Protecting Critical Infrastructure in Nigeria: A Framework for Integrated Cybersecurity Approach

Destiny Young

Faculty of Natural and Applied Sciences, Department of Computer Science and Information Technology, Paul University, Awka, 420102, Anambra State, Nigeria

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90700095

Received: 26 June 2025; Accepted: 17 May 2025; Published: 31 July 2025

ABSTRACT

This paper proposes an integrated cybersecurity framework optimised for Nigeria's critical infrastructure protection. The framework leverages some recognised standards like International Organisation for Standardisation (ISO) 27001 and National Institute of Standards and Technology (NIST), while including technological advanced components such as threat intelligence, incident response, and continuous monitoring. It addresses sector-specific challenges confronting Nigeria's oil and gas, telecoms, power, and healthcare industries. The framework's unique characteristics include:

1. Tailoring to Nigeria's peculiar circumstances.
2. Improving threat intelligence capabilities.
3. Industry-centric recommendations and implementation strategies.
4. Innovative cybersecurity technologies integration.
5. Mapping sections to complement Nigeria’s existing regulations.
6. Comprehensive, targeted incident response plans.

By combining these features, the proposed framework offers a more robust and adaptable approach to cybersecurity risk management for Nigeria's critical infrastructure, boosting resilience against changing cyber threats and ensuring the continuity of key services.

Keywords: critical infrastructure, cybersecurity, cybersecurity framework, risk management, data protection

INTRODUCTION

Critical infrastructure (CI) is a sum of systems (physical and cyber-based), telecommunications networks, public utilities, and services that are fundamental to the basic operations of a society. With the increasing sophistication of zero-day attacks and the rapid expansion of the attack surface in critical infrastructure, cyber-attacks in this area could have a disruptive and devastating effect on a society and should attract the needed attention from the government. These attacks can disrupt essential services, compromise sensitive data, and even threaten national security.

According to the Africa Cyber Security Report 2016, Nigeria had substantial cybersecurity issues, with an estimated loss of $550 million due to cyber-attacks in 2016 alone (Serianu, 2017). This number emphasizes the urgent need for a robust, coordinated cybersecurity system to secure Nigeria's vital infrastructure.

The readiness and capacity to react to significant events involving a country's or region's critical infrastructure is known as critical infrastructure protection, or CIP. It acknowledges the importance of specific infrastructure components to a nation's economic and national security as well as the necessary precautions to safeguard them (OPSWAT, Inc., 2023).

A widely recognised and known international standard is the ISO 27001 - which provides a framework for establishing, implementing, and maintaining an Information Security Management System (ISMS) (ISO/IEC 27001:2022, 2023). While ISO 27001 offers a strong foundation for cybersecurity implementation, its

effectiveness can be enhanced by integrating additional components, such as threat intelligence, incident response planning, and continuous monitoring.

This paper proposes an integrated cybersecurity framework that builds upon ISO 27001 by incorporating these additional elements. The framework seeks to provide an integrated cybersecurity approach to securing government infrastructure against evolving cyber threats.

Critical infrastructure in Nigeria

Critical infrastructures in the context of Nigeria comprise various sectors vital for national functioning. Some of the critical infrastructures are:

- Oil and Gas Pipelines: Oil and Gas sector is Nigeria's major source of foreign exchange.
- Telecommunications Networks: This is sector is considered critical for connectivity and communication within the nation.
- Power Infrastructure: Essential for sustaining economic activities and daily life.
- Healthcare Facilities: Integral for the nation's health system and emergency management.

Research Problem

The paper identifies the vulnerability of Nigeria's critical infrastructure to cybersecurity threats as a significant concern. The complex interconnections of these systems mean that any cybersecurity threat can jeopardise national security, necessitating robust and adaptable security measures (Barrett; 2018).

Research Objectives

The primary objective of the study is to propose an integrated cybersecurity framework to protect Nigeria's critical government infrastructure. This framework aims to:

- Leverage established cybersecurity standards, such as ISO 27001.
- Integrate additional components like threat intelligence, incident response, and continuous monitoring.
- Provide a comprehensive approach to mitigating cyberattacks and ensure the protection of critical government assets (Barrett; 2018).

Significance of the Research

The significance of the study lies in its potential to enhance the cybersecurity posture of Nigeria's critical infrastructure by:

- Mitigating the risks associated with cyber threats to critical infrastructure.
- Ensuring the continuous functionality of essential services that are vital to Nigeria's economic security and public safety.
- Providing a structured approach to managing cybersecurity risks, thereby improving resource allocation and incident response capabilities (Barrett; 2018).

Related Works

Several existing frameworks address cybersecurity for critical infrastructure.

Study	Methodology	Key Findings	Limitations
Ismaila et al. (2023)	Design framework analysis	Developed cybersecurity solutions for threats to electricity power systems in Nigeria	Focused only on electricity sector; limited scope
Udotai (2007)	Framework development	Proposed a cybersecurity framework for Nigeria focusing on policy changes, capacity building, and international cooperation	Dated study; may not reflect current cybersecurity landscape
Daniel & Victor (2024)	Literature review	Identified emerging trends in cybersecurity for critical infrastructure protection in Nigeria	Theoretical study; lacks empirical data
Daily Trust (2023)	News report analysis	Exposed vulnerabilities in Nigeria's IT security, particularly in digital infrastructure	Limited to reported incidents; may not cover all sectors
Barrett (2018)	Framework development	Presented the NIST Framework for Improving Critical Infrastructure Cybersecurity	Not specifically tailored to Nigerian context
DeLima (2022)	Industry analysis	Highlighted ongoing cyber security threats to critical infrastructure globally	Not specific to Nigeria; general overview
Paganini (2017)	Framework analysis	Introduced the NIST Cybersecurity Framework for cyber menaces landscape	Not specific to Nigeria; general cybersecurity approach

Table 1.1: Related Studies/Literature

Table 1.1 is a compilation of some research papers discussing cybersecurity and protection of infrastructure specifically in Nigeria's context. These studies delve into topics such, as developing frameworks for security evaluations and analyzing industries to adhere to standards, shedding light on the existing conditions and hurdles faced by infrastructure protection in Nigeria and the rest of the world.

