International Journal of Scientific Research in Technology, Applied Sciences & Health Studies | **IJSRTASHS**
p-ISSN: *2579-1036* | ***e-ISSN:*** *2579-1044*
Volume 5, Number 1 October 2025

Cyber Risk Model on Judiciary System: A Study of Federal High Court Kaduna

[1]M. Ibrahim, [2]M. Isah & [3]Elizabeth Mallin
[1&3]Department of Cyber Security;
[2]Department of Intelligence and Security Studies,
Faculty of Military Science and Interdisciplinary Studies,
NDA (Kaduna)

Abstract

The study determined Cybersecurity threats pose significant challenges to the integrity and security on judicial systems worldwide. This study investigated cyber threat landscape faced by the Federal High Court Kaduna in Nigeria. The study employed the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 2.0 to conduct a comprehensive cyber threat assessment. The study introduced mixed methods, the applications of qualitative and quantitative methods have significantly improved the objectivity of the study. 250 questionnaires were distributed to various section in the judicial system Data collection methods included document reviews, semi-structured interviews with Federal High Court Kaduna personnel, and analysis of IT infrastructure. The assessment revealed concerning vulnerabilities within the Federal High Court's IT environment, including: limited cybersecurity awareness among staff as 79% demonstrated low awareness. The study findings highlighted the urgent need for the Federal High Court Kaduna to prioritize cybersecurity improvements. The research emphasizes the importance of enhancing cybersecurity awareness training, upgrading outdated IT infrastructure, implementing robust data security controls, and developing a formal incident response plan. The study recommended this could serve as a roadmap for the Federal High Court Kaduna and other courts within the Nigerian judiciary system to strengthen their overall cybersecurity posture and mitigate cyber threats.

Keywords: *Cybersecurity, Cyber threat and Judiciary system*

Article DOI: 10.48028/iiprds/ijsrtashs.v5.i1.06
Corresponding Author: *M. Ibrahim*

https://internationalpolicybrief.org/international-journal-of-scientific-research-in-technology-applied-science-health-studies-volume-5-number-1/

Background to the Study

Cybersecurity has become a critical issue in the modern world, with organizations increasingly relying on digital systems to store and process sensitive information. The judiciary system is no exception, as court records, case files, and other sensitive information are often stored digitally. This has led to an increased threat of cyber-attacks, which can have serious consequences for the integrity of the judicial process (Garrie, 2020). The Federal High Court Kaduna, as a critical component of the judiciary system in Nigeria, faces numerous cyber threats that demand attention and proactive measures to mitigate (KSJ, 2024). As the judiciary increasingly relies on digital infrastructure for case management, communication, and data storage, vulnerabilities to cyber threats have become more pronounced.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a widely recognized standard for assessing and managing cybersecurity threats. The CSF provides a common language and sets of practices for organizations to identify, protect, detect, respond, and recover from cyber threats (National Institute of Standards and Technology, 2024a). The CSF has been widely adopted by organizations in various sectors, including the judiciary system (National Institute of Standards and Technology, 2024b). By adopting the NIST CSF 2.0, the Federal High Court Kaduna can establish a structured approach to identify, protect against, detect, respond to, and recover from cyber threats.

This study uses the NIST CSF 2.0 to assess the cybersecurity posture of the Federal High Court Kaduna. The CSF 2.0 is an updated version of the framework, which includes new features such as improved scalability and flexibility, as well as enhanced support for supply chain threat management (Computer Security Division, 2016). The use of the CSF 2.0 in the judiciary system is particularly important, as courts often handle sensitive information and are vulnerable to cyber-attacks. In a recent study, it was found that over 50% of courts in the United States had experienced a cyber-attack in the past year (Ken, 2023). Therefore, it is essential for courts to have a robust cybersecurity framework in place to protect against these threats. The objective of this research is to improve cybersecurity resilience in the judicial system by undertaking a thorough examination of cyber threats, vulnerabilities, and mitigation techniques. Furthermore, by focusing on a specific case study, this study aims to provide actionable insights and recommendations that can be applied not only within the Federal High Court Kaduna but also extrapolated to inform cybersecurity practices in other judiciary systems facing similar challenges.

Statement of the Problem

The increasing integration of technology into the operations of the judiciary system, particularly within the Federal High Court Kaduna, has exposed it to numerous cybersecurity threats and challenges. Reid & Van Niekerk, (2014) explained that such challenges manifest in various forms, posing significant threats to the integrity, confidentiality, and availability of judicial information and services. One of the primary problems confronting the Federal High Court Kaduna is the lack of a comprehensive understanding of the specific cyber threats it faces. Without a thorough assessment of vulnerabilities and threats, the High Court is ill-equipped to implement effective cybersecurity measures to safeguard its digital infrastructure and sensitive data. Furthermore, the evolving nature of cyber threats presents a continuous challenge for the judiciary system. Kirwan & Power, (2013) poised that the malicious actors, including cybercriminals and state-sponsored hackers, constantly devise new techniques to exploit vulnerabilities and breach security defences. This dynamic threat landscape necessitates proactive measures and continuous monitoring to detect and mitigate emerging cyber threats effectively.

Another significant problem is the potential impact of cyber-attacks on the administration of justice. The disruption or compromise of judicial services due to cyber incidents can undermine public trust in the judiciary system and impede the fair and timely resolution of legal disputes (Ogah & Aliyu, 2020). Addressing these challenges requires a concerted effort to assess, understand, and mitigate cyber threats within the Federal High Court Kaduna. Whitman & Mattord, (2021) explains that by identifying specific vulnerabilities and threats like such faced by the judiciary system, stakeholders can develop targeted strategies to bolster cybersecurity defences and ensure the resilience of judicial operations in the face of cyber threats.

