International Journal of Science Academic Research
Vol. 04, Issue 09, pp.6301-6310, September, 2023
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

A CYBER SECURITY FRAMEWORK TO STRENGTHEN SMALL AND MEDIUM SCALE ENTERPRISES (SMES) IN NIGERIA

***Vincent Onuwabhagbe OGBEIDE, Osaremwinda OMOROGIUWA and Emmanuel Eturpa SALAMI**

Department of Computer Science and Information Technology, Igbinedion University Okada, Edo State, Nigeria

Received 25th July 2023; **Accepted** 20th August 2023; **Published online** 30th September 2023

Abstract

Small and Medium Scale Enterprises (SMEs) in Nigeria are currently experiencing variety of cyber threats which is a big challenge as they are faced with wide range of cyber attacks that impact their businesses negatively. Challenges such as lack of access to finance, modern technology among others has hampered SMEs to perform their role as the engine growth in the economy. Despite the known challenges, most SMEs feels they are safe from cyber attacks than large organizations. However, something can be done for SMEs to at least prevent or mitigate these cyber attacks by addressing and understanding cyber security problems, developing good cyber culture and by creating a more proactive strategy that is suitable to SMEs. Therefore, firstly six known cyber security frameworks are thoroughly analyzed with the identified strengths and weaknesses. Subsequently, we propose a cyber security framework for SMEs in Nigeria that is dynamic, simple and cost effective, which is suitable to SMEs context.

Keywords: Small and Medium Scale Enterprises (SMEs), Framework, Cyber Attacks, Cyber Security, Cyber Threats.

INTRODUCTION

The advancement in technology has created exciting business opportunities for Small and Medium Scale Enterprises (SMEs), this opportunities are marred with new chanellages such as the ability to manage data, and a new source of risks (Calabrese *et al.,* 2019; Jafari-Sadeghi, 2021; Shah *et al.,* 2019). The rapidly evolving use of technology makes life easy and fast but also expose organisations to danger because of the threats from cyber crime. SMEs are faced with the same levels of cyber security issues as large organizations. However, limited resources and capabilities made them fragile against cyber risks (Baggott & Santos, 2020; Benz & Chatterjee, 2020). This inherent gap in cyber security has made SMEs a primary target for cybercriminals with 43% of all attacks in 2019 aimed at SMEs (Verizon, 2020). The web and the Internet globally provide an essential medium for SMEs and offer a lot of opportunities to both SMEs and the large scale industries (Apau *et al.,* 2019). SMEs in Nigeria face more cyber threats with attacks increasing by 89 per cent in 2021, this is according to Kaspersky researchers, which assessed the dynamics of attacks on SMEs between January and April 2022 and the same period in 2021, they warned that these threats pose an increasing danger to entrepreneurs **(**Adepetun, 2022). The costs and consequences of such attacks on businesses and governments are considerable. Cyber attacks cost organizations over $5 billion in 2017 and are anticipated to cost over $6 trillion in 2021 (Morgan 2021). Most SMEs do not have robust security measures against cyber threats and these makes cyber criminals attracted to them. This is a major reason for majority of SMEs failures (Moura & Serrão, 2018). The capacity of SME to perform their role, as the engine of growth in the economy, is often hampered by challenges such as lack of access to finance, modern technology, and market with unfair competition to imported goods, among others. Despite this, the top management in SMEs tend to think that their company is safe from cyber attacks because attackers are more likely to target larger enterprises (Bisson, 2021; Bullguard, 2020). Due to a lack of IT specialists and resources to implement the cyber security system with technological tools, SMEs face more cyber security-related development obstacles and concerns than larger businesses. Cyber attacks are becoming more common, emphasizing the significance of proper cyber security. Cyber security protects an organization's IT-related assets, such as data, systems, and networks, from digital attacks that might access, delete, or manipulate sensitive data or disrupt company operations (Kim & Solomon 2016). However, most local businesses lack adequate monitoring and security measures against unauthorised modification, resulting in unauthorised disclosure. Specifically, the owners regularly lack the proper processes to control evolving cyber security risks and information systems security threats that characterize the use of these technologies (Njenga & Jordaan, 2016). Indeed, emerging obstacles such as information security and cyber risks have resulted in widespread financial and nonfinancial losses (Arcuri *et al.,* 2017). Therefore, cyber risk management and preparation is a crucial competencies for not only survival but also the growth of SMEs (Chatterjee, 2019; Hoppe *et al.,* 2021). The need for SMEs to be aware of and understand the consequences of cyber security and how it can be addressed cannot be understated because this awareness and the understanding can potentially "influence the adoption of secure behaviours" (Bada & Sasse 2014). Mijnhardt, et al (2016) inform us that larger organisations have responded by adopting security standards such as ISO 27000x series, COBIT, NIST, and related frameworks but these frameworks are complicated and expensive for SMEs to adopt and implement. Given the above fact, six well known cyber security frameworks were thoroughly analyzed according to their principles and standards. Their basic strengths and weaknesses were also identified. Finally, a cyber security framework that is dynamic, simple and cost effective is proposed for SMEs in Nigeria. The

Corresponding Author:** ***Vincent Onuwabhagbe OGBEIDE,
Department of Computer Science and Information Technology, Igbinedion University Okada, Edo State, Nigeria

framework will assist SMEs to overcome cyber security challenges.