The proposed framework draws upon these existing frameworks while adapting them to the specific needs of government infrastructure. It emphasizes the importance of compliance with ISO 27001 standards and integrates additional components for enhanced risk management, threat intelligence, and incident response capabilities.

Recent Studies and Frameworks

A study by Osho, et al (2015), provides an in-depth analysis of Nigeria's National Cyber Security Policy and Strategy. The authors highlight key strengths and weaknesses, noting that while the policy addresses many critical areas, it lacks specific implementation guidelines and metrics for measuring success. This analysis can inform the development of our proposed integrated framework by identifying areas that need more concrete action plans.

Emerging Trends in Cybersecurity

Recent literature highlights the evolving cybersecurity landscape for critical infrastructure, highlighting emerging trends and challenges such as sophisticated cyber threats, regulatory compliance, and industry collaboration (How Cyber-attacks Exposed Nigeria's IT Security Vulnerability in 2023 - Daily Trust, 2023).

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework remains a cornerstone

for improving critical infrastructure cybersecurity (Barrett, 2018). It provides a risk-based approach that integrates industry standards and best practices, helping organisations manage cybersecurity risks effectively (How Cyber-attacks Exposed Nigeria's IT Security Vulnerability in 2023 - Daily Trust, 2023).

CISA Cybersecurity Performance Goals

The Cybersecurity and Infrastructure Security Agency (CISA) has developed Cybersecurity Performance Goals (CPGs) aligned with the NIST Framework (Cross-Sector Cybersecurity Performance Goals | CISA, n.d.). These goals serve as foundational cybersecurity practices applicable to all critical infrastructure sectors, aiming to reduce operational risks ((2) (PDF) Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review, 2024).

Framework for Cybersecurity in Nigeria

The International Telecommunication Union (ITU) has outlined a framework focusing on policy changes, capacity building, and international cooperation to enhance cybersecurity in Nigeria. This framework emphasizes the importance of public-private partnerships and regulatory improvements (Daniel, S & Victor, S; 2024).

Case Studies and Examples

Successful Cybersecurity Implementation

Several case studies illustrate successful cybersecurity implementations in critical infrastructure. For instance, the electricity sector in Nigeria has seen the development of cybersecurity solutions tailored to protect against threats and attacks, highlighting the importance of sector-specific approaches.

Cybersecurity Challenges in Nigeria

- Oil and Gas Sector: This sector generates about 10% of the country's Gross Domestic Product and is known to be often attacked through cyber threats. Recently, a malware attack on the systems used in the operations of a big oil company caused tremendous disruption in operations.

- Telecommunications Sector: This fast growing sector currently is supporting over 200 million mobile subscribers, and it continually faces constant threats from hackers. A leading telecom provider with millions of users was in 2020 attacked and its database leaked.

- Power Sector: Despite the current reforms, this sector is not free from infrastructure challenges that can be worsened by cyber threats. According to a study conducted in 2019, 35% of the cyber-attacks aimed at Nigeria attacked the power sector hence threatening the stability of the power grid in the country.

Successful Cybersecurity Implementation

Recent reports have exposed vulnerabilities in Nigeria's IT security, particularly in the face of cyber-attacks targeting vital digital infrastructure. These incidents underscore the need for robust cybersecurity frameworks and the implementation of best practices to safeguard critical assets (Ismaila, et al; 2023).

International Example

Globally, successful cybersecurity strategies have been implemented in various sectors, such as energy and telecommunications. These examples often involve adopting comprehensive frameworks like ISO 27001 and integrating advanced threat intelligence and incident response capabilities to enhance resilience against cyber threats (International Journal of Critical Infrastructure Protection | ScienceDirect.com by Elsevier, n.d.).

Analysis of Existing Frameworks

Framework	Key Features	Strengths	Limitations
NIST Cybersecurity Framework (CSF)	- Five core functions: Identify, Protect, Detect, Respond, Recover - Risk-based approach - Integrates industry standards and best practices	- Flexible and adaptable to various sectors - Widely recognised and adopted - Provides common language for cybersecurity	- Voluntary nature may lead to inconsistent adoption - Lacks sector-specific guidance - May require significant resources to implement fully
ISO 27001	- Information Security Management System (ISMS) - Risk assessment and management - Continuous improvement process	- Internationally recognised standard - Comprehensive approach to information security - Certification available	- Generic approach, not tailored to critical infrastructure - Can be complex and resource-intensive to implement - May not address all sector-specific risks
CISA Cybersecurity Performance Goals (CPGs)	- Aligned with NIST Cybersecurity Framework (CSF) functions - Sector-agnostic baseline practices - Focus on operational risk reduction	- Provides concrete, actionable goals - Designed for critical infrastructure - Regularly updated	- Voluntary nature - May not cover all sector-specific needs - Relatively new, with limited long-term track record
ITU Framework for Nigeria	- Focus on policy changes - Emphasis on capacity building - International cooperation	- Tailored to Nigerian context - Addresses regulatory aspects - Promotes public-private partnerships	- May lack technical depth - Limited focus on operational aspects - Potentially outdated (2007)
U.S. DOE Electricity Subsector Cybersecurity RMP	- Sector-specific approach - Risk management process - Aligns with NIST guidelines	- Tailored to electricity sector - Detailed risk management guidance - Incorporates industry best practices	- Limited to electricity sector - May not fully address cross-sector dependencies - U.S.-centric approach
Proposed Integrated Framework	- Builds on ISO 27001 - Incorporates threat intelligence and incident response - Tailored for Nigerian critical infrastructure	- Comprehensive approach - Addresses specific Nigerian challenges - Integrates advanced technologies	- Untested in real-world scenarios - May require significant resources to implement - Potential resistance to change

Table 1.2: Analysis of Existing Frameworks

The above table compares seven comparable frameworks, highlighting their essential features, strengths, and drawbacks. Each framework offers diverse approaches to critical infrastructure security, with varying degrees of specialisation, adaptability, and comprehensiveness. The suggested integrated framework intends to combine the strengths of recognised standards like ISO 27001 with unique solutions for the Nigerian environment, addressing some of the shortcomings of existing frameworks.