Literature Review/Theoretical Framework

This study explores existing body of research on cyber threat assessment methodologies and their application in relation to its application in the judicial system. A comprehensive understanding of existing frameworks and best practices are explained and studied for developing a tailored approach to cyber threat assessment within the judiciary system using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Cyber Threat

Courts face increasing cyber threats, from ransomware to advanced data theft schemes. we provide expert guidance and tailored solutions — including risk assessments and policy frameworks — to help safeguard court systems and sensitive data from sophisticated attacks. with decades of experience in court operations, case management systems, and technology infrastructure, we understand the unique cybersecurity and continuity challenges courts face. cyber threat assessment is a crucial component of cybersecurity for any organization, Including judicial systems. according to kure et al., (2018) cyber threat assessment involves a systematic process of identifying, analysing, and evaluating potential threats, vulnerabilities, and their impact on critical assets. this process allows decision-makers to prioritize threats, allocate resources for mitigation strategies, and ensure the confidentiality, integrity, and availability of sensitive judicial data.

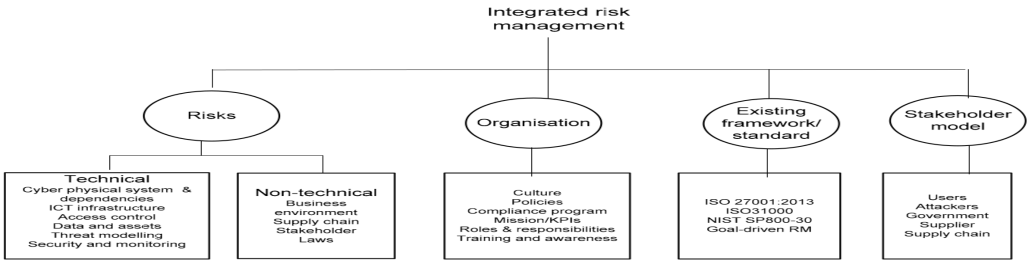


Figure 1: An integrated cyber threat management approach (Kure et al., 2018)

Threat assessment is a technical task to perform which has many challenges. Ruan, (2017) try to address the challenges involving measuring cyber threat by proposing novel threat units, BitMort (BM) and hekla, which are inspired by MicroMort (MM) for medical threat measure and Value-at-Threat (VaR) for market threat measure. Figure 2.1 shows an integrated threat management approach which covers both technical aspects such as ICT infrastructure, access control, data, assets etc. and non-technical aspects such as environment, laws, stakeholders, supply chain etc. Several established frameworks can guide cyber threat assessments. This section reviews four prominent frameworks to understand their strengths and how they are applied in the context of cyber threat assessment within the judicial system.

The ever-evolving landscape of cyber threats necessitates a paradigm shift in cybersecurity strategies. organizations grapple with safeguarding their digital assets from sophisticated attacks, traditional security measures are proving to be inadequate. In response to this escalating threat environment, the concept of integrated threat management has emerged as a pivotal approach to fortifying cybersecurity defenses. This comprehensive guide aims to unravel the intricacies of integrated threat management, empowering businesses to bolster their cybersecurity posture effectively.

Another significance of the above model is to defining integrated threat management and its relevance in cybersecurity. Integrated threat management can be defined as a comprehensive cybersecurity approach that integrates various security solutions and technologies to provide a cohesive defense against cyber threats. This proactive stance enables organizations to identify potential risks and vulnerabilities, mitigate attacks, and respond swiftly to security incidents. The relevance of integrated threat management lies in its ability to adapt to the dynamic threat landscape, offering a multifaceted defense strategy that encompasses preventive, detective, and corrective measures.

The Purpose of Integrated Threat Management for Cybersecurity

At its core, the purpose of integrated threat management revolves around fortifying the resilience of organizations against diverse cyber threats. By leveraging an integrated approach, organizations can streamline their cybersecurity operations, optimize resource utilization, and enhance their ability to thwart sophisticated attacks effectively. Additionally, integrated threat management aligns with the broader goal of fostering a cybersecurity posture that is proactive, adaptive, and aligned with the organization's risk tolerance and business objectives.

Understanding how Integrated Threat Management Works in Cybersecurity

Integrated threat management functions as a cohesive framework that unifies multiple security technologies and processes to create a synergistic defense mechanism. This approach involves the integration of threat intelligence, security analytics, incident response, and other cybersecurity capabilities into a unified ecosystem. From proactive threat detection to rapid incident response, integrated threat management equips organizations with the essential tools to combat a wide spectrum of cyber threats effectively.

NIST Cybersecurity Model

The NIST CSF 2.0 offers a classification of high-level cybersecurity outcomes that can be applied by organizations of all sizes and sectors to enhance their cybersecurity efforts. It has been updated to serve a wider audience beyond critical infrastructure sectors, providing flexibility for organizations to adapt it according to their specific needs (Computer Security Division, 2016). NIST (2024a) explains this framework provides a flexible and threat-based approach to cybersecurity, consisting of five core functions: Identify, Protect, Detect, Respond, and Recover. These functions help organizations to understand their cybersecurity posture, prioritize investments, and improve their overall resilience to cyber threats.

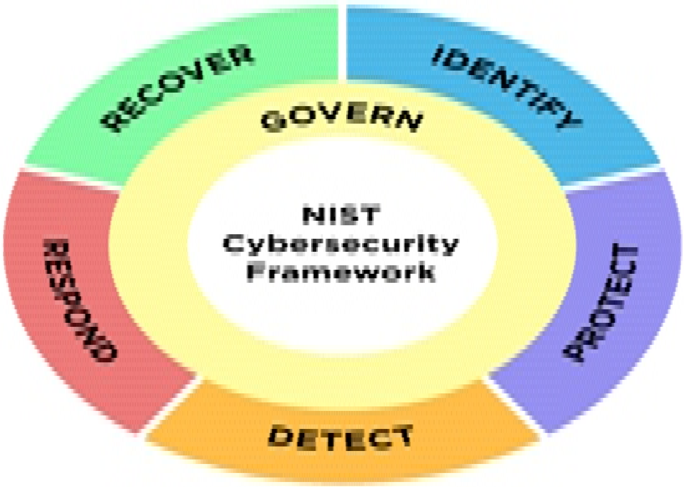


Figure 2: NIST CSF functions (NIST, 2024b)

Significance of NIST as one of the cybersecurity models could be examine as follows

i. Identify
ii. Protect
iii. Detect
iv. Respond
v. Re-cover

These five Functions were selected because they represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions.

