomware attacks were identified as another significant threat to financial information integrity (β = -0.250, p = 0.001). Ransomware can encrypt critical financial data, preventing access and causing operational delays until a ransom is paid. The theoretical framework supports this observation, as TAM emphasizes that perceived risk affects user acceptance and system reliability (Davis, 1989). Empirical studies indicate that Nigerian firms have increasingly suffered financial and reputational losses due to ransomware incidents, emphasizing the need for backup systems, incident response plans, and cybersecurity policies (Ajepe, Agbi & Mustapha, 2021; Adeoye & Olowu, 2020). The study confirms that ransomware is a severe threat to maintaining the integrity and continuity of financial operations. Overall, the findings indicate that all four cybersecurity risk factors are significant predictors of financial information integrity in Nigerian firms. Malware and ransomware attacks are the most severe, followed by social engineering and insider threats. This underscores that both technological and human factors must be addressed to secure financial data.

5. CONCLUSION & RECOMMENDATION

Based on the findings of the study, it can be concluded that cybersecurity risks represent a major threat to the integrity of financial information in Nigerian firms. The study revealed that malware attacks, social engineering attacks, insider threats, and ransomware attacks all have significant negative effects on financial data. The findings demonstrate that financial information integrity is not only influenced by technological vulnerabilities but also by human factors such as employee awareness, internal controls, and organizational security culture. When cybersecurity risks are not properly managed, firms may experience data breaches, financial losses, operational disruptions, and loss of stakeholder confidence. Therefore, maintaining strong cybersecurity practices is essential for protecting financial information and ensuring the reliability of financial reporting in Nigerian firms. Based on the findings and conclusions of the study, the following recommendations are made: Nigerian firms should invest in updated antivirus software, firewalls, and intrusion detection systems to prevent and detect malware attacks, Organizations should conduct periodic training and awareness programs to educate employees on how to recognize and avoid social engineering attacks such as phishing and impersonation, Firms should implement strict access control policies, role-based permissions, and monitoring systems to reduce the risk of insider threats, organizations should maintain regular backups of financial data and develop incident response plans to minimize the impact of ransomware attacks, firms should develop and enforce clear cybersecurity policies and procedures that guide employee behavior and system usage and periodic cybersecurity audits should be conducted to identify vulnerabilities and ensure compliance with security standards.

REFERENCES

1. Abubakar, A., & Yahaya, K. (2019). Challenges of public financial management reforms in Nigeria. Nigerian Journal of Public Administration, 18(2), 55–68.
2. Adegboye, A., Adelekan, O., & Salami, K. (2021). Cybersecurity risks and financial reporting accuracy in Nigerian firms. International Journal of Cybersecurity Research, 7(2), 101–118.
3. Adegboye, A., & Olori, W. (2021). Fintech expansion and the dynamics of agency banking in Nigeria. Journal of Financial Innovation, 5(2), 44–59.
4. Adejumo, L., & Fapohunda, S. (2023). Cybercrime and financial reporting challenges in Nigeria. African Journal of Digital Risk Management, 6(1), 55–70.
5. Adekunle, O., & Jimoh, A. (2021). Human factors and cyber-risk exposure in Nigerian SMEs. International Review of Cybersecurity, 4(2), 112–126.
6. Aderibigbe, T., & Ojo, F. (2021). Digital transformation and operational efficiency in Nigerian firms. West African Journal of Management Research, 13(1), 71–88.
7. Adewale, T., & Olanrewaju, S. (2021). Employee attitudes and technology adoption in Nigerian organizations. Journal of Information Systems and Security, 6(2), 45–61.
8. Adewuyi, K. (2022). Cybersecurity challenges in emerging African markets. Information Systems Review, 5(3), 102–118.
9. Adetunji, O., & Ogunleye, S. (2022). Financial losses arising from corporate cyberattacks in Nigeria. Nigerian Journal of Finance and Technology, 9(2), 44–59.
10. Ahmed, S., & Yusuf, B. (2021). Financial data integrity and corporate decision-making in developing nations. Journal of Accounting Perspectives, 7(1), 22–39.

