Cybersecurity Readiness of Ministries, Departments, and Agencies in Nigeria: A Quantitative Assessment Using CRMM Framework

Aimola Amos Ayodele
Department of Computer Science,
Federal College of Education, Okene, Kogi State, Nigeria
Email: aimola4jesus@yahoo.com
DOI: 10.56201/wjimt.v9.no6.2025.pg112.120

Abstract
The increasing sophistication of cyber threats poses a significant risk to government digital infrastructure. This study critically assesses the cybersecurity readiness of Ministries, Departments, and Agencies (MDAs) in Nigeria using the Cybersecurity Resilience Maturity Measurement (CRMM) framework. Data from 20 ICT-dependent MDAs were analyzed through a computational model and Python programming. The findings revealed that only four MDAs exhibited very high readiness, six had high readiness, another six showed low-to-medium readiness, and four MDAs demonstrated very low cybersecurity preparedness. The research underscores critical gaps in cybersecurity infrastructure and recommends strengthening cyber policies, training personnel, and enforcing national cyber laws to build resilience against growing cyber threats.

Keywords: *Cybersecurity, Critical Infrastructure, MDAs, Nigeria, Readiness Assessment, Cyber Threats*

Introduction

The internet's role in governance, commerce, and communication has led to a digitally dependent society vulnerable to cyberattacks. As organizations increasingly adopt ICT systems, the risk of cybercrime escalates. Government agencies, custodians of sensitive data and national operations are prime targets. In Nigeria, repeated cyberattacks on MDAs highlight the urgent need to assess and enhance cybersecurity readiness. According to Lucas (2017) the interconnected society is exposed to risks created by the inherent vulnerabilities and threats that daily seek to exploit the cyber resources of organisations to the detriment of the resource owners. Kott et al (2015) noted that cyber threats will be one of the main factors that will ascertain definitely if a war will be won or lost in warfare.

According to Mbanaso (2018) the safeguarding of information and property from theft, corruption, or natural disaster and making them to remain accessible and useful to its intended users is the major objective of cybersecurity. This simply means the confidentiality, integrity and availability, authenticity, non-repudiation and trust of information infrastructure and resources. All these can be achieved by (i) allowing only the authorized users to gain access (ii) encrypting all information to be sent (iii) routinely checking for new vulnerabilities (iv) using protected software and (v) creating disaster recovery plan in case of any disaster. This study evaluates the preparedness of Nigerian MDAs in facing cyber threats and their capability to mitigate such risks using a structured quantitative approach. Just as human immune system defends and fights infections and other forms of attacks from finding its way to the body, cyber systems should also be enforced to fight every

form of threats and attacks and be able to recover from such attacks immediately (Linkov *etal.* 2014). Marvin (2017) believes that there are two things that are true about cybersecurity in general. Firstly, no matter the security measures put in place, attackers will always attempt to hack our computers to steal and carry out their nefarious activities. Secondly, our system will always be vulnerable to various forms of attacks from cybercriminals.

Despite policies promoting ICT adoption in Nigerian public institutions, cybersecurity breaches persist. Currently, there is no standardized framework or model in place to evaluate the cybersecurity readiness of MDAs. This study addresses this gap by developing and testing a cybersecurity readiness model to assess and rank MDAs based on their ability to anticipate, prevent, and respond to cyber threats. In carrying out the study, the following questions were formulated:

i. What is the current state of cybersecurity readiness of MDAs?
ii. What cybersecurity control measures are in place at the MDAs?
iii. How can cybersecurity readiness index of MDAs be ranked?

The aim of this work is to assess the cybersecurity readiness of Ministries, Departments and Agencies (MDAs) using cybersecurity controls to gauge their preparedness to wade-off cyberattacks. To achieve this aim, the following specific objectives will guide the work:

i. Identify cybersecurity control metrics and indicators applicable to MDAs.
ii. Develop a computational model using CRMM to measure cybersecurity readiness.
iii. Analyze readiness scores and rank MDAs accordingly.