METHOD

This paper aims at providing a conceptual framework of an integrated cybersecurity model based on ISO 27001 and NIST Frameworks for improving Critical Infrastructure Cybersecurity. The framework is defined based on a synthetisation of existing literature, the analysis of industry best standards and relevant standards.

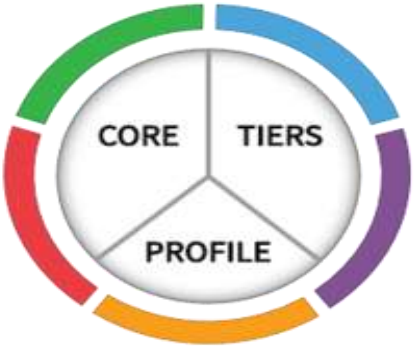

Figure 1.1: Cybersecurity Framework Core (Cybersecurity Framework Components | NIST, 2023)

The Framework Core:

The Core Framework is a collaborative resource for critical infrastructure industries, outlining essential cybersecurity tasks, outcomes, and valuable resources. Developed by NIST in 2018, it provides a shared blueprint for cybersecurity, organising key activities into five clear functional areas. These include: identifying potential risks and vulnerabilities, protecting assets with effective measures, detecting signs of compromise, responding swiftly to contain incidents, and recovering systems and services after a breach. This structured approach facilitates industry collaboration and strengthens cybersecurity posture.

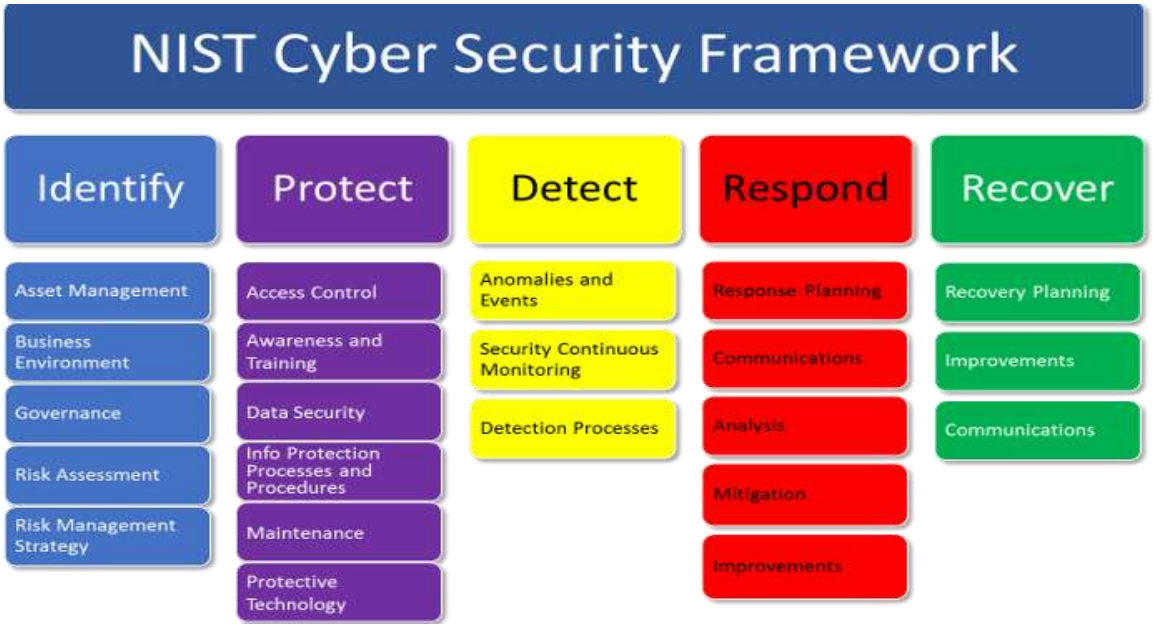

Figure 1.2: NIST Cyber Security Framework (Paganini, 2017)

The Framework Implementation:

An organisation's approach to cybersecurity risk management is shaped by its implementation of the Framework's Tiers, as outlined by NIST in 2018. The Tiers reflect the organisation's maturity in managing cybersecurity risks, progressing from a basic, Partial approach (Tier 1) to more sophisticated levels: Risk-Informed (Tier 2), Repeatable (Tier 3), and ultimately, Adaptive (Tier 4), which enables proactive and responsive security postures. This tiered structure provides a valuable benchmark for organisations to assess and enhance

their cybersecurity risk management capabilities.

The Framework Profile:

According to NIST's 2018 guidelines, Framework Profiles provide a tailored snapshot of an organisation's specific needs, goals, risk tolerance, and resources, aligned with the desired outcomes of the Framework Core.

CISA Cybersecurity Best Practice for Critical Infrastructure

The Cybersecurity and Infrastructure Security Agency (CISA) has introduced Cybersecurity Performance Goals (CPGs), a comprehensive set of practices designed to mitigate risks to critical infrastructure operations. These goals are aligned with the NIST Cybersecurity Framework's (CSF) five key functions:

- Identify: Recognise potential risks
- Protect: Safeguard assets
- Detect: Monitor for threats
- Respond: Address incidents
- Recover: Restore services

The CPGs provide a structured approach to enhancing cybersecurity resilience.