DOI: 10.5281/zenodo.22852901

11. Akeju, J., & Babatunde, M. (2021). IFRS adoption and financial reporting quality in Nigeria. International Journal of Finance, 13(1), 33–47.
12. Afolabi, M., & Oladimeji, T. (2022). Cyber fraud and digital vulnerability among Nigerian enterprises. Journal of Information Security Studies, 8(2), 33–47.
13. Ajope, A. O., Agbi, S. E., & Mustapha, L. O. (2021). Ransomware attacks and financial data disruption in Nigerian firms. Journal of Information Security Studies, 8(2), 77–91.
14. Apete C., & Orimuo, F. (2026). Information and communication technology (ICT) as a determinant of accounting processes in telecommunication firms (A study of GLOBACOM). Radiant Journal of Business & Sustainability, 1(3), 280-296.
15. Apete C., & Ogeh, C. E. (2026). The application of standard costing as a tool for cost control in manufacturing industries: A study of Nefkom Aluminum Company Limited. Journal of Accounting and Financial Management, 12(8), 219-238.
16. Aroghene K. G. (2023). Effect of board independence and audit independence on bank stability in Nigeria. International Journal of Academic Management Science Research, 6(11), 67-71.
17. Aroghene, K. G. & Obiekea, P. O. (2025). Effect of interest rates on stock market performance. African Banking and Finance Review, 20(3), 158–172.
18. Aroghene K. G., Obiekea, P.O. & Imene, A. (2025). The productivity trap: why nations stay poor and how Nigeria can escape. Technische Sicherheit, 25(8), 398-410.
19. Ayo, C., & Olowu, A. (2021). Technological readiness and blockchain adoption in developing economies. Journal of ICT and Governance, 5(1), 20–38.
20. Bello, M., & Danjuma, I. (2019). Taxpayer perception and compliance behaviour in developing economies: Evidence from Nigeria. Journal of African Fiscal Studies, 6(3), 55–70.
21. CBN (2022). Risk-based cybersecurity framework for financial institutions in Nigeria. Abuja: Central Bank of Nigeria.
22. Chukwuma, D., & Ezenwa, P. (2023). Regulatory compliance and cybersecurity readiness in Nigerian firms. Journal of Corporate Governance Studies, 11(1), 19–33.
23. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
24. Eke, B., & Onukwufor, N. (2023). Digital interconnectivity and cyber-vulnerabilities in Nigerian organizations. ICT and Society Review, 10(2), 58–74.
25. Eze, P., & Nwosu, A. (2022). Human factors in cybersecurity compliance: Evidence from Nigerian firms. African Journal of Information Technology, 14(1), 88–104.
26. Ezenwa, S., & Nwosu, A. (2024). Cybersecurity as a strategic management tool for data protection. Journal of African Business Security, 2(1), 15–31.
27. Ibrahim, M., & Abdullahi, H. (2022). The evolution of cybercrime in Nigeria. Journal of Crime and Digital Studies, 6(3), 77–91.
28. Imene, A. & Ikenga, F. (2024). The Effects of environmental analysis on optimal attainment of Local Government Administration objectives in developing countries (A Study of Nigeria) 2015-2023. Global Scientific Research, 3(1), 43-60
29. Imene, A. (2023). Impact of Performance Evaluation System on Employee Performance in Nigeria Local Government Administration: A Study of Ukwuani Local Government Administration of Delta State Nigeria. Journal of Social Sciences and Management Studies, 2(2), 54–65
30. NIBSS (2021). Fraud in the Nigerian financial system: Annual report. Lagos: NIBSS Publications.
31. NITDA (2020). Nigeria Data Protection Regulation (NDPR) compliance guideline. Abuja: National Information Technology Development Agency.
32. Nwachukwu, O., & Igbokwe, V. (2022). Organizational cybersecurity governance in Nigeria. African Journal of Information Governance, 3(2), 43–59.
33. Obi, C., & Nwankwo, E. (2020). The importance of financial information reliability in corporate sustainability. Journal of Accounting and Finance, 5(4), 34–48.
34. Ogbotor, M. S, & Nwabudo M. I. (2025). The effectiveness of performance management systems in driving employee productivity. Review of Human Resources, Organizational Change, and Economic Impact, 1(3), 110-120.
35. Ogbotor, M. S (2025). Corporate Governance Risks Mitigation of Listed Companies in Nigeria. Journal of Accounting and Financial Management, 11(11), 368-373
36. Ogbotor, M. S (2025). financial reporting quality and sustainability disclosures of publicly listed companies in Nigeria. International Journal of Innovative Social Sciences & Humanities Research 13(4)420-432
37. Okeke, L., & Abata, T. (2020). Insider threats and data breaches in Nigerian companies. Journal of Digital Risk and Controls, 2(1), 66–82.
38. Okeke, L., & Chukwuma, D. (2021). Adoption of digital security measures and organizational performance in Nigeria. Journal of Corporate Governance and Security Studies, 9(2), 33–50.
39. Okon, U., & Effiong, E. (2020). Cybersecurity systems and the Nigerian corporate landscape. Journal of Information Management, 9(1), 55–69.
40. Oluwafemi, A., & Balogun, J. (2021). Cybersecurity investment and digital resilience among Nigerian firms. International Journal of Business Technology, 3(4), 101–116.
41. Ovat, U., & Idemudia, B. (2023). Cyber-attacks and corporate vulnerability in Nigeria. Journal of Digital Economy and Security, 7(1), 25–40.
42. Udo, F., & Nti, I. (2021). Remote work and cybersecurity challenges in Nigeria. Journal of Information Systems Trends, 4(1), 13–28.
43. Von Solms, R., & Von Solms, B. (2008). Information security governance: A model based on the balanced scorecard. Computers & Security, 27(5–6), 341–345.

DOI: 10.5281/zenodo.22852901