Literature Review

Cybersecurity readiness involves proactive measures such as regular audits, vendor assessment, and incident response planning (Graham, 2021). Frameworks like NIST, MITRE, and GCI offer guidelines for assessing and enhancing resilience. These frameworks emphasize governance, risk identification, protection strategies, and recovery protocols. However, their practical application in developing economies requires contextual adaptation, particularly in ICT-dependent public institutions like Nigeria's MDAs.

Rehak et al, (2019) quoting Petit et al (2013) argued that the essence of cyber resilience is to reduce the probability of failure of cyber systems that underlie Critical Infrastructures (CIs) pre-event; reduce the impact of failure (during the active phase of the event) and reduce the time to recovery (post event). However, making organisations or nations resilient as one way of managing national cyber risks requires that the cybersecurity resilience maturity of the national assets be assessed to understand the level of resilience and the gaps that need to be filled for a more resilience national Critical Information Infrastructure (CII).

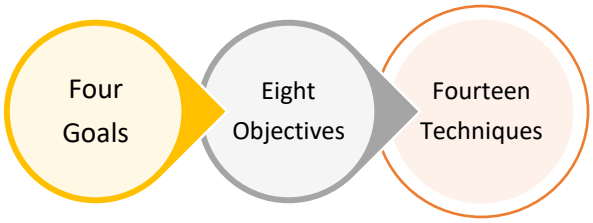
National Institute of Standards and Technology (NIST) Cybersecurity Framework (2018)

This Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

NIST Framework Core

MITRE Corporation Framework

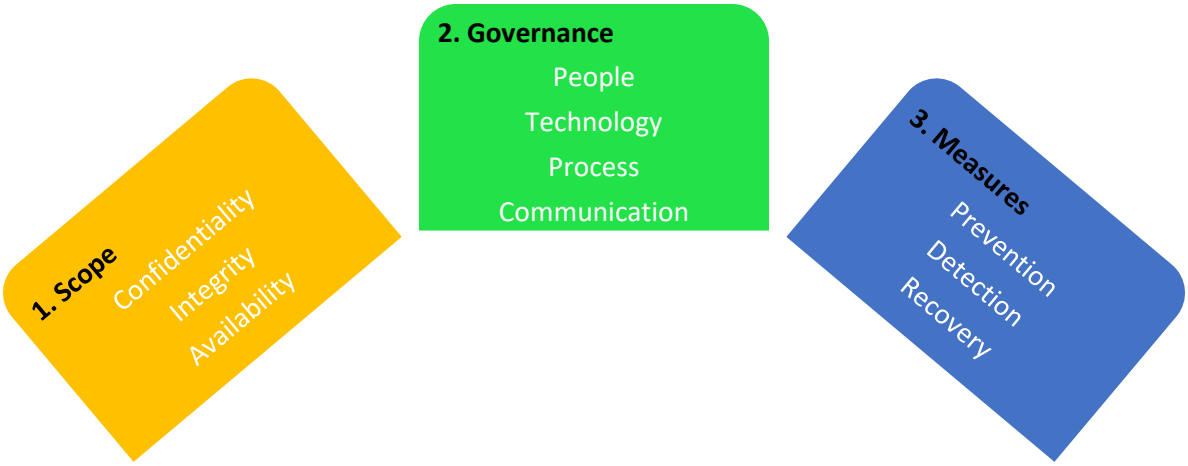
In an attempt to minimize the impact of the consequences of cyber breaches on cyber resources and enhance the management of cybersecurity risk, the MITRE corporation designed The MITRE Cyber Resiliency Engineering Framework (CREF), it consists of four goals (anticipate, withstand, recover and evolve), eight objectives (understand, prepare, prevent/avoid, continue, constrain, reconstitute, transform, re-architect) and fourteen techniques (adaptive response, analytical monitoring, deception, diversity, dynamic positioning, non-persistence, privilege restriction, segmentation/isolation, coordinated defense, dynamic representation, realignment, redundancy and substantiated integrity). It is argued here that an advanced cyber threat can simulate or take advantage of all other forms of adversity, and can establish and maintain a persistent and covert presence.