Information Security System (ISO/IEC 27001:2013)

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly developed the ISO/IEC 27001 standard. It provides a comprehensive set of requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) (Humphreys, 2016). While not solely focused on cyber threats, ISO/IEC 27001 offers a structured approach to managing information security threats, which encompasses cybersecurity threats. It provides a systematic approach to managing sensitive information and ensuring its confidentiality, integrity, and availability (Longras et al., 2018). ISO/IEC 27001:2013 includes a comprehensive threat assessment process, enabling organizations to identify and mitigate information security threats effectively.

Center for Internet Security Controls

The Center for Internet Security (CIS) Controls are a prioritized set of configuration recommendations for hardening critical infrastructure against cyberattacks. These controls are developed by a community of cybersecurity professionals and continuously updated to address evolving threats (Amiruddin et al., 2021). According to Groš, (2021), CSI Controls consists of 20 prioritized controls and 171 sub-controls that provide actionable guidance for implementing essential cybersecurity measures. The CIS Controls cover various aspects of cybersecurity, including inventory and control of hardware assets, continuous vulnerability management, secure configuration for hardware and software, and data recovery capabilities (Bashofi & Salman, 2022).

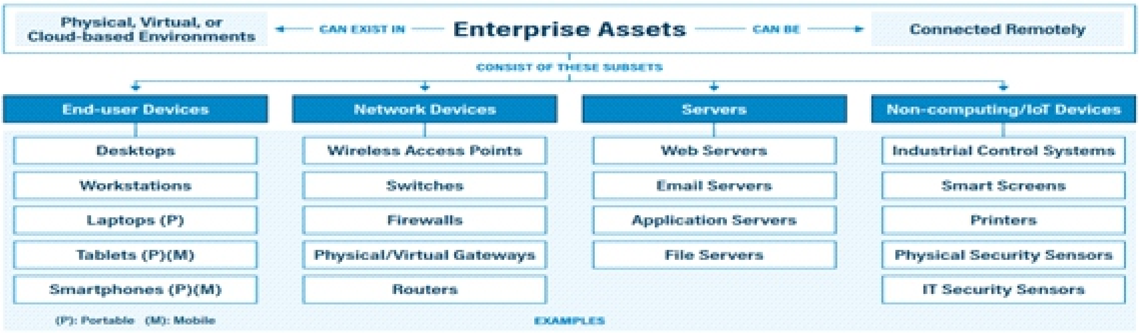


Figure 3: Enterprise assets, as defined in CIS Controls v8 (CIS, 2024)
Source: Functions of the above model

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure, physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate. Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to enterprises' networks. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web or email-based malware; and adversaries can leverage weak security configurations for traversing the network, once they are inside.

Factor Analysis of Information Threat

Factor Analysis of Information Threat (FAIR) is a threat quantification methodology that enables organizations to understand, analyse, and quantify information security threats in financial terms (Freund & Jones, 2014). FAIR provides a structured approach to threat assessment, focusing on factors such as threat event frequency, vulnerability, control effectiveness, and financial impact (Dreyling et al., 2021). Wang et al., (2020) explains that while FAIR can be a valuable tool for senior management to understand the financial implications of cyber threats, it may not be essential for all cyber threat assessments, particularly within the context of the judiciary system where financial loss might not be the primary concern. FAIR relies on expert estimates which are based on a specific type of Probability Distribution (PERT) and is made by qualified people who are trained in the estimation techniques (Freund & Jones, 2014). The final estimates are used in a Monte Carlo simulation to assess overall threat. Figure 4 shows a step flow of FAIR cyber threat analysis.

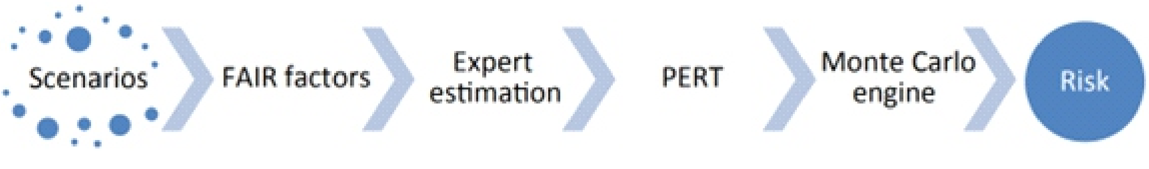


Figure 4: FAIR Cyber analysis steps (Freund & Jones, 2014)

FAIR is a framework for threat modeling and a standard methodology for applying Value at Risk (VaR) principles to cybersecurity and operational risk. It promotes a consistent and measurable approach to analysing and quantifying risk. FAIR approaches risk from a quantitative rather than a qualitative perspective. Traditional risk management scales that use rank or order, for example Red-Amber-Green, High-Medium-Low, or Rated 1-5, as ordinal data are qualitative in nature. FAIR provides a more precise and objective way to assess risk by focusing on numerical data, enabling better-informed decision making, and a clearer understanding of the potential financial impact.

NIST Cybersecurity Framework

There are various frameworks available to conduct cyber threat assessments and some of them major frameworks are explored in Section 2.2.2 of this study. This study utilises NIST CSF Version 2.0 as its theoretical foundation. The NIST CSF is a voluntary, flexible framework that provides a comprehensive approach to managing cybersecurity threat. It outlines core functions critical for any organization to govern, identify, protect, detect, respond to, and recover from cyberattacks. This study uses the NIST CSF 2.0 structured and standardized approach to cyber threat assessment for the Federal High Court Kaduna. The framework's focus on core functions aligns well with the need to establish a robust cybersecurity posture for the judiciary system, safeguarding sensitive data and ensuring the continued operation of critical judicial processes. This section of the study explores the theoretical aspects of the NIST Cybersecurity Framework.