PROPOSED INTEGRATED CYBERSECURITY FRAMEWORK

The proposed integrated cybersecurity framework presents significant advantages over conventional approaches to securing government infrastructure. This comprehensive solution incorporates key components of OPSWAT technology, offering a more efficient and effective method of protection. By consolidating various security measures into a single, cohesive system, this framework addresses the multifaceted challenges faced by government IT systems. The integration of OPSWAT elements enhances the framework's capability to detect, prevent, and respond to a wide array of cyber threats. This approach not only streamlines security processes but also potentially reduces operational costs and improves overall system resilience. The framework's holistic nature allows for better coordination between different security functions, potentially closing gaps that might exist in more fragmented security setups. As cyber threats continue to evolve in sophistication, this integrated approach provides a more adaptive and robust defence mechanism for critical government digital assets.

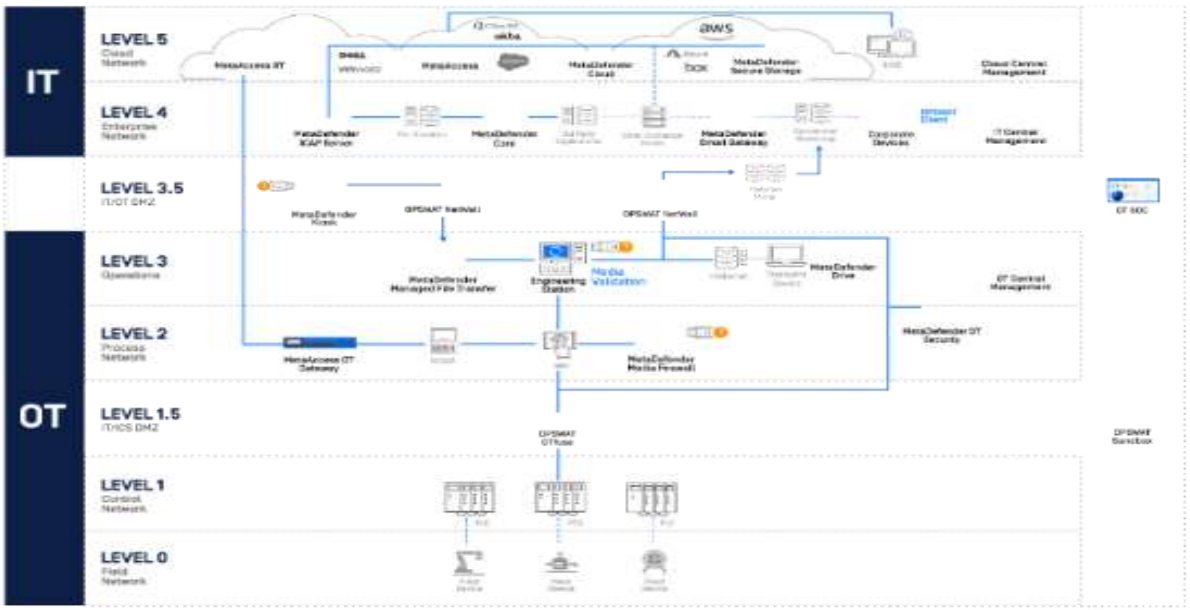

Figure 1.3: OPSWAT Integrated Critical Infrastructure Protection Design (opswat.com, 2023)

OPSWAT, a leading cybersecurity services provider in the critical infrastructure sector, believes that fundamental to effectively securing critical infrastructure is eliminating malware and zero-day attack (OPSWAT, Inc., 2023b).

To solve the challenges faced by critical infrastructure organisations and to shut off major attack vectors, this Framework proposes a set of protection technologies for the protection of critical infrastructure sector in Nigeria as follows:

Deep Content Disarm and Reconstruction (CDR)

Malware is becoming more sophisticated and adept at eluding detection by conventional anti-malware programmes. Antivirus software that relies on signatures to identify threats is vulnerable to zero-day malware. Enterprises frequently employ traditional malware prevention, which is insufficient against contemporary threats since it is too passive. Businesses want sophisticated threat protection that handles each file as a possible threat and does not rely on detection. This is where Deep Content Disarm and Reconstruction come in.

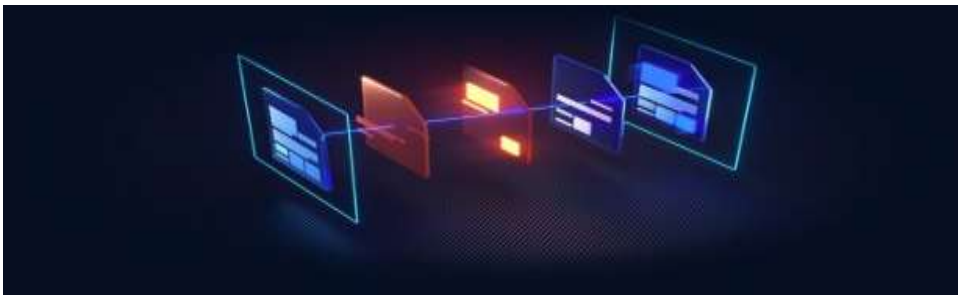

Figure 1.4: OPSWAT Deep CDR Scan (opswat.com, 2023)

Potentially harmful and against-policy content that is concealed in files is exposed by Deep CDR. This innovative solution offers web applications complete prevention-based security by identifying and eliminating possible threats before they have a chance to do any damage (OPSWAT, Inc., 2023b).

File-Based Vulnerability Assessment

The number of application vulnerabilities rises with software complexity. The number of known vulnerabilities, which include file-based vulnerabilities, binary components, Internet of Things (IoT) firmware, and operating system and application vulnerabilities, breaks record every year.