MITRE Cyber Resilience Framework

Committee on Payments and Market Infrastructures Cyber Resilience Framework (2012)

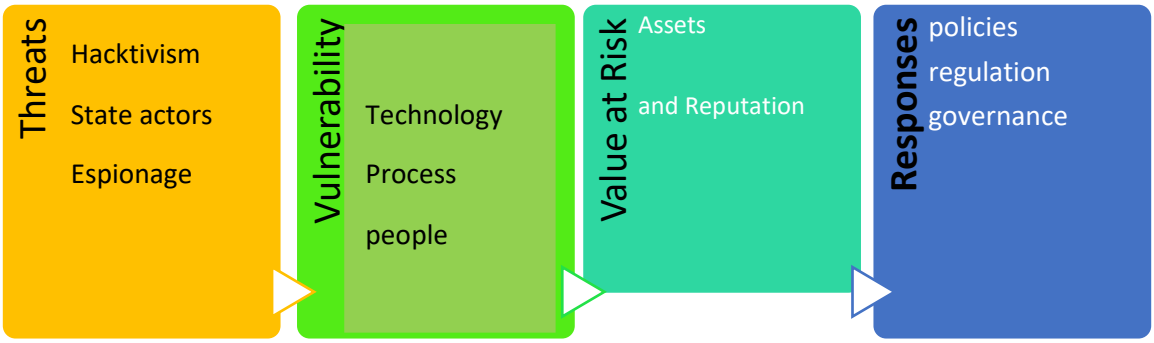
This framework, referred to as an Integrated Approach (IA) is a derivative of the (NIST Framework, 2014, WEF cyber resilience approach, 2015 and MITRE framework 2013). The goal is to ensure the survivability of Financial Markets Infrastructures - FMI operations, even if services have to be conducted in a degraded state. Survivable operations are designed to absorb the shock of an attack without systems breaking down totally. The framework covers three broad dimensions viz: scope – which addresses a number of scenarios that may result from a cyber-attack, covering confidentiality breach, an availability breach and an integrity breach (CIA breaches), cyber governance – touching on people, processes and communication and range of measures – which emphasis prevention, detection and recovery. This approach essentially combines conventional cybersecurity measures with cyber resilience to ensure the achievement of goals. This framework is summarized in the figure below.



Integrated Approach to Cyber Resilience

World Economic Forum Cyber Risk Framework

This is a cyber risk framework that is designed around four critical high-level components, namely: threats (existing threats), vulnerabilities, value-at-Risk and potential responses. The framework is intended to allow for deep understanding of the underling risk sources, by evaluating the key drivers referred to as components – and hence provides insights about how to improve the current risk exposures of organisations. The figure below is the presentation of the framework.