REVIEW OF RELATED LITERATURES

The study referred to existing literatures, focusing on various cyber security related problems faced by SMEs globally. Security issues continues to be a major concern for SMEs. This can lead to loss of customers, income, and in some instances forfeiture of business. According to Sunnews (2022), businesses that are running with low employees suffer from cyber threats a lot and it is estimated that these companies lose an average of $2.5 million every year. As far as Nigerian SMEs are concerned then they are also subjected to cyber attacks. Studies show that sometimes organizations have a budget limit to fix a few known vulnerabilities (Cohen *et al.,* 2022). Mutalib et al. (2021), focused on how SMEs coped with cyber-attacks in a developing country such as Malaysia, compared to the UK. It was confirmed that SMEs often found it difficult when experiencing a cyber attack on how to recover their business in the aftermath of the tragedy. It was reported that SMEs in developing nations such as South Africa, challenges to implementing cyber security in SMEs include a lack of management support owing to other company objectives, a low budget, and a lack of resources with technical skills and cyber security tools (Armenia *et al.,* 2021 ; Kabanda *et al.,* 2018). Benz and Chaterjee (2020) believed that SMEs are among the most immature and critically vulnerable types of companies. SMEs are not immune to the threats posed by the use of information and communication technologies. Studies have noted that SMEs may be more vulnerable to cyber threats when compared to larger firms (Singh *et al.,* 2022). Benz & Chatterjee (2020) reported in their studies that more than 50% of SMEs are lagging far behind to have the latest cyber-risk strategy and the IT leaders don't know starting point to improve cyber security posture. According to another study conducted for SMEs in Kenya, businesses face two key hurdles when it comes to implementing cyber security. One was a lack of sufficient funds, and another was a lack of leadership support for cyber security implementation, which could be because they have other business-related issues that are a priority for them (Muhati, 2018). According to a recent survey of SMEs in the United Kingdom, roughly 73 percent of businesses had trouble accessing cyber security information to adopt. Cyber attacks and data loss were not considered a significant risk by one-third of businesses (Rae & Patel, 2019). Cyber security must be embedded into organisational culture as it is critical and required to protect sensitive personal data against adversaries or hackers gaining access to organisations data (Antunes *et al.,* 2021; Benz & Chatterjee, 2020). Other studies such as Kalhoro et al. (2021) & Emer et al. (2021), suggested that practicing “cyber hygiene” within the SME industry would provide a better protection, better security, monitoring, and maintenance of the networks of software development organizations. According to a 2019 study conducted by Ponemon Institute, “cyber threats against SMEs are becoming more targeted”. The study reports that 66% of SMEs experienced a cyber attack in the past year and that there was a significant increase in data breaches in SMEs over the past three years (Ponemon Institute, 2019). Despite this, SMEs tend to think that their organisation is safe from cyber attacks because attackers are more likely to target larger enterprises (Bisson, 2021; Bullguard, 2020). Another survey uncovered that 20% of SME owners believe they have zero vulnerabilities (Bullguard, 2020). A recent security reports show that a significant proportion of cyber security breaches are caused by employee noncompliance with organizational information security policies (Alshaikh, 2020). Ponsard et al (2019) stated, it is well known that technological tools alone cannot guarantee the security of an IT system. This also requires collaboration with the employees inside their organisation. Hence, cyber security awareness must be considered and tailored for both employees and their organisation.

METHODOLOGY

The study adopts a qualitative exploratory methodology as it followed the study of (Kabanda *et al.,* 2018). The use of qualitative exploration method facilitates the assessment of preventive measures in the field of cyber security. It afford the use of interviews with open ended questions, description conveyed in languages and literature reviews that investigate generalizablilty and propositions. Secondary sources of data which include scholarly journals, published papers, reputable websites and scholarly books which comprise of a broad range of information sources, were used to gather data for the study. A thorough examination of the literatures was done by an extensive content analysis of thematic exploration which entails the accumulation of relevant data that can be applied in the pursuit of resolving the studies inquiry.

ANALYSIS OF CYBER SECURITY FRAMEWORKS AND POLICY

Managing and identifying cyber attack is important in any organisation. Therefore, SMEs should make appropriate security investment and decisions for the mitigation of cyber attack. There are many cyber security frameworks that provide standards to identify and mitigate cyber attacks. These frameworks can also be used to assess, evaluate, and improve the security status of an organisation. Many frameworks, policies and standards have been developed to help organizations mitigate cyber attacks. Presented below, are six known cyber security frameworks.

NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) Cyber security Framework was developed based on an executive order by the US federal legislations, the purpose is to enhance the security of the country’s critical infrastructure, thus protecting them from internal and external attacks. Although the framework’s design aims to secure critical infrastructures, private organizations implement it to strengthen their cyber defenses. In particular, NIST CSF describes five functions that manage the risks to data and information security. The functions are Identify, Protect, Detect, Respond, and Recover. The Identify function guides organizations in detecting security risks to asset management, business environment, and IT governance through comprehensive risk assessment and management processes. The Protect function defines security controls for protecting data and information systems. These include access control, training and awareness, data security, information protection procedures, and maintaining protective technologies. The Detect provides guidelines for detecting anomalies in security, monitoring systems, and networks to uncover security incidences, among others. The Response function includes recommendations for planning responses to security events, mitigation procedures, communication processes during a response, and activities for improving security resiliency.

Lastly, the Recovery function provides guidelines that an organisation can use to recover from attacks. Despite the fact that the NIST framework provides general and regulatory guide for organizations to manage risk, the framework has limitations that make it difficult to be implemented by SMEs in Nigeria.