Figure 1.5: System Files Icon (vecteezy.com)

File-Based Vulnerability technology enables security experts and IT administrators to scan machines for the purpose of finding vulnerabilities associated with specific files or application versions before attackers could exploit those vulnerabilities. This offers security professionals the ability to:

1. Check certain programme types for known vulnerabilities prior to installation.
2. Check systems for known vulnerabilities when devices/data is at rest
3. Rapidly scan loaded libraries and running apps for vulnerabilities

Proactive Data Loss Prevention (DLP)

Confidential business information privacy is a vital lifeline for any organisation in today's fiercely competitive and litigious business world. Channels like the internet, emails, portable storage devices, and cloud services, can be used to reveal or transmit confidential information to unauthorised parties. Examples of these channels include trade secrets, intellectual property, and financial statements. Data breaches can be expensive, harm a business's reputation and brand, and erode partners' and consumers' trust.

By content-checking files and emails before they are exchanged, proactive DLP can assist organisations in preventing sensitive and regulated material from leaving or entering the organisation's systems.

Figure 1.6: OPSWAT Data Loss Prevention (opswat.com, 2023)

Benefits of Data Loss Prevention (DLP):

- Prevent the entry or exit of private and sensitive data from an organisation without impeding user productivity.
- Use AI driven by machine learning to find and categorise unstructured text into pre-established groups.
- By automatically recognising different data structures, including passwords, access keys, API keys, and key IDs produced by outside parties, we can stop secret breaches.
- Create unique policies to satisfy our unique policy needs.

Multi-scanning

Advanced threat detection and prevention technology known as multi-scanning shortens outbreak detection timeframes, boosts detection rates, and strengthens single vendor anti-malware solution resilience.

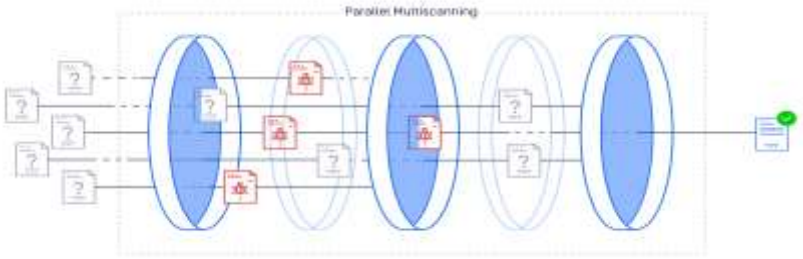

Figure 1.7: OPSWAT Parallel Multi-scanning (opswat.com, 2023)

Threat Intelligence

In critical infrastructure contexts, preventing or halting attacks requires efficient and sophisticated analysis of dangerous content trends. Access points for binary reputation, vulnerable programmes, malware analysis reports, portable executable information, static and dynamic analysis, IP address reputation, and—most importantly—the correlations between them can be all analysed by threat intelligence technology, which examines data from millions of devices.

Figure 1.8: OPSWAT Advanced Threat Prevention Platform (OPSWAT, 2023)

Digitally connected organisations, particularly large firms with thousands of employees and contractors, are exposed to multiple attack vectors, making it challenging for them to monitor and defend against threats. File uploads, mobile media players, and email attachments are just a few examples of data transfer channels that can be vulnerable to focused attacks that harm a company's brand, finances, and clients in addition to damaging critical infrastructure, and sensitive equipment.

Threat intelligence offers comprehensive file upload security to guard against malware and data breaches offering a combination of: Analysis, Detection, and Prevention capabilities.

Sandbox

Sandboxes are commonly used to run untested code and third-party apps in an attempt to reduce risk because it's critical to maintain crucial infrastructure environments working efficiently. Because of this, CIP cyber experts are able to evaluate data without giving it access to networks and systems that are essential to mission operations.

Figure 1.9: OPSWAT Adaptive Threat Analysis? (OPSWAT, 2023)

The special adaptive threat analysis technology of Filescan sandbox allows for zero-day malware detection and has the ability to detect indicators of comprise. (OPSWAT, Inc., 2023c).

Endpoint Compliance

Certain businesses are required to comply with internal and external guidelines, such as Payment Card Industry (PCI), Nigeria Data Protection Regulation (NDPR), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA). Monitoring and maintaining compliance on endpoints in a heterogeneous environment can be very challenging.

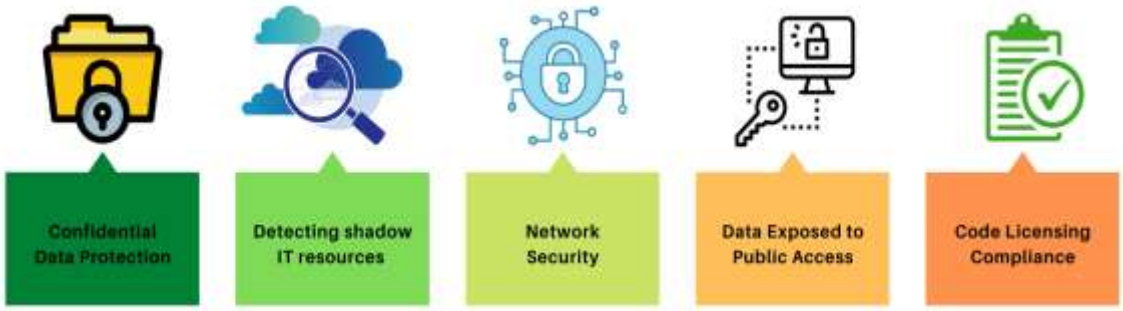

Figure 1.10: Manage Endpoint Compliance as Code (Charles, 2023)

Organisations can use Endpoint Compliance to find, assess, and update device apps that violate a set of operational and security guidelines that have been set forth and upheld. It reduces the risk of data loss and the chance that a malware infection would propagate throughout the entire organisation.