WEF Cyber Risk Framework

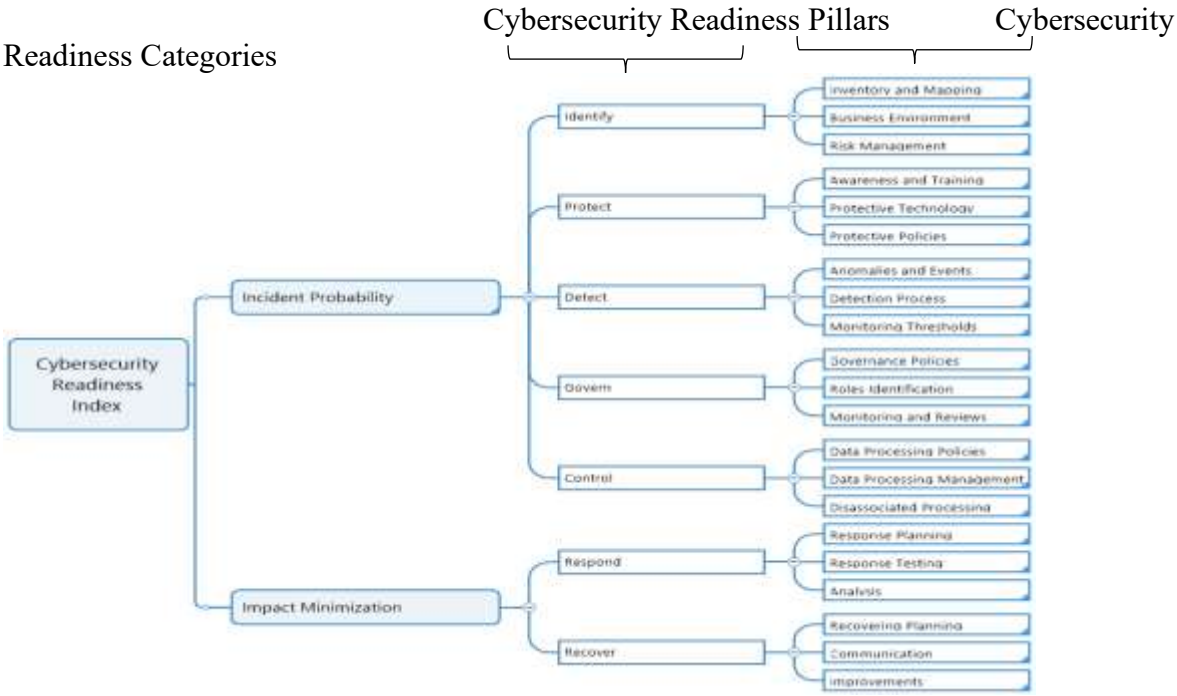
Global Cybersecurity Index (GCI) Conceptual Framework (ITU, 2014)

The GCI conceptual framework (ITU, 2014) is not necessarily a cyber risk management or cyber resilience framework in the real sense of it. It was designed to effectively measure each nation state's level of cybersecurity development, compare their cybersecurity capability levels and rank them so as to motivate nation states into arising to tackle the global challenge of cybersecurity, with the believe that this way, there will be global awareness and cooperation hence cyber resilience will be achieved. The following high level work areas were the focus of this framework: Legal measures, technical measures, organisational measures, capacity building and cooperation. Each of these five areas has a set of sub activities that define or measure preparedness. This framework is adopted to enhance data collection on the activities of the Nigerian government with respect to cyber risk management.

Methodology

A quantitative approach was adopted using CRMM, adapted from NIST and data privacy frameworks. A sample of 20 MDAs was selected using purposive sampling, guided by ICT-dependency rankings (Mbanaso et al., 2022). Data were collected from official reports, personnel surveys, and ICT infrastructure assessments. Python code was used to compute readiness scores, which were then ranked and mapped to cybersecurity readiness quadrants (Q1–Q4).

Cybersecurity Readiness Framework



Cybersecurity Readiness Framework Adapted from NIST Cybersecurity Framework CSF and NIST Data Privacy Framework

Results

This equation $0.70(CRAM_{ipm}) + 0.30(CRAM_{iim})$ is the mathematical model used for the evaluation of the cybersecurity readiness of the MDAs. The value of CRI is between 0.00 and 1.00

Computing WEIGTH (%) i.e. Score Achieved/Targeted Score * Expected %

Weights of Cybersecurity Readiness Assessment Metrics (CRAM) – Adapted from (Mbanaso & Kulugh, 2021)