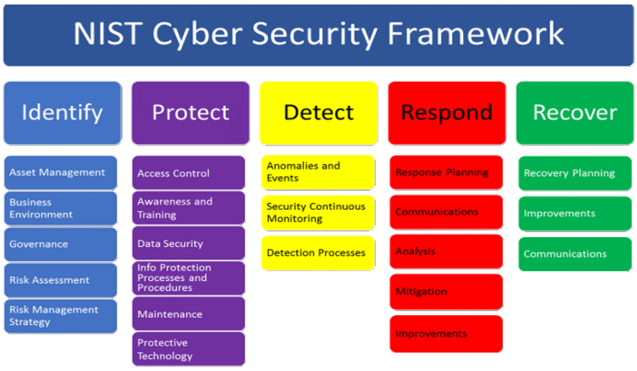


Figure 1. NIST Cyber Security Framework (Hall, 2020)

Strengths of the NIST Framework

The basic Strength of the NIST Framework are:

- The framework provides guide and general regulation for organizations to manage risk.
- The framework can be implemented by organizations of different sizes.
- The framework is a tool used to raise awareness to understand current practices.
- The framework is free and can be downloaded online.
- The framework can serve multiple purposes in various organizations.
- The framework can be combined with other frameworks.

Weaknesses of the NIST Framework

The basic Weakness of the NIST Framework are:

- The framework was designed to comply with the US federal legislations.
- The framework requires expert to implement making it expensive and complex for SMEs to implement.
- The design of the framework is more suitable for government agencies and less convenient for SMEs.
- The framework has a generalized view of risk assessment and risk management.
- The extensive nature of the standard's documentation makes it quite difficult for organizations to extract from it.
- The framework focuses on compliance, it does not tell you what to do or how to do it.

Control Objectives for Information and Related Technologies (COBIT)

Control Objectives for Information and Related Technologies (COBIT) is a security framework for adopting good business practices in relation to IT management, governance, and security. COBIT was crafted by Information Systems Audit and Control Association (ISACA), an international association of professionals focused on IT security governance. COBIT was firstly focus on auditing when it was created. The Information Systems Audit and Control Association (ISACA) updated its COBIT framework in 2019 to create a Governance System and Governance Framework. Instead of basing compliance on individual security controls, COBIT 2019 starts with stakeholders' needs, assigns job-related governance responsibilities to each type, and then maps the responsibility back to technologies. Ultimately, COBIT's goal is to ensure appropriate oversight of the organization's security posture. The latest version, COBIT 19 is based on COBIT 5 that was released in 2014. ISACA introduced more importance on IG and risk Management. Besides the ability of supervision and management of Information Security, COBIT provides you guidance on audit and vulnerabilities management. COBIT is organized into four major domains: Planning and Organization, Procurement and Implementation, Delivery and Support, Monitoring. ISACA also gives COBIT certifications to whoever wants to learn more about the framework. The framework has all the descriptions in terms of processes, activities, and responsibilities, but costly to implement. COBIT does not tell you how to do it, instead it tells you what to do which makes it hard to implement an action plan. It requires a lot of knowledge and skill in order to implement as a tool to provide support to information technology governance.

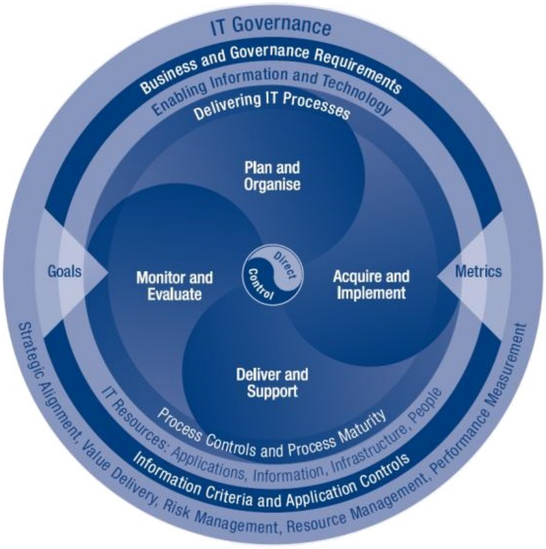

IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Monitor and Evaluate
Direct Control
Acquire and Implement
Deliver and Support
Goals
Metrics
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement
IT Resources: Applications, Information, Infrastructure, People
Process Controls and Process Maturity
Information Criteria and Application Controls

Figure 2. COBIT Framework (Soujanya, 2023)

Strengths of the COBIT Framework

The basic Strength of the COBIT Framework are:

- The framework can be used in wide range of organizations.
- The framework optimizes the use of resources available i.e. applications, infrastructure and people.
- The framework is a business oriented framework that emphasis on IT governance and management.

Weaknesses of the COBIT Framework

The Basic weakness of the COBIT Framework are:

- The framework requires expert to implement to support IT governance.
- The framework is expensive to implement.
- The framework is hard to implement because of its rigid nature.

ISO/IEC Series

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) is a standardization entity, and was established in Geneva, Switzerland in 1947. It gives a set of rules and regulations that helps manage information inside an organization. It covers employees, third parties, customers, clients, peers and all assets data inside an organization. It is a worldwide framework used by multinationals. It is an objective framework, but less complex and easier to implement in organizations. It is suitable for companies of all sizes and types. The ISO/IEC 27001 uses the steps based on the "Plan-Do-Check-Act" (PDCA) by structuring the management system in more detail by showing what are the control requirements and objectives and how to structure your Information Security Management System. ISO series gives you an overview of ISMS that helps identify, analyse and treat data risks. For example, in the ISO/IEC 27001 you have a vocabulary explaining the meaning of all terms that helps understand the definition being easy when using it to construct your policy and a briefly guidance on how to implement it. In the ISO/IEC 27002 you will find all the controls deep explained and, in the ISO/IEC 27005 you will find in detail how to implement risk management process inside the organization. ISO can be used independently or combined with another international framework like COBIT, there is no usage limitation.