Benefits:

1. Endpoint Anti-Malware Detection
2. User Authentication Compliance
3. Disk Encryption Compliance
4. Patch Management Compliance

Endpoint Vulnerability Assessment

An endpoint is any device that connects to your network. Every device has the ability to spread infection. Complicating endpoint vulnerability is the quantity of apps on each device and whether or not they comply with security regulations. Even a small business may have thousands of potential vulnerabilities due to compromised installed software and outdated or absent operating system patches.

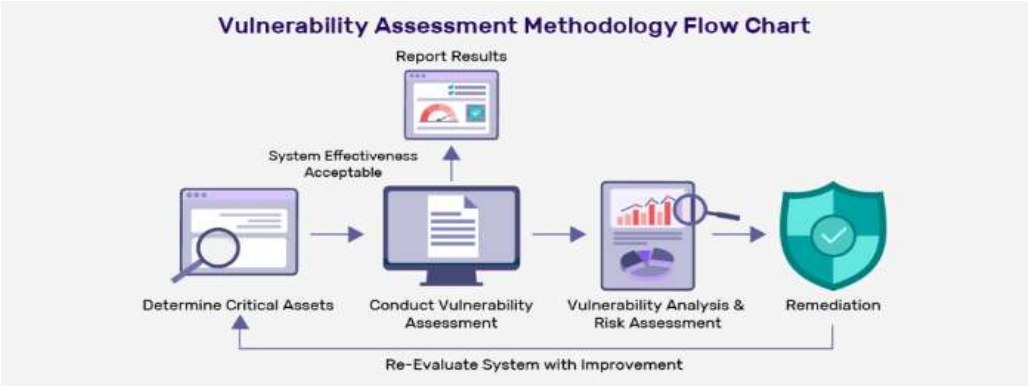

Figure 1.11: Vulnerability Assessment Methodology Flow Chart (Indusface weekly, 2023)

By verifying that all applications are running the most recent versions, Endpoint Vulnerability Assessment enhances endpoint security. When vulnerabilities are found, they can be fixed as quickly as feasible via automatic patching. This can also be accomplished manually by obtaining the remediations that are available and selecting the update that best meets the requirements of the organisation.

Endpoint Malware Detection

Endpoint Malware Detection technology uses machine learning (AI), heuristics, and signatures to detect a variety of threats at the gateway before they reach a network. It has one main benefit: it may increase its knowledge base by learning from multi-scanning findings. As a result, it has excellent accuracy when identifying new threats. It also has a decreasing false positive rate since it will routinely analyse samples using multiple anti-malware engines and use the data generated to train its intelligent Endpoint Malware Detection system.

Endpoint Application Removal

Security programs including firewalls and antivirus software, as well as Potentially Unwanted Applications (PUA), can be removed with the help of the Endpoint Application Removal tool. System administrators can use it to prevent users from installing and using certain popular and legitimate apps considered not needed in the organisation.

Data Protection

With data protection controls like anti-keylogger, anti-screen capture, and removable media protection, organisations can enable data integrity and prevent file-based attacks on endpoints. This limits access to authorised processes or prohibits users from using portable devices like USBs and smartphones in order to achieve this goal.

Business Email Compromise (BEC) Attack Detection and Prevention.

By using zero-day prevention technology in conjunction with a sophisticated email gateway security layer, organisation can augment their threat detection rates to 99% and stop Business Email Compromise (BEC) attacks. Anti-phishing and spam filtering can be implemented to guard against malware outbreaks.

By leveraging established cybersecurity standards and incorporating additional components presented in this paper, the framework provides a comprehensive and adaptable approach to mitigating cyber risks.

Despite these challenges, the benefits of adopting an integrated cybersecurity framework outweigh the risks.

By proactively addressing cybersecurity threats, Nigerian government can protect critical infrastructures, ensure data security, and maintain public trust.

Comparability Analysis of the Proposed Framework

The proposed integrated cybersecurity framework for Nigeria's critical infrastructure incorporates several novel elements that distinguish it from existing models. A comparative analysis reveals key differences between our framework and three other notable approaches. The following table presents a detailed comparison, highlighting the unique aspects of our proposed framework:

Feature	**Proposed Framework**	**NIST Cybersecurity Framework**	**ISO 27001**	**ITU Framework for Nigeria**
Foundation	ISO 27001 with enhancements	Risk-based approach	Information Security Management System (ISMS)	Policy and capacity building focus
Scope	Tailored for Nigerian critical infrastructure	Generic for all critical infrastructure	Generic for all organisations	Broad cybersecurity landscape in Nigeria
Threat Intelligence Integration	Advanced, real-time threat intelligence	Limited	Not explicitly included	Not explicitly included
Incident Response	Comprehensive, sector-specific plans	General guidelines	General guidelines	Limited focus
Continuous Monitoring	Emphasized with specific technologies	General principle	Part of ISMS	Not explicitly addressed

Regulatory Compliance	Aligned with Nigerian regulations	Voluntary guidelines	Generic compliance	Focus on policy development
Sector-Specific Approach	Detailed considerations for oil & gas, telecom, power, and healthcare	Generic approach	Generic approach	Limited sector-specific guidance
Technology Integration	Detailed guidance on integrating advanced cybersecurity technologies	Limited technology recommendations	Technology-neutral	Limited technology focus
Public-Private Collaboration	Emphasised for threat sharing	Encouraged	Not explicitly addressed	Mentioned but not detailed

Table 1.3: Comparative Analysis of the Proposed Framework

This comparative overview demonstrates the distinctive features of our framework, illustrating how it addresses specific challenges within Nigeria's cybersecurity landscape. By examining these differences, we can better understand the potential impact and effectiveness of our proposed approach in safeguarding the nation's critical infrastructure.