Historical of NIST Cybersecurity Framework

The NIST CSF emerged in response to the growing need for a standardized approach to managing cybersecurity threat. In 2013, following a series of high-profile cyberattacks on critical infrastructure, President Obama issued Executive Order 13636 which called for the development of a framework to help businesses and organizations improve their cybersecurity posture (National Institute of Standards and Technology, 2018a). NIST engaged with stakeholders from across industry, government, and academia to develop the framework, drawing upon existing standards, guidelines, and best practices.

After a period of extensive public comment and collaboration, NIST released the first version of the Cybersecurity Framework in February 2014 (National Institute of Standards and Technology, 2014). The framework has undergone revisions since its initial release, with Version 1.1 published in 2018 was released with updates on self-assessing cybersecurity threat, authentication, identity, and vulnerability disclosure (National Institute of Standards and Technology, 2018b). The latest version, NIST CSF Version 2.0 of the framework, published in February 2024, represents a significant update that incorporates new best practices and methodologies tailored for the modern digital ecosystem with the addition of “Govern” core function (National Institute of Standards and Technology, 2024a).

Objectives and Scope of NIST Cybersecurity Framework

The primary objective of the NIST Cybersecurity Framework is to provide organizations with a common language and framework for managing cybersecurity threats effectively. Other objectives include the following (National Institute of Standards and Technology, 2024a):

i. **Facilitate Threat Management:** The framework enables organizations to identify, assess, and prioritize cybersecurity threats based on their business objectives, threat landscape, and organizational context.

ii. **Improve Cyber Resilience:** By adopting the framework's recommended practices, organizations can enhance their ability to prevent, detect, respond to, and recover from cybersecurity incidents and breaches.

iii. **Enhance Communication and Collaboration**: The framework fosters communication and collaboration among stakeholders within and across organizations, including executives, IT professionals, threat managers, and cybersecurity experts.

iv. **Align with Industry Standards and Best Practices:** The framework aligns with existing cybersecurity standards, guidelines, and best practices, allowing organizations to leverage and integrate their existing cybersecurity investments and efforts.

The scope of the NIST Cybersecurity Framework is broad, encompassing organizations of all sizes, sectors, and industries. It is applicable to both public and private sector entities, including critical infrastructure sectors such as energy, finance, healthcare, and government (National Institute of Standards and Technology, 2018a). The framework is designed to be scalable, adaptable, and customizable to meet the unique needs and requirements of diverse organizations.

Core Components of NIST CSF

The NIST CSF is structured around a hierarchical framework with three core components: Functions, Categories, and Subcategories. These components work together to provide a comprehensive approach to managing cybersecurity threat. Figure 5 shows the structure of the NIST CSF 2.0 core and the relationship between the core.

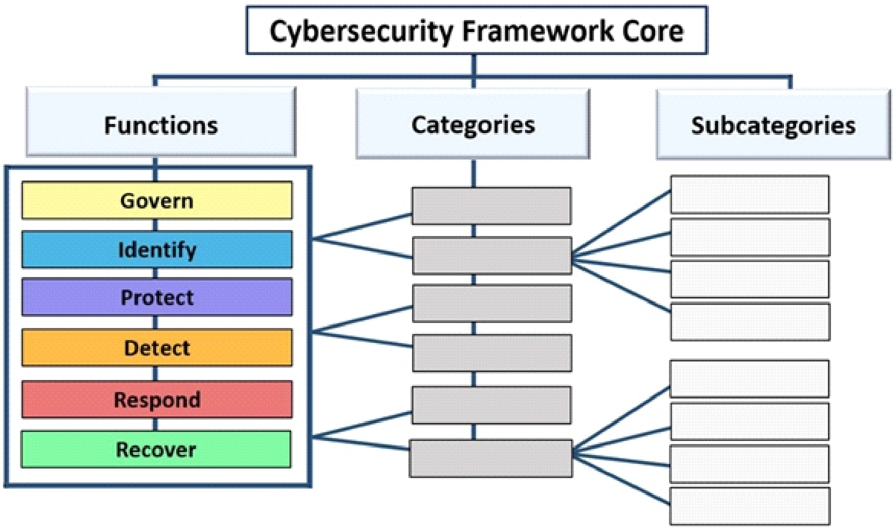


Figure 5: NIST CSF core structure (NIST, 2024b)

The NIST CSF defines six core functions that represent the high-level activities critical for any organization's cybersecurity posture:

i. **Govern:** This function focuses on understanding the organization's cybersecurity threat management strategy, expectations, and policies.
ii. **Identify:** This function focuses on understanding the organization's systems, assets, data, and the potential threats they face.
iii. **Protect:** This function involves developing and implementing safeguards to protect critical assets from cyberattacks.
iv. **Detect:** This function emphasizes the ability to identify and report cybersecurity events in a timely manner.
v. **Respond:** This function outlines the steps necessary to contain, mitigate, and recover from a cyberattack.
vi. **Recover:** This function focuses on restoring capabilities and services after a cybersecurity incident.

These core functions provide a high-level roadmap for organizations to build a robust cybersecurity program. Each core function is further broken down into Categories. Categories represent the key areas of focus within each function. For example, the Identify function includes categories such as Asset Management, Business Environment, and System Security Procedures. There is a total of 22 Categories across the six core functions (National Institute of Standards and Technology, 2024a). Each Category is further divided into Subcategories. Subcategories provide specific examples of the activities and considerations within each Category. There are hundreds of Subcategories within the NIST CSF, offering a granular level of detail for organizations to tailor their cybersecurity practices (National Institute of Standards and Technology, 2024a). Table 1 shows the core functions and categories of NIST CSF 2.0 and their identifiers. A full list of all functions, categories and sub-categories is contained in Appendix A.