ISO standards also provide data management guidance. How you treat the data inside your organization is very important to ensure its safety and the ISO/IEC 27001 provides you controls on how to acquire, validate, store, protect, and process data. It also provide controls in other areas like: HR Management, physical controls, information security controls, stakeholder's management, operations and access controls, incident management, business continuity management. Although the ISO is suitable for companies of all sizes and types and less complex and easier to implement, its series publications are sold they are not available for free. Applying ISO standards requires experts and costly to implement.

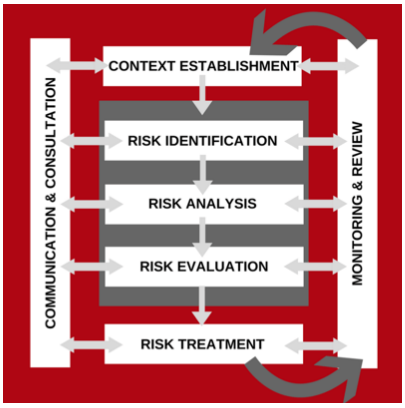


Figure 3. ISO 27001 Framework (Vinck, 2021)

Strengths of the ISO/IEC Framework

The basic Strength of the ISO/IEC Framework are:

- It is an internationally recognized and accepted framework with certification.
- The framework is suitable for organizations of all sizes and types.
- The framework has no usage limitation.
- The framework is less complex and easier to implement in organizations.
- The framework is the most popular cyber security framework.
- It is a widely used framework for general information security management system internationally.

Weaknesses of the ISO/IEC Framework

The Basic weakness of the ISO/IEC Framework are:

- The framework fails to recommend how the security processes may be implemented practically.
- The framework requires a lot of resources for implementation.
- The framework is too extensive, it does not offer direct instruction on how to align with specific objectives.
- The standard certification will be too expensive and complex for SMEs.
- The framework requires substantial expertise to understand and implement.
- The framework series publication is not free.
- The standard is rather overwhelming to navigate.

Center for Internet Security (CIS)

The Center for Internet Security (CIS) Critical Security Controls are a set of 20 actions designed to mitigate the threat of the majority of common cyber attacks. Created by the SANS Institute, the CIS Controls gives an effective framework for systems management. It was designed as a complementary set of regulations that will help structure the controls granting a better cyber security and not designed to replace any regulatory framework that already exist inside the organization. CIS works well for organizations that want to start out with baby steps. Their process is divided into three groups. They start with the basics, then move into foundational, and finally, organizational. It can be used combined with a lot of regulatory frameworks like: NIST Cyber security Framework, NIST 800-53, ISO 27000 series, ITIL, COBIT. It also can be used combined with other security regulations like: GDPR, PCI DSS, HIPAA, FISMA. This organization works with benchmarks, or guidelines based on commonly used standards, such as NIST and HIPAA, that not only map security standards to help companies comply with them but offer alternative basic security configurations for those who don't require compliance but want to improve their security.

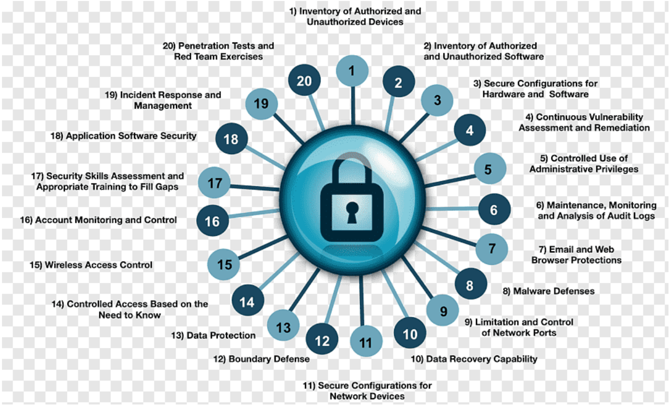

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Figure 4. CIS Framework (Pngwing, 2023)

Strengths of the CIS Framework

The basic Strength of the CIS Framework are:

- The framework is concise and prioritized.
- The standard provides technical implementation.
- The CIS publication is updated yearly.
- The framework is suitable for business managers.
- The framework can be combined with other regulatory frameworks.
- The framework is free and can be downloaded online and implemented by any organization.

Weaknesses of the CIS Framework

The basic Weakness of the CIS Framework are:

- The CIS framework is not as popular like other frameworks.
- The framework did not discuss in detail the overall organizational posture at executive level.
- The framework does not offer employee training and policy development for small technical teams.
- The framework will be difficult to implement in Small business because of lack of resources.

Committee of Sponsoring Organizations (COSO)

The Committee of Sponsoring Organization (COSO) Framework is a framework for designing, implementing and evaluating internal control for organizations, providing enterprise risk management. It was published for the Internal Control Integrated Framework or ICIF and it is widely used in the United States. The framework allows organizations to identify and manage cyber security risks. The core points behind the framework's development include monitoring, auditing, reporting, controlling, among others. Also, the framework consists of 17 requirements, which are categorized into five different categories. The categories are control environment, risk assessments, control activities, information and communication, and monitoring and controlling. All of the framework's components collaborate to establish sound processes for identifying and managing risks. Using the framework routinely identifies and assesses security risks at all organizational levels, thus improving its cyber security strategies. The framework recommends communication processes for communicating information risks and security objectives up or down in an organization. The framework further allows for continuous monitoring of security events to permit prompt responses.

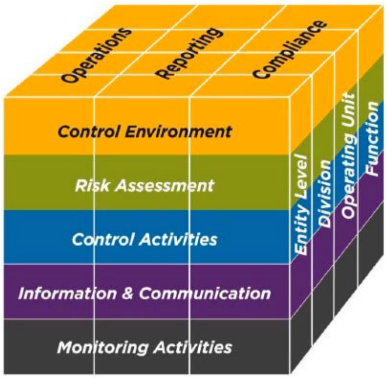


Figure 5 COSO Framework (MacMullen, 2022)

Strengths of the COSO Framework

The basic Strength of the COSO Framework are:

- The framework is the most accepted ERM framework by enterprises.
- The framework involves key executives with its collaborative approach nature.
- The framework is fairly easy to understand and implement
- The framework can be implemented by organizations of different sizes.