The framework that has been proposed is distinguished in several critical respects:

1. **Tailored Approach:** In contrast to other widely used models such as NIST and ISO 27001 frameworks, our model is developed for the Nigerian environment and takes into consideration most critical sectors including the oil and gas and telecommunications industries, which are most affected by auditing challenges in Nigeria (Udotai, 2007).

2. **Enhanced Threat Intelligence:** The framework includes high-level threat intelligence functions and is not just based upon the concepts identified in the other frameworks (OPSWAT, Inc., 2023a).

3. **Sector-Specific Guidance:** Bearing in mind the considerations for some of the critical sectors in Nigeria offers much more concrete measures as opposed to NIST and ISO 27001 compliance (Ismaila et al., 2023).

4. **Technology Integration:** Unlike the general guidelines of the ISO 27001 or the few recommendations given by NIST, our framework offers a precise checklist of measures with focus on the utilization of innovative cybersecurity technologies such as the Deep Content Disarm and Reconstruction (Deep CDR) and the proactive Data Loss Prevention (DLP) (OPSWAT, Inc., 2023a).

5. **Regulatory Alignment:** The framework is intended to be consistent with Nigerian regulations, providing a more pertinent compliance approach than the voluntary nature of NIST or the generic compliance of ISO 27001 (Udotai, 2007).

6. **Comprehensive Incident Response:** Our approach offers comprehensive, sector-specific incident response plans that are specifically tailored to Nigerian critical infrastructure, in contrast to other frameworks that provide generic guidelines (Barrett, 2018).

DISCUSSIONS

Benefits of the Proposed Framework

The key benefits of this framework include:

1. Enhanced Risk Management: A structured approach to mitigating cybersecurity risks, leading to more efficient allocation of available resources.
2. Improved Security Posture: Implementing robust security controls integrated cybersecurity best practices and tailoring them to address specific threats.
3. Faster Incident Response: A well-defined incident response plan enables rapid and coordinated action to contain and mitigate cyberattacks.
4. Continuous Improvement: Consistent monitoring and assessment of the ISMS ensure its effectiveness in the face of evolving cyber threats.
5. The International Telecommunication Union (ITU)'s Global Cybersecurity Index (GCU) 2018 ranks Nigeria 57th out of 175 countries in terms of cybersecurity commitment (International Telecommunication Union (ITU), 2018). While this signals growth, there is still tremendous space for development. Our proposed framework should attempt to enhance Nigeria's standing in future rankings by addressing the key areas examined by the GCI: legal, technical, organisational, capacity building, and collaboration measures.

Challenges and Mitigation Strategies

(Ogu, Ogu, & Oluoha, 2020) identified numerous critical difficulties in Nigeria's cybersecurity ecosystem, including inadequate infrastructure, lack of competent workers, and insufficient funding. Our suggested framework should address these difficulties by including methods for capacity building, infrastructure development, and sustainable finance sources:

- **Resource Requirements**: Implementing and maintaining a comprehensive cybersecurity programme requires significant resources, including personnel, technology, and budget.
  - **Mitigation**: Identify and give priority to critical assets and systems that are fundamental to the functioning of the infrastructure. This will help to channel resources on the most important areas and ensure that they are protected.
- **Change Management**: Integrating new security measures may require changes to existing processes and workflows, potentially encountering resistance from personnel.
  - **Mitigation**: Communicate the need for the cybersecurity programme to obtain buy-in from stakeholders and employees.
- **Technical Expertise**: Implementing and managing an ISMS requires specialised technical knowledge and expertise.
  - **Mitigation**: Employees should be trained on cybersecurity best practices and ensure that they become familiar with the risks associated with cyber threats. This will help will everyone to work together to protect organisation’s critical infrastructure
- **Socio-technical Challenge**: (Olayemi, 2014) underlines the need of incorporating socio-cultural issues in cybersecurity solutions.
  - **Mitigation**: Our proposed framework should encompass steps to address the human element of cybersecurity, including public awareness campaigns, education programs, and strategies to counteract the cultural acceptability of certain cybercrimes.

CONCLUSION AND FUTURE WORKS

This study proposes an integrated cybersecurity framework for Nigeria's critical infrastructure. It blends ISO 27001 standards with key elements like threat intelligence, incident response, and ongoing monitoring. The framework tackles weak points in vital sectors such as oil and gas, telecommunications, power, and healthcare.

Nigeria's infrastructure faces unique challenges. Our approach considers these specific issues, offering tailored solutions. By combining proven standards with advanced practices, the framework aims to create a robust defence against complex cyber threats.

The framework's main goal is to keep essential services running smoothly. This is crucial for Nigeria's economic health and public safety. It is being designed it to adapt to new threats, ensuring long-term protection.

Its approach goes beyond simple compliance. It promotes a culture of active security across all critical sectors. This shift in mindset is essential for staying ahead of evolving cyber risks.

By implementing this framework, Nigeria can better safeguard its vital systems. This, in turn, supports national growth and stability. It's a practical step towards a more secure digital future for the country.

Future Works

1. Developing case studies: Applying and assessing the described framework in real life governmental contexts.
2. Studies may be directed towards the factors that lead to human mistakes and ways of moderating risks that are linked to such mistakes.

RECOMMENDATIONS

1. **Implementation of the Framework**: It is recommended that Nigerian government agencies and critical infrastructure operators adopt the proposed integrated cybersecurity framework. This adoption should include the establishment of robust incident response mechanisms and continuous improvement processes to adapt to evolving cyber threats.

2. **Capacity Building and Training**: Enhance the technical expertise of cybersecurity personnel through targeted training programs. This will ensure that staff are well-equipped to implement and manage the Information Security Management System (ISMS) and respond effectively to cyber incidents.