#	CRAM	Code	Description	Weights (%)	Weight factor (wf)
1	Incident Probability minimization	*Ipm*	Reduces the probability of a successful breach on the cyber assets of MDAs	70%	0.70%
3	Incident impact minimization	*Iim*	Reduces the impact of a successful breach on the cyber assets of MDAs	30%	0.30%
	Total			**100%**	**1.00%**

The python codes below compute the incident probability minimization ipm for the five pillars and the two pillars for incident impact minimization iim of the sample MDAs.

```
df_mdas['Weight_lpm']=((df_mdas['IDENTIFY']/36)*20)+((df_mdas['PROTECT']/48)*20)
+((df_mdas['DETECT']/36)*20)+((df_mdas['GOVERN']/24)*20)+((df_mdas['CONTROL']/24)*
20)
```

and df_mdas['weight_iim']=((df_mdas['RESPOND']/24)*50)+((df_mdas['RECOVER']/36)*50)

The codes below compute the cybersecurity readiness assessment metrics i.e impact probability minimization and incident impact minimization.

df mdas['CRAM_IPM'] = (df_mdas['Weight_Ipm']*0.70)/100 and

df_mdas['CRAM_IIM'] = (df_mdas['weight_iim']*0.30)/100

Computing Cybersecurity Readiness Quadrant (CRQ)

Cybersecurity Readiness Quadrant adapted from (Mbanaso, Abrahams, & Apene, 2019)

Quadrant	Range	Description
Q1	0.00 – 0.25	The MDA is at a very low level of readiness for cybersecurity incidences, this means the MDA is at high cyber risk.
Q2	0.26 – 0.50	This shows a low to medium level of cybersecurity readiness by the MDAs. This implies a low to moderate cyber risk
Q3	0.51 – 0.75	This depicts a high level of readiness by the MDA to address cybersecurity risk but with some readiness components not maximized
Q4	0.76 – 1.00	This quadrant shows that the level of readiness is very high and maximized with cybersecurity risk at it minimal level.

Below is the python code used to compute the cybersecurity readiness quadrant of the sampled MDAs:

```
CRQ= np.arange(20)conditions = [ (df_mdas['CRI'] > 0.75) & (df_mdas['CRI'] <= 1.00),
(df_mdas['CRI'] >= 0.51) & (df_mdas['CRI'] < 0.76),(df_mdas['CRI'] >= 0.26) & (df_mdas['CRI']
< 0.51),(df_mdas['CRI'] >= 0.0) & (df_mdas['CRI'] < 0.26),]
values = ['Q4','Q3','Q2','Q1']  df_mdas['CRQ'] = np.select(conditions, values)
```

The code below is used to sort the value count as obtained by each MDAs

df_mdas_sorted['CRQ'].value_counts() and the result is

*Q2 6 Q3 6 Q4 4 Q1 4

Name: CRQ, dtype: int64

This shows that 6 MDAs are in Q2, 6 in Q3, 4 in Q4 and 4 in Q1

Computing Cybersecurity Readiness Index

Cybersecurity Readiness Measure Scale

Quantitative	Qualitative	Description
0	None	None-existence of the indicative cybersecurity readiness practice in the MDA, implying a zero score
1	Low	Has little or low value of the indicative cybersecurity readiness practice in the MDA's operations, functions or service
2	Moderate	Has moderate value of the indicative cybersecurity readiness practice in the MDA's operations, functions or service
3	High	Has high value of the indicative cybersecurity readiness practice in the MDA's operations, functions or service
4	Very High	Has very high value of the indicative cybersecurity readiness practice in the MDA's operations, functions or service

The code below computes the cybersecurity readiness index of all the sampled MDAs
df_mdas_viz = df_mdas[['MDA CODE','CRI']]df_mdas_viz.round(2) the result is