Weaknesses of the COSO Framework

The basic Weakness of the COSO Framework are:

- The framework is too broad and cumbersome to apply to specific operations.
- The framework is complex, it has a multi-layered model that many organizations finds difficult to understand.
- The framework lacks detail implementation guidance which makes it difficult for small organizations to execute.
- The implementation of the framework requires a manager with sufficient knowledge and expertise to identify the most significant risk.
- The framework ignores the area that need effective risk management in order to support organizational risk or objectives
- The framework annual review for every process results in a waste of time and money.

National Cyber Security Policy and Strategy (NCPS) of Nigeria

The National Cyber Security Policy and Strategy, which was developed through the office of the National Security Adviser (ONSA) in 2014, is said to be a framework that provide guidance for mainstreaming Nigeria's National Cyber Security program. It aims to strengthen cyber security governance, coordinate and foster a trusted cyber environment that enhances Nigeria's cyber security readiness. Therefore setting the path for effective coordination of the activities of all relevant stakeholders across government, academia and private sector to handle dynamism of security threats in the cyber domain. The new 2021 policy is a review of the 2014 edition. It is designed to realign the nation's cyber security efforts to effectively tackle the dynamic and emergent nature of threats in the nation's cyberspace. Nigeria is one of the leading digitally connected countries on the continent with over 104 million active internet users. The policy strategic area of focus is based on 8 pillars which form the support of the National Cyber Security Programme. The pillars are:

a. Strengthen cyber security governance and coordination
b. Fostering protection of critical and national information infrastructure
c. Enhancing cyber security incident management
d. Strengthening the legal and regulatory framework
e. Enhancing cyber defense capability
f. Promoting a thriving digital economy
g. Assurance monitoring and evaluation
h. Enhancing international cooperation

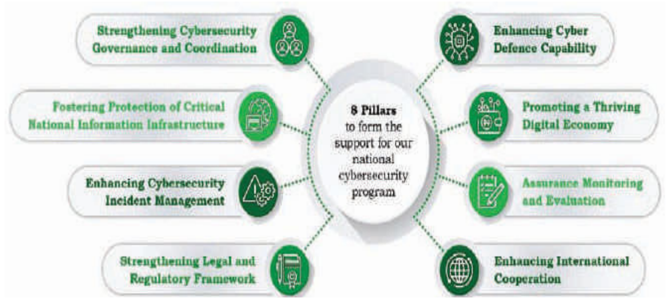

Strengthening Cybersecurity Governance and Coordination
Enhancing Cyber Defence Capability
Fostering Protection of Critical National Information Infrastructure
8 Pillars to form the support for our national cybersecurity program
Promoting a Thriving Digital Economy
Enhancing Cybersecurity Incident Management
Assurance Monitoring and Evaluation
Strengthening Legal and Regulatory Framework
Enhancing International Cooperation

Figure 6. NCPS Framework (ONSA, 2021)

Strengths of the NCPS

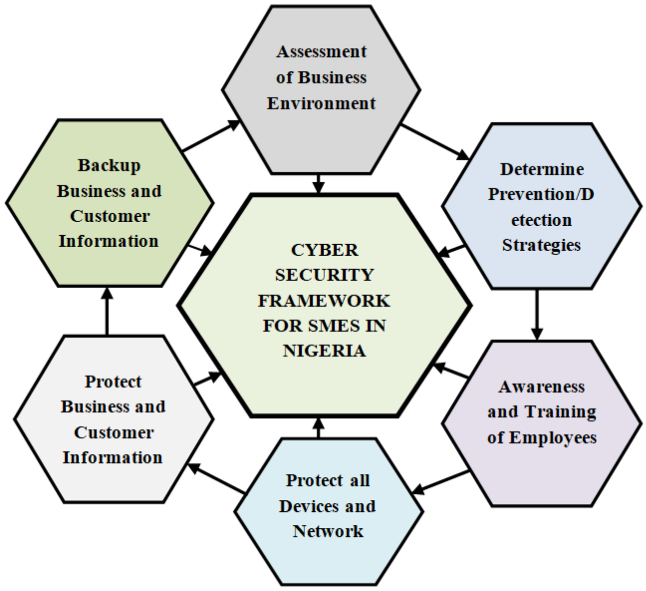
The basic Strengths of the NCPS Framework are:

- The NCPS provides guide and coordinate activities for stakeholders across government, academia and private sector to manage risk.
- The NCPS will serve as a guide to how experts can build stronger systems to easily identify cyber threats.
- The NCPS is designed to curtail cyber threats and ensure the protection on the nation’s assets in the digital infrastructure
- The NCPS highlights how potential threats will be addressed with the introduction of emerging technologies like the 5G, artificial intelligence, machine learning amongst others.
- The NCPS document is free and can be downloaded online.

Weaknesses of the NCPS

The basic Weakness of the NPCS are:

- The NCPS provides a generalized guide to coordinate organization's activities and manage risk which makes it difficult for SMEs to execute.
- The NCPS will require substantial expertise to understand and implement.
- The broad nature of the NCPS will make it difficult for SMEs to implement.
- The NCPS will require a lot of resources thereby making it expensive for SMEs to implement.