NIST CSF Profiles

The NIST CSF Profiles allow organizations to customize the framework to their specific needs and threat tolerance. A profile defines the desired state of cybersecurity maturity for an organization, specifying which functions, categories, and subcategories are relevant and how they should be implemented and prioritized (National Institute of Standards and Technology, 2024a). NIST CSF 2.0 provides some sample Profiles, but organizations can also develop their own customized Profiles. Figure 6 shows proposed steps by National Institute of Standards and Technology, (2024b) for organisations to follow when creating and using the NIST CSF Figure 6**.**

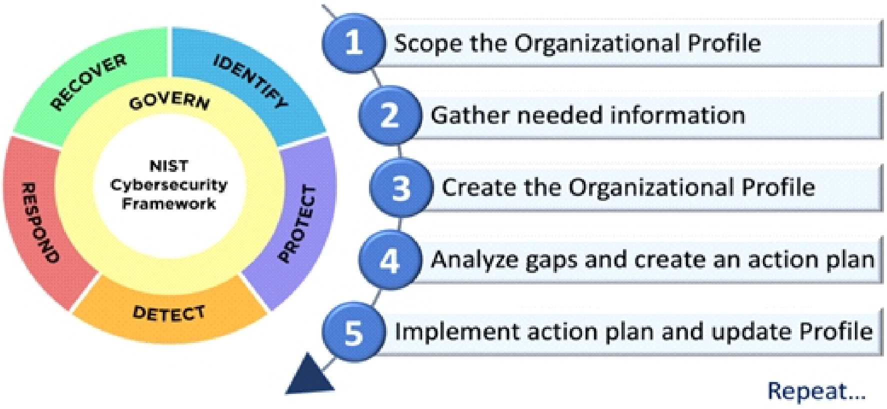

RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT
1 Scope the Organizational Profile
2 Gather needed information
3 Create the Organizational Profile
4 Analyze gaps and create an action plan
5 Implement action plan and update Profile
Repeat...

Figure 6: NIST Proposed steps for creating and using a CSF Organizational Profile (NIST, 2024b)

NIST CSF Tiers

The NIST CSF Tiers provide a way for organizations to assess their current cybersecurity maturity level and define their desired level of cybersecurity threat management. The framework defines four tiers of cybersecurity maturity, ranging from Partial (Tier 1) to Adaptive (Tier 4), shown in Figure 7, based on the organization's threat management practices, integration of cybersecurity into business processes, and responsiveness to changing cybersecurity threats and challenges. Appendix B contains a notional illustration of the CSF Tiers.

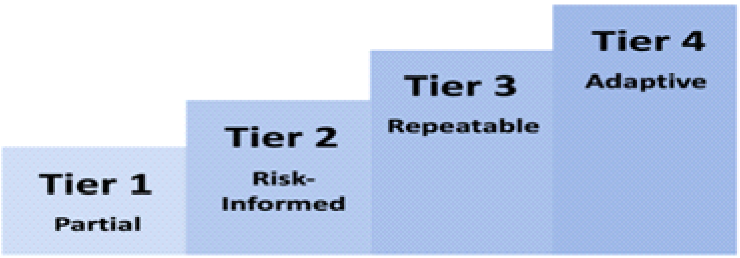


Figure 7: NIST CSF Tiers for cybersecurity threat governance and management (NIST, 2024b)

i. **Partial:** This Tier indicates that an organization has some cybersecurity practices in place but may lack a comprehensive program.
ii. Threat-Informed: This Tier suggests that the organization considers cyber threats when making decisions but may not have a fully documented program.
iii. **Repeatable:** This Tier signifies that the organization has a documented cybersecurity program and can consistently implement its controls.
iv. **Adaptive:** This Tier represents the most mature level, where the organization continuously improves its cybersecurity program based on lessons learned and evolving threats,

Empirical Related

Senécal & Benyekhlef, (2009) made a comprehensive analysis of the legal threats associated with the implementation of cyberjustice, focusing on the transition from traditional paper-based legal systems to electronic ones. The study outlines a method for assessing legal threats by examining the impact of information technology on the justice system's basic tenets, such as constitutional and legal requirements, values, and principles. The major findings suggest that while cyberjustice systems offer significant potential for improving access to justice, they also pose threats to privacy, equality of arms, and public trust in the legal process. The limitations of the study include its preliminary nature and the need for a more integrated approach that considers the broader cultural, economic, and sociological impacts of cyberjustice. Recommendations include the development of a comprehensive theory for assessing legal threats, multidisciplinary research to understand the full implications of cyberjustice, and careful consideration of the digital divide in access to justice. The study emphasizes the importance of understanding the functions of legal rituals and formalities in the new electronic environment to ensure continuity with traditional justice processes.

Gaps from the Relevant Literature

The literature review on cyber threat assessment in the judiciary system reveals several key insights and contributions from existing studies. However, despite the wealth of research in this area, there are notable gaps that warrant further investigation:

Limited Focus on Specific Judicial Systems: While studies such as those by Senécal & Benyekhlef (2009) and Hamin et al. (2012) provide valuable insights into the legal threats and security challenges associated with the adoption of information and communication technology (ICT) in judicial systems, they primarily focus on specific contexts such as cyberjustice implementation in Canada and ICT adoption by Malaysian High Courts. There is a need for research that examines cyber threat assessment frameworks and practices within the context of other judicial systems, such as the Federal High Court Kaduna, to identify unique challenges and develop tailored strategies for managing cybersecurity threats effectively.