S/NO.	MDA CODE	CRI	S/NO.	MDA CODE	CRI
1	WDVB	0.59	11	CVBN	0.26
2	QWRT	0.04	12	YUIO	0.80
3	PLKJ	0.25	13	BNHY	0.29
4	ASDF	0.71	14	MKYU	0.68
5	BCVG	0.43	15	GFDS	0.62
6	POIY	0.29	16	CVBL	0.38
7	QSCV	0.24	17	OCXG	0.44
8	HYGB	0.06	18	BXVT	0.83
9	JKLY	0.93	19	XWTY	0.66
10	XEFG	0.73	20	GFYK	0.93

From the result above, only four organizations from the sampled MDAs are in Q4. This quadrant shows that the level of readiness is very high and maximized with cybersecurity risk at its minimal level. Six MDAs are in Q3. This result depicts a high level of readiness by the MDA to address cybersecurity risk, but with some readiness components not maximized. Six MDAs are in Q2, and this shows a low to medium level of cybersecurity readiness by the MDAs. This implies a low to moderate cyber risk. Four MDAs are in Q1, showing that the MDAs are at a very low level of readiness for cybersecurity incidences. This means the MDAs are at high cyber risk.

Discussion

The assessment reveals significant disparities in cybersecurity capabilities across Nigerian MDAs. Many agencies lack structured security policies, recovery plans, or governance mechanisms. While a few demonstrate strong readiness, the majority operate with medium or low-level defenses. The CRMM framework proves effective for quantifying readiness and guiding targeted interventions.

Conclusion

Cyber threats continue to evolve, requiring a robust and dynamic cybersecurity posture among public institutions. This study shows that while some MDAs are prepared, most remain vulnerable. Implementing CRMM-based evaluations provides a systematic way to assess risks, identify weaknesses, and prioritize improvements in cybersecurity infrastructure.

Recommendations

1. Enforce Cybersecurity Laws: Ensure full implementation of Nigeria's cybercrime legislation across all MDAs.
2. Promote Awareness Campaigns: Train personnel and the general public on cybersecurity best practices.
3. Adopt National Frameworks: Mandate the use of CRMM or similar models for regular assessment.
4. Strengthen ICT Governance: Establish cyber governance units within all MDAs.
5. Recruit Cybersecurity Experts: Employ trained cybersecurity professionals to oversee digital defense.
6. Continuous Monitoring and Auditing: Regular vulnerability assessments and penetration testing.
7. Develop Incident Response Plans: Institutionalize recovery and response strategies across MDAs.

References

Global Cybersecurity Index Report (2020) e-Governance Academy Foundation. International Telecommunication Union. https://www.itu.int.

Graham K. (2021) Cybersecurity Readiness: What is it and how do you evaluate your Security Performance Management. Bitsight Security Rating Blog Cybersecurity News & Tips.

Kott, Alexander, Cliff, Wang Erbacher, Robert F. (2015). *Cyber Defense and Situational Awareness*. Springer International Publishing, Switzerland.

Linkov, I., Anklam, E., Collier, Z. A., DiMase, D., Renn, O. (2014). *Risk based standards: integrating top-down and bottom-up approaches*. Environment System Decisions 34 (1): 134–137.

Lucas A. (2017, 20 September). *How prepared is Nigeria for cyber-attacks*? The Nation Newspaper.

Marvin Waschke (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime.* Bellingham, Washington, USA.

Mbanaso, U. M. (2018). *Principles of Security Lecture Note*. Nasarawa State University, Keffi, Nasarawa State.

Mbanaso, U., Kulugh, V., Musa, H., Aimufua, G., & Dandaura, E. (2022). Quantitative Assessment of Critical Infrastructures Degree of Dependency on Information and Communications Technology. *International Journal of Critical Infrastructures*, *15* (3).

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. 1 (1): Draft. https://doi.org/10.1109/JPROC.2011.2165269

Petit, F., Bassett, G., Buehring, W. A., & Whitfield, R. G. (2013). *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Journal of Critical Infrastructure (IJCIS) 7 (3): 200-219.

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, 125–138. https://doi.org/10.1016/j.ijcip. 2019.03.003