Assessment of Business Environment
Determine Prevention/Detection Strategies
Awareness and Training of Employees
Protect all Devices and Network
Protect Business and Customer Information
Backup Business and Customer Information
CYBER SECURITY FRAMEWORK FOR SMES IN NIGERIA

Proposed Cyber Security Framework for SMEs in Nigeria

The proposed Framework is divided into six segments and identifies steps to be used in order to protect SMEs against cyber threats. The framework process is in a clockwise form, starting from the top (Assessment of Business Environment) to the right, then down to the left up to (Backup Business and Customer Information).

1. Assessment of SME Environment

The first key component of the framework will require SMEs to access their environment to know what devices they have within the environment such computers, laptop, software, smartphones and any other device that needs to be listed out. Also, SMEs need to identity cyber threat causes to their business and the ability to deal with the threats. Unfortunately, many SMEs are still unprepared when it comes to managing cyber risk and understanding their vulnerabilities. There is need for SMEs to be on the lookout for cyber threats, especially because it is possible to identify cyber risk before a cyber attack, data breach or business interruption actually happens. SMEs in Nigeria are technically less aware of the threats being faced because they have limited resources to equip themselves against attacks.

The study identified major cyber threat causes, they are:

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

2. Prevention/Detection Strategies

There is need for SMEs to define strategies for preventing and detecting cyber threats. Some of the ways are:

Prevention Strategies

a. Develop Cyber Security Policies: a cyber security policy helps your staff to understand their responsibilities and what is acceptable when they use or share data, computers and devices, emails, internet sites.
b. Educate your employees: one of the most effective strategies to fight against cyber attacks and all forms of

data breaches is to train your staff on cyber attack prevention and keeping them informed about current cyber assaults.

c. **Constantly update software and systems**: cyber assaults frequently occur because your systems or security software are outdated, exposing threats. Cyber criminals take advantage of these flaws to get access to your network. Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
d. **Install and Enable a Firewall**: a firewall is important when defending your data against malicious attacks. An effective firewall can prevent unauthorised access to your computers and network. This protects your data from being compromised
e. **Backup Data Regularly**: one sure way to avoid inconveniences in the event of an attack is to backup your data regularly. This way, you will have a backup solution should the worst happen.

Detection Strategies

a. **Antivirus Software**: Most antivirus mechanisms can detect malware, spyware, ransomware, and malicious email attachments and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cyber criminals.
b. **Penetration Testing**: it is used to find any security weaknesses in a system. It is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. If you think the way a cyber criminal would, security experts can scan their IT environments for vulnerabilities, such as unpatched software, authentication errors, and more.
c. **Automated monitoring systems**: Business can enhance their cyber security by integrating automated threat detection systems. These platforms can help organizations by tracking device performance and activity, monitoring web traffic, and notifying the cyber security team when irregularities are detected.
d. **Analyzing User Behavior**: an organization can better understand what normal behavior for an employee would look like. This includes the kind of data they access, the time of day during which they log on, and their physical location. That way, any outlying behavior will stand out as unusual, and it will be easier for a security analyst to know what behavior to investigate.
e. **Threat Detection Log**: Most cyber security platforms offer advanced logging capabilities that will help you detect suspicious activity on your networks and systems. You can have access to a detailed assessment of your network's security by maintaining and reviewing these logs.

3. Awareness and Training of Employees

Employees should be sensitized and trained on protecting the business and themselves from cyber security threats. An employee is one of the easiest ways cyber criminals can get access to you and organistions data. Cyber criminals can send fraudulent emails impersonating someone in your organisation and will either ask for personal details or for access to certain files. An employee that is untrained can easily click a link that seems legitimate thereby, falling into the trap.

An employee should be educated on the following:

a. Checking links before clicking them.
b. Be prudent when sending sensitive information. If a request seems odd, verify by calling the person in question before acting upon the "request"
c. Check email addresses from the received email.
d. Maintain good passwords and passphrases
e. How to spot email phishing scams to prevent them from accidentally installing a virus.
f. Not to share their password with anybody.
g. Identifying and avoiding cyber threats.

4. Protect All Devices and Network

Protecting all devices and networks from unauthorised access is important. If devices are compromised, it becomes a problem to the businesses. Some ways you can protect your business devices and networks include:

a. **Ensure you update your software**: make sure your operating system and security software are programmed to update automatically. The updates may contain important security upgrades for recent viruses and attacks. For convenience, most updates allow you to schedule the updates after business hours. These updates fix serious security flaws, so it is important to never ignore update prompts.
b. **Install security software**: it is vital to install security software on your business computers and devices to help prevent infection. Ensure the software includes anti-virus, anti-spyware and anti-spam filters. Malware or viruses can infect your computers, laptops and mobile devices.
c. **Set up a firewall**: firewall: acts as the gatekeeper for all incoming and outgoing traffic. It is a piece of software or hardware that sits between your computer and the internet. Firewalls need to be updated regularly to make it effective.
d. **Turn on your spam filters**: spam filters will help reduce the amount of spam and phishing emails that your business receives. Spam and phishing emails can be used to infect your computer with viruses or malware or steal your confidential information. Delete Spam, phishing emails or other emails you do not known their sources. Spam filter when applied, will help reduce the chance of you or your employees opening a spam or dishonest email by accident.
e. **Passphrases**: Use passphrases instead of passwords to protect access to your devices and networks that hold important business information. Passphrases are passwords that are a phrase, or a collection of different words. They are simple for humans to remember but difficult for machines to crack. Do not use the same passphrase for everything, if you do and someone gets hold of it, all your accounts could be at risk. A secure passphrase should be long, complex, unpredictable and unique.
f. **Administrative privileges**: This privilege allows someone to undertake higher or more sensitive tasks than normal, such as installing programs or creating other accounts. These will be very different from standard privileges or guest user privileges. Criminals will often seek these privileges to give them greater access and control of your business. Only use accounts with administrative privileges when necessary, never read emails or use the internet when using an account with administrative privileges and limit those who have access to it.