Gap in Application of Frameworks to Specific Contexts: While studies like Almuhammadi & Alsaleh (2017) and Amiruddin et al. (2021) provide insights into the application of frameworks such as the NIST Cybersecurity Framework (CSF) to information security management, there is a lack of research that specifically examines the application of these frameworks to the unique operational environment of judicial systems. Given the sensitive nature of legal data and the critical role of the judiciary in upholding justice and due process, there is a need for research that evaluates the effectiveness of existing cybersecurity frameworks in mitigating threats within the judiciary system.

Methodology

This study presents a detailed explanation of the methodology adopted for conducting a cyber threat assessment within the Federal High Court Kaduna, contextualized within the

NIST Cybersecurity Framework (CSF) 2.0. In line with best practices in cybersecurity research and national cyber governance principles, this methodology integrates qualitative and quantitative techniques to provide a robust and realistic portrayal of cyber risk posture. By employing a structured and replicable research approach, the study ensures its findings are academically rigorous and practically relevant. The application of the NIST CSF 2.0 serves to anchor the analysis within a globally recognized cybersecurity assessment standard. This chapter also articulates the rationale for choosing a case study strategy and outlines the step-by-step procedures used in designing, collecting, and analysing the data necessary to address the study's research questions. This study outlines the research methodology employed in this case study to assess cyber threats within the Federal High Court Kaduna using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 2.0...

Research Design

The research design adopted for this study is a mixed-method study, which allows for a holistic exploration of the cyber threat environment in the Federal High Court Kaduna. A case study design is particularly useful in cybersecurity research as it facilitates a detailed contextual analysis of a specific organization or system, especially where phenomena under study are complex, dynamic, and context-dependent (Yin, 2018). The mixed-methods approach integrates qualitative insights with quantitative data, enhancing the validity of the findings through triangulation. Qualitative methods such as interviews, document reviews, and observations provide depth and nuance, while quantitative data such as statistics from security logs and surveys provide generalizability and scale. This design is consistent with prior studies on cybersecurity practices in judicial and public institutions, offering a rich account of organizational vulnerabilities, security culture, and strategic readiness.

Results, Analysis and Discussions

This study presents the findings from the study on cyber threat assessment practices within the Federal High Court Kaduna using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 2.0 framework. It details the key findings obtained through the various data collection methods employed in the case study. The chapter then analyses the findings, interpreting them in the context of existing research on cyber threat assessment in the judiciary system. Finally, the chapter discusses the implications of the findings, highlighting their significance for improving cyber threat assessment practices within the Federal High Court Kaduna and potentially for the broader judiciary system.

Cyber Threat Assessment Findings

The findings from the cyber threat assessment of the Federal High Court Kaduna conducted are presented in this section. The findings are categorized into two main sections: General Cyber Threat Landscape, and Judiciary-Specific Cyber Threats.: The General Cyber Threat Landscape section outlines the overall cyber threat landscape at the Federal High Court Kaduna, identifying common vulnerabilities and potential threats. The Judiciary-Specific

Cyber Threats section on the other hand focuses on cyber threats specific to the judiciary system within the Federal High Court Kaduna, considering the unique data types, legal environment, and operational processes.

General Cyber Threat Landscape

The application of the NIST CSF framework to the Federal High Court Kaduna revealed several key findings regarding the general cyber threat landscape:

i. Limited Cybersecurity Awareness: Interviews with Federal High Court Kaduna personnel revealed a lack of widespread awareness regarding cyber threats and best practices for cybersecurity hygiene. This highlights the need for increased training and education programs to improve overall cybersecurity awareness among staff.

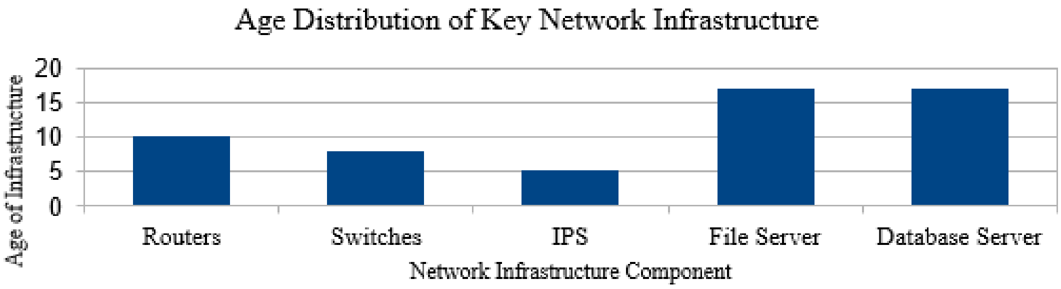
Table 1: Staff Cybersecurity awareness Levels

Category	Description	Percentage of Respondents
High Awareness	Understands common cyber threats and can identify suspicious activity.	4.7%
Moderate Awareness	Somewhat familiar with cyber threats but may lack knowledge of best practices.	16.4%
Low Awareness	Limited understanding of cyber threats and vulnerabilities.	78.9%

Source: Field, work 2025

ii. Outdated IT Infrastructure: Document reviews and observations indicates that some aspects of the Federal High Court's IT infrastructure may be outdated or lack proper security configurations. This can create vulnerabilities that cyber attackers can exploit.

Figure 8.



11: Age distribution of key network infrastructure components

Source: Field work, 2025

The graphs presented in Figure 1, Figure 2, and Figure 3 visually represent the age of critical IT infrastructure components (e.g., servers, network devices) at the Federal High Court Kaduna. These graphs highlight that server, recorders, public address system, and printer infrastructures are over 10 years old and considered outdated which pose security threats.

iii. Data Security Concerns: Analysis of IT policies and procedures reveal weaknesses in data security controls, including inadequate access control mechanisms or data encryption practices. This raises concerns about the confidentiality and integrity of sensitive judicial data. Table 2 shows data based on the study findings regarding the implementation status of some data security controls within the Federal High Court Kaduna.