3. **Public-Private Partnerships**: Foster collaboration between government entities and private sector stakeholders to share threat intelligence and best practices. This collaboration can enhance the overall cybersecurity posture and facilitate a coordinated response to cyber threats.

4. **Regulatory and Policy Support**: Encourage policymakers to develop and enforce regulations that mandate the adoption of cybersecurity best practices across all critical infrastructure sectors. This regulatory support will ensure compliance and drive the implementation of necessary security measures.

5. **Continuous Research and Development**: Support ongoing research to explore emerging cybersecurity technologies and methodologies. This will help in adapting the framework to address new challenges and threats, ensuring its relevance and effectiveness in protecting critical infrastructure.

By implementing these recommendations, Nigeria can significantly enhance the resilience of its critical infrastructure against cyber threats, safeguarding national security and economic interests.

List of Figures

List of Tables

Declaration

- The authors have no relevant financial or non-financial interests to disclose.
- The authors have no competing interests to declare that are relevant to the content of this article.
- All authors certify that they have no affiliations with or involvement in any organisation or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.
- The authors have no financial or proprietary interests in any material discussed in this article.

REFERENCES

1. Anderson, E. (2021, November 11). How to comply in 2020 with the 5 functions of the NIST Cybersecurity Framework. Forescout. Retrieved December 21, 2023, from https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/.
2. Anderson, E. (2021, November 11). How to comply in 2020 with the 5 functions of the NIST Cybersecurity Framework. Foreshoot. Retrieved December 21, 2023, from https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/.
3. Barrett, M. P. (2020, January 27). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 | NIST. NIST. Retrieved December 30, 2023, from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
4. Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, [online], https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework (Accessed August 26, 2024)
5. Cross-Sector Cybersecurity Performance Goals | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency (CISA). Retrieved December 30, 2023, from https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
6. Charles, S. (2023, March 6). Manage endpoint compliance as code. Chef Blogs. https://www.chef.io/blog/manage-endpoint-compliance-as-code.
7. Daniel, S & Victor, S (2024). Emerging Trends in Cybersecurity For Critical Infrastructure Protection: A Comprehensive Review. Computer Science and IT Research Journal, March 2024. Retrieved August 26, 2024, from https://www.fepbl.com/index.php/csitrj/article/view/872/1073
8. DeLima, M. (2022, July 21). Ongoing Cyber Security Threats to Critical Infrastructure. Thales. Retrieved December 19, 2023, from https://cpl.thalesgroup.com/blog/identity-data-protection/ongoing-cyber-security-threats-to-critical-infrastructure.
9. How cyber-attacks exposed Nigeria's IT security vulnerability in 2023 - Daily Trust. (2023, December 28). Daily Trust. Retrieved August 26, 2024, from https://dailytrust.com/how-cyber-attacks-exposed-nigerias-it-security-vulnerability-in-2023/

10. Indusface weekly. (2023, July 27). The Importance of Vulnerability Assessment: Types and Methodologies. LinkedIn. Retrieved
11. December 24, 2023, from https://www.linkedin.com/pulse/importance-vulnerability-assessment-types-methodologies-indusface/
12. International Journal of Critical Infrastructure Protection | ScienceDirect.com by Elsevier. (n.d.). https://www.sciencedirect.com/journal/international-journal-of-critical-infrastructure-protection
13. International Organization for Standardization, Risk management – Principles and guidelines, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm.
14. International Organization for Standardization/International Electrotechnical Commission, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html.
15. International Telecommunication Union (ITU). (2018). Global Cybersecurity Index (GCI) 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
16. Ismaila, I., Adeleke, I., Anogie Uduimoh, A., & J. Tom, J. (2023). Design Framework of Cyber Security Solutions to Threats and Attacks on Critical Infrastructure of Electricity Power Systems of Nigeria Companies. International Journal of Computing, Intelligence and Security Research, 2(1), 17–23. Retrieved from https://ijcsir.fmsisndajournal.org.ng/index.php/new-ijcsir/article/view/21
17. *ISO - ISO 31000 — Risk management*. (2021, December 7). ISO. Retrieved September 20, 2024, from https://www.iso.org/iso-31000-risk-management.html
18. Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39, March 2011. https://doi.org/10.6028/NIST.SP.80039.
19. NIST (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. The National Institute of Standards and Technology (NIST). Accessed December 23, 2023, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
20. Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116-125.
21. Ogu, E. C., Ogu, C., & Oluoha, U. (2020). Cybersecurity Issues in Nigeria: Problems, Prospects, and Solutions. In Handbook of Research on Cyber Crime and Information Privacy (pp. 301-324). IGI Global.
22. OPSWAT, Inc. (2023, May 17). What is Critical Infrastructure Protection - OPSWAT. OPSWAT. https://www.opswat.com/critical-infrastructure-protection
23. OPSWAT, Inc. (2023b, December 4). About us - OPSWAT. OPSWAT. https://www.opswat.com/company/about.
24. Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology, 9(1), 120-143.
25. Paganini, P. (2017, December 2). Introduction to the NIST Cybersecurity Framework for a Landscape of Cyber Menaces. Security Affairs. Retrieved December 23, 2023, from https://securityaffairs.com/58163/laws-and-regulations/nist-cybersecurity-framework-2.html.
26. Serianu. (2017). Africa Cyber Security Report 2016. Retrieved from https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
27. U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003, May 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf.
28. Udotai, B. (2007). A Framework for Cybersecurity in Nigeria. (2007, November 29). ITU. Retrieved August 26, 2024, from https://www.itu.int/ITU-D/cyb/events/2007/praia/docs/udotai-nigeria-cybersecurity-framework-praia-nov-07.pdf
29. (2) (PDF) Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive review. (2024, August 1). ResearchGate. https://www.researchgate.net/publication/378858052_Emerging_Trends_in_Cybersecurity_for_Critical_Infrastructure_Protection_A_Comprehensive_Review/citations