5. Protect Business and Customer Information

It is vital for businesses and customer to safeguard information. It will be a problem for businesses when sensitive information are lose, and also when customer information is compromised it will damage the business reputation, which could led to some legal issues. Some ways to ensure safety of businesses and customer information are:

a. **Encrypt all Information**: this is one of best possible defense against a security breach. Encryption converts your data into a secret code before you send it over the internet. Even if hackers again access to your business and customer information, an encrypted database will mean they have nothing. Data or information should be held securely, to ensure safety of your business and customer information, encrypt data when not in use and store it as encrypted files in a password-protected environment.
b. **Always Scan for Vulnerabilities**: these are loopholes and security gaps in the software your business uses. When you scan for Vulnerabilities, it allows you to check your software stack for any recognizable security gaps or dangerous loopholes. There is always room for improvement as no software is perfect. Scanning for Vulnerabilities essentially look for flaws in the software that a hacker might be able to use to gain access to information.
c. **Restricting Access**: ensure not everyone in your organization have full access to information. Limiting access to information means there are fewer points of vulnerability for your organization. Having fewer employees with access to your business and customer information also reduces the risk of internal data abuse.
d. **Use secured Wi-Fi**: avoid using public Wi-Fi or an insecure connection that could put your business and customer information at risk when working remotely or when connecting to the internet. Public Wi-Fi networks, those that are open to everyone and not secured by a password, can’t be trusted.
e. **Use Screen and Device Lock**: this is an important security measure. Always remind employees to log out of all organization application every time they take a break. Taking steps to lock your screen when you leave your desk is a simple thing to do, but will prevent someone else from accessing your computer. Remember that employee computers and devices are not 100% manned all the time.
f. **Dispose Records and Equipment Securely**: ensure no business or customer information is left on computers, laptops or any other devices before getting rid of them. Always delete completely from computer or any other devices. This will ensure no one have access to information they are not supposed to see when you dispose of the equipment.
g. **Avoid BYOD (Bring your own device) Trend**: organizations tend to ignore the security implication of BYOD because it increases productivity and reduce costs. Accessing sensitive information on personal devices such as laptops, smart phone and other portable devices means that data is travelling outside the confines of your organization. Therefore restrict the sort of information that can be transferred outside organisation devices.

6. Backup Business and Customer Information

Backing up businesses data is crucial for protecting business continuity. The business can recover information lost after experiencing a cyber attack or have computer issues. It is important that businesses back up most vital information regularly. It is appropriate to use multiple back-up methods to help ensure the safety of your essential files. Businesses need to establish a data backup system that follows these three steps:

a. Backup business data regularly
b. Create backups on reliable media or in the cloud
c. If using media for backups keep the devices in a secure, off-site location

Benefits of the Proposed Cyber Security Framework

i. The proposed framework will provide SMEs with clear understanding on how to identify cyber threats to their business and the appropriate strategy on how to act accordingly.
ii. SMES will be able to mitigate identified threats and develop the needed cyber culture to implement appropriately the proposed framework security segments which will be able to reduce cyber threats to their businesses.
iii. The proposed framework will not require an expert to implement making it less expensive and easy for SMEs.
iv. The proposed framework is cost effective as it was designed with the consideration of SMEs in mind to identify and mitigate cyber attacks.

CONCLUSION AND RECOMMENDATION

The study thoroughly analyzed six known cyber security frameworks with the aim of identifying their basic strengths and weaknesses. Current literatures regarding cyber security challenges in SMEs were highlighted with the research gap identified. Considering the limitations identified in the existing frameworks, a cyber security framework for SMEs in Nigeria that is dynamic, simple and cost effective was proposed and discussed. The proposed framework can be used strategically to identify and mitigate specific cyber risks, achieving the same aim as a global framework**.** Most of the existing cyber security frameworks are expensive, broad, require certifications and substantial expertise which makes it difficult for SMEs to implement. However, the proposed framework is cost effective and simple to implement. Another feature of the proposed framework is that it was designed with the consideration of SMEs in mind, which focuses clearly on understanding SMEs context at the national and international levels. Therefore, as a recommendation from this study, SMEs need to overcome the risk of getting attacked by implementing the proposed recommended framework. The framework provides an easy guideline that can help SMEs to attain a good cyber security infrastructure that can safeguard their businesses.

REFERENCES

Adepetun, A. (2022). *Cyber attack on Nigerian SMEs up by 89 per cent in 2022*. The Guardian Nigeria News - Nigeria and World News. https://guardian.ng/business-services/cyber-attack-on-nigerian-smes-up-by-89-per-cent-in-2022/

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Antunes, M. G., Mucharreira, P. R., Justino, M. R. T., & Texeira-Quirós, J. (2021). Effects of Total Quality Management (TQM) Dimensions on Innovation—Evidence from SMEs. *Sustainability*, *13*(18), 10095. https://doi.org/10.3390/su131810095

Apau, R., Koranteng, F. N., & Gyamfi, S. A. (2019). Cyber-Crime and its Effects on E-Commerce Technologies. *Journal of Information,* 5(1), 39–59. https://doi.org/10.18488/journal.104.2019.51.39.59

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. *CEUR Workshop Proceedings*, *1816*(2015), 175–193.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Bada, M., & Sasse A. 2014. Cyber security awareness campaigns: Why do they fail to change behaviour? Accessed March 14, 2017. http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid. *Risk Analysis*, 40(9), 1744–1761. https://doi.org/10.1111/risa.13511

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cyber security evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Bisson, D. (2021). *The State of Small Business Cyber security in 2021*. Security Intelligence. Retrieved 20.01.22 from: https://securityintelligence.com/articles/state-small-business-cybersecurity-2021/

BullGuard. (2020). New Study Reveals One In Three SMBs Use Free Consumer Cyber security And One In Five Use No Endpoint Security At All. BullGuard. Retrieved 21.02.22 from: https://www.bullguard.com/press/press-releases/2020/new-study-reveals-one-in-three-smbs-use-free-consu.aspx

Calabrese, R., Andreeva, G., & Ansell, J. (2019). "Birds of a feather" fail together: Exploring the nature of dependency in SME Defaults. *Risk Analysis*, 39(1), 71– 84. https://doi.org/10.1111/risa.12862

Chatterjee, D. (2019). Should executives go to jail for cyber security breaches? *Journal of Organizational Computing and Electronic Commerce*, 29(1), 1– 3.