Table 2: Data Security control Implementation Status

Control	Description	Implementation Status
Access Control	User access to data is restricted based on the principle of least privilege.	Partially Implemented
Data Encryption	Sensitive data is encrypted at rest and in transit.	Not Implemented
Server Access	Staff access to physical infrastructure in the server room.	Implemented

Source: Field, work 2025

iv. Incident Response Planning Gaps: Document reviews identify the lack of formal incident response plan and inadequate procedures for detecting, responding to, and recovering from cyberattacks. This can lead to delays and confusion in the event of a security breach.

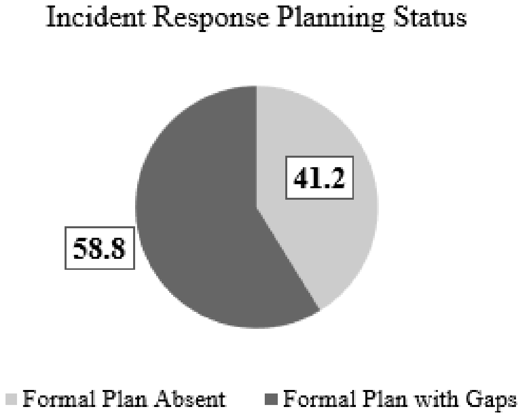


Figure 9.

The pie chart presented in Figure 9 visually represent the presence field work, 2025 formal incident response plan at the Federal High Court Kaduna. The chart shows that there are no plans for response in case of some cybercrime incidents (such as Denial of Service and data breach attacks) and there is a low level of preparedness if a plan exists (e.g., documented procedures, trained personnel).

Judiciary-Specific Cyber Threats

The study also identified cyber threats specific to the judiciary system within the Federal High Court Kaduna. Qualitative analysis was applied to this study to identify some major cyber threats specific to the Federal High Court Kaduna for which are presented in Table 3.

Table 3: Cyber threats specific to Federal High Court Kaduna

Cyber Threat	**Description**
Insider Threat	Internal threats from disgruntled employees or inadvertent actions
Data Breaches	Unauthorized access and disclosure of sensitive judicial data
Data Manipulation or Eavesdropping	Manipulate or eavesdrop on electronic court filings or communications, jeopardizing the integrity of the judicial process.
Denial-of-Service (DoS)	Disrupting critical judicial services and public access to justice.
Malware Attacks	Proliferation of malware compromising the integrity of court systems
Phishing	Targeted emails leading to unauthorized access or data theft
Third-party Threat	Threats associated with external vendors and service providers

Source: Field, work 2025

Threat Prioritization

Based on the identified cyber threats, a threat prioritization was conducted using the NIST CSF 2.0 threat assessment explained in section 3.7 of this study. This threat assessment considers factors such as the likelihood of a threat occurring, the potential impact on the Federal High Court's operations and data, and the existing controls in place. The prioritized list of cyber threats is presented in Table 4 and used to guide the development of recommendations for improving the Federal High Court's cyber threat assessment practices and overall cybersecurity posture.

Table 4: Prioritised Cyber threats specific to Federal High Court Kaduna

Cyber Threat	**Likelihood**	**Potential Impact**
Insider Threat	Moderate	Moderate
Data Breaches	High	Very High
Data Manipulation or Eavesdropping	Moderate	High
Denial-of-Service (DoS)	High	High
Malware Attacks	High	Very High
Phishing	Very High	High
Third -party Threat	Low	Moderate

Source: Field, work 2025

Organisational Evaluation using NIST CSF

The study made a full NIST CSF 2.0 assessment of the Federal High Court Kaduna and the analysis of results provides insights the NIST CSF Organizational Profile and Tier of the Federal High Court Kaduna.

Organisation Tier Evaluation

The NIST CSF framework categorizes organizations into four tiers based on their cybersecurity maturity as explained in Section 2.3.5 of this study. These tiers range from Tier 1 (Partial) to Tier 4 (Adaptive). Analysis of Federal High Court Kaduna Tier and implications are as follows:

i. **Limited Cybersecurity Awareness:** The low cybersecurity awareness among staff suggests a lack of formal security awareness programs, placing the Federal High Court Kaduna on the lower end of the maturity spectrum (Tier 1).

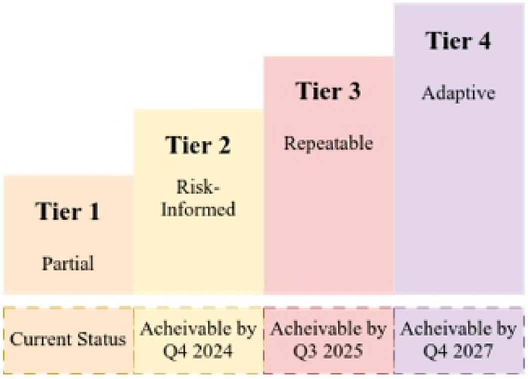
ii. **Outdated IT Infrastructure:** Outdated IT equipment indicates a reactive approach to cybersecurity, placing the Federal High Court Kaduna in Tier 2.

iii. **Data Security Concerns:** Weaknesses in data security controls suggest a need for improvement in securing sensitive data, potentially indicating Tier 2 or below.

iv. **Incident Response Planning Gaps:** The absence of a formal incident response plan is a significant gap, suggesting a Tier 1 maturity level.

Overall, based on the analysis, the Federal High Court's current cybersecurity posture falls within Tier 1 of the NIST CSF 2.0 framework. This indicates a need for significant improvement in various areas to achieve a more mature and robust cybersecurity posture. Figure 10 shows the current Tier of the Federal High Court Kaduna cyber security posture according to the NIST CSF 2.0 and the estimated timeline for improvement if the recommendations of this study are implemented.