Cohen, D., Elalouf, A., & Zeev, R. (2022). Collaboration or separation maximizing the partnership between a 'Gray hat' hacker and an organization in a two-stage cyber security game. *International Journal of Information Management Data Insights, 2* (1), Article 100073. 10.1016/j.jjimei.2022.100073.

Emer, A., Unterhofer, M., & Rauch, E. (2021). A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises. *IEEE Engineering Management Review*, *49*(2), 98–109. https://doi.org/10.1109/emr.2021.3078077

Hall, J. (2020). *A guide to the NIST Cyber Security Framework*. IFSEC Insider | Security and Fire News and Resources; IFSEC Insider. https://www.ifsecglobal.com/cyber-security/a-guide-to-the-nist-cyber-security-framework/

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance*, 22(3/4), 240– 260. https://doi.org/10.1108/JRF-02-2020-0024

Jafari-Sadeghi, V. (2021). Internationalisation, risk-taking, and export compliance: A comparative study between economically advanced and developing Country. *International Journal of Entrepreneurship and Small Business*, 43(3), 384– 408. https://doi.org/10.1504/IJESB.2021.10039076

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cyber security practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access*, *9*, 99339–99363. https://doi.org/10.1109/ACCESS.2021.3097144

Kim, D., & Solomon, M. (2016). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

MacMullen, J. (2022). *COSO Framework: What It Is and How You Can Implement It*. https://techgenix.com/coso-framework/

Mijnhardt, F., Baars, T. & Spruit, M. (2016) 'Organizational Characteristics Influencing SME Information Security Maturity', Journal of Computer Information Systems, 56(02), pp. 106-115

Morgan S. (2021) Top 5 cyber security facts, figures, predictions, and statistics for 2020 To 2021. https:// cyber security ventures. com/ top-5- cyber security- facts-figures- predictions- and- statistics- for- 2019- to- 2021/.

Moura, J., & Serrão, C. (2018). Security and Privacy Issues of Big Data. Web Services, October 2017, 2197–2229. https://doi.org/10.4018/978-1-5225-7501-6.ch114

Muhati, E. (2018). Factors affecting cyber-security in Kenya -a case of small medium enterprises. URL:https:// su-plus.strathmore. edu/ bitstream/ handle/ 11071/ 6013/ Factors%20affecting%20cyber%20-%20security%20in%20Kenya%20-%20A%20Case% 20of%20Small%20Medium%20Enterprises.pdf?sequence=3.

Mutalib, M. M. A., Zainol, Z., & Halip, M. H. M. (2021). Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, *6*, 1–6. https://doi.org/10.1109/icraie52900.2021.9703991

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralization approach to managing information systems security by small businesses. The African Journal of Information Systems, 8(1), 3. 42-63. Retrieved from http://digitalcommons.kennesaw.edu/ajis/

Office of the National Security Adviser (ONSA). (2021). *Federal republic of nigeria national cybersecurity policy and strategy*. http://ctc.gov.ng/wp-content/uploads/2021/02/national-cybersecurity-policy-and-strategy-2021_e-copy_24223825.pdf

Pngwing. (2023). The CIS Critical Security Controls for Effective Cyber Defense Computer security Center for Internet Security SANS Institute, Cyber Essentials, text, information Technology, technical Standard png | PNGWing. Www.pngwing.com. https://www.pngwing.com/en/free-png-dmopg

Ponemon Institute. (2019). Exclusive Research Report 2019 Global State of Cyber security in Small and Medium-Sized Businesses. https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and Lessons Learned on Raising SME Awareness about Cybersecurity. *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0007574305580563

Rae, A., & Patel, A. (2019). Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K. *Information Security Practice and Experience*, 362–380. https://doi.org/10.1007/978-3-030-34339-2_20

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. *Information Technology and People*, 32(5), 1125– 1129. https://doi.org/10.1108/ITP-10-2019-564

Singh, R., Chandrashekar, D., Subrahmanya Mungila Hillemane, B., Sukumar, A., & Jafari-Sadeghi, V. (2022). Network cooperation and economic performance of SMEs: Direct and mediating impacts of innovation and internationalisation. *Journal of Business Research*, *148*, 116–130. https://doi.org/10.1016/j.jbusres.2022.04.032

Soujanya N. (2023). *What Is COBIT Framework - COBIT Principles?* Mindmajix. https://mindmajix.com/cobit-framework

Sunnews. (2022). What are the major cyber threats faced by SMEs in Nigeria? https://sunnewsonline.com/what-are-the-major-cyber-threats-faced-by-smes-in-nigeria/? Expand _article=1

Verizon (2020) 2019 Data Breach Investigations Report, Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigationsreport.pdf

Vinck, J. (2021). *How FAIR & ISO 27001 Work Together*. Www.risklens.com. https://www.risklens.com/resource-center/blog/how-fair-iso-27001-work-together

****