Figure 10: Organisation CSF Tiers for cybersecurity threat governance and management



Source: Field work, 2025

Policy Implications

The cyber threat assessment findings presented in this chapter highlight the need for comprehensive cybersecurity policies and procedures within the Federal High Court Kaduna. Discussion in this section considers the legal and regulatory frameworks governing cybersecurity in the judiciary system. The Federal High Court Kaduna can create a strong cybersecurity policy framework that safeguards its information, reduces cyber threats, and promotes a more secure judicial environment by putting these recommendations into practice and abiding by pertinent legislative frameworks.

Recommendations for Policy Development

Based on the analysis from this study, the following recommendations are proposed for developing Federal High Court Kaduna cybersecurity policies:

i. **Develop a comprehensive Information Security Policy (ISP):** This overarching policy should define the Federal High Court's overall approach to cybersecurity, outlining its commitment to data security, user responsibilities, and acceptable use of IT resources.

ii. **Implement an Acceptable Use Policy (AUP):** An AUP should clearly define acceptable and unacceptable uses of IT systems and resources by staff and authorized users. This policy should address issues such as personal device usage, data transfer procedures, and password management.

iii. **Establish a Data Security Policy:** This policy should outline specific measures for protecting sensitive judicial data. It should address data classification, access control, encryption practices, data disposal procedures, and data breach notification protocols.

iv. **Develop an Incident Response Policy:** As mentioned earlier, a formal incident response plan outlined in a policy document is crucial. This policy should detail procedures for detecting, investigating, containing, eradicating, and recovering from cyberattacks.

Legal and Regulatory Considerations

When developing cybersecurity policies, the Federal High Court Kaduna needs to consider the legal and regulatory frameworks governing data privacy and cybersecurity within Nigeria's judiciary system. Relevant legislation, such as the Nigerian Data Protection Regulation (NDPR) of 2019, outlines specific requirements for data security and breach notification. These legal requirements should be incorporated into the Federal High Court's cybersecurity policies to ensure compliance.

Collaboration with relevant government agencies and judicial bodies can be instrumental in developing effective cybersecurity policies. Sharing best practices and learning from the experiences of other courts can inform the Federal High Court's policy development process. Cybersecurity threats and technologies are constantly evolving. Therefore, the Federal High Court's cybersecurity policies should be regularly reviewed and updated to reflect the changing landscape. Regular threat assessments, as recommended in Section 4.4, can inform these policy updates and ensure they remain relevant and effective.

Chapter Conclusion

In conclusion, this chapter has provided a comprehensive analysis of the cyber threat assessment findings at the Federal High Court Kaduna, conducted using the NIST CSF 2.0. The examination of the general cyber threat landscape and judiciary-specific cyber threats has revealed significant vulnerabilities and challenges within the judiciary system's cybersecurity posture. The findings underscore the critical importance of enhancing cybersecurity measures to safeguard judicial operations, protect sensitive data, and maintain public trust in the integrity of the judiciary system. Key insights from the analysis include the need for: improved cybersecurity awareness among court personnel to recognize and mitigate cyber threats effectively, modernization and fortification of IT infrastructure to address vulnerabilities and ensure robust security configurations, strengthened data security controls, policy updates and development of comprehensive cybersecurity policies and procedures tailored to the judiciary system's unique needs and challenges, compliance with legal and regulatory frameworks governing cybersecurity and data protection within the judiciary system. These insights have significant implications for enhancing cybersecurity resilience and threat management practices in the judiciary system, ultimately safeguarding judicial processes, protecting sensitive information, and upholding public confidence in the administration of justice.

Recommendations

Building upon the findings and conclusions from this study, the following recommendations are proposed for the Federal High Court Kaduna and the broader Nigerian judiciary system:
Recommendation for the Federal High Court Kaduna:

1. There is need for Critical Security Controls for Effective Cyber Defense, from the Center for Internet Security (CIS Controls), are priority actions for defense against pervasive cyber threats, i.e., those that easily spread or infiltrate computer systems. They are best cybersecurity practices that help protect organizations from the most common.

2. The federal and the state levels should ensure selection of the CIS Controls framework was based on various decisive factors. Initially, it is notable that CIS claims to adopt the Pareto principle by maximizing efficiency by implementing the most effective and relevant controls, thus avoiding a proliferation of potentially unnecessary measures.
3. Develop and implement comprehensive cybersecurity awareness training programs to equip staff with the knowledge and skills to identify and mitigate cyber threats. Focus on improving awareness from the current 79% with low awareness to a significantly higher percentage demonstrating a strong understanding of cybersecurity best practices.

Recommendation for the Nigerian Judiciary System:

i. This method is to allows organizations particularly, judicial system to seek the highest level of security while avoiding an extensive number of controls, which could overload management and compromise security effectiveness.

ii. There should be partnerships between the National Cybersecurity Strategy and the Judiciary (ENSECPJ) employs version 7 of the CIS controls to protect critical infrastructures and manage identities and access control

iii. To presents some examples of proposed complementary controls. The complete list of all additional controls for each of the judicial unit, and risk available.

References

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for Nist cyber security framework. *International Conference on Industrial Technology*. https://doi.org/10.5121/CSIT.2017.70305

Amiruddin, A., Afiansyah, H. G., & Nugroho, H. A. (2021). Cyber-threat management planning using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS, 19–24. https://doi.org/10.1109/ICIMCIS53775.2021.9699337

Bashofi, I., & Salman, M. (2022). Cybersecurity maturity assessment design using NISTCSF, CIS Controls v8 and ISO/IEC 27002. *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, 58–62. https://doi.org/10.1109/CyberneticsCom55287.2022.9865640

CIS. (2024). *CIS Controls Version 8*. CIS. https://www.cisecurity.org/controls/v8/

Computer Security Division, I. T. L. (2016). *CSF Filters—Cybersecurity Framework | CSRC | CSRC*. CSRC | NIST. https://csrc.nist.gov/projects/cybersecurity-framework/filters

Dreyling, R., Jackson, E., & Pappel, I. (2021). *Cyber security threat analysis for a virtual assistant G2C digital service using fair model.* 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG), 33–40