3MTT NIGERIA/TEDPRIME HUB CYBERSECURITY COHORT2 GROUP 4 REPORT

POTENTIAL CYBERSECURITY RISK ASSESSMENT IN GOVERNMENT/PUBLIC SECTOR

CASE STUDY – NIMC(NIN)

A. Background Information

Cybersecurity has become a critical concern in the digital age, as the increasing reliance on technology exposes organizations to various threats. In the public sector, the stakes are even higher, as government entities manage sensitive data and provide essential services that are vital to the functioning of society. The National Identity Management Commission (NIMC) of Nigeria, responsible for managing the National Identification Number (NIN), represents a prime example of a public sector organization that must prioritize cybersecurity to protect citizens' data and ensure the integrity of its operations.

B. Importance of Cybersecurity in the Public Sector

The government handles vast amounts of critical data, including personal, financial, and national security information, making it a prime target for cyberattacks. Past cybersecurity breaches in the public sector, such as the Office of Personnel Management (OPM) data breach in the United States, highlight the severe consequences of inadequate security measures. These breaches can lead to significant financial losses, compromised national security, and a loss of public trust. Therefore, robust cybersecurity measures are essential to protect the public sector's operations and the sensitive information it manages.

C. Purpose and Scope of the Project

This report aims to analyze the potential cybersecurity risks within the government/public sector, with a specific focus on the NIMC and its management of the NIN. By examining the various types of threats and vulnerabilities that could impact government operations, the report seeks to provide a comprehensive assessment of the risks and propose strategies for mitigating them. The sections covered in this project include an exploration of external and internal threats, an assessment of vulnerabilities in government systems, and a review of the consequences of cybersecurity breaches.

Likelihood & Impact Key

Very Low- 1, Low- 2, Medium- 3, High- 4, Very High- 5

Risk

Low Risk: 1-5, Medium Risk: 6-10, High Risk: 11-15, Very High Risk: 16-20, Extreme: >20

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ASSETS | THREATS | LIKELIHOOD | IMPACT | RISK | JUSTIFICATION |
| NIMC-Databases | Insider Threats  (Identity theft) | 5- Nigeria ranks high in most corrupt countries in the world | 5- This access depending on the privileges can greatly compromise data of almost 200M people | 25 | Extreme- A strong encryption, avoidance of privilege creep, adequate remuneration for office holders and background checks will help resolve this. |
| NIMC- Buildings | Natural Disasters | 1- Nigeria is not prone to Natural Disasters | 5- Disasters occurring will ruin properties housed in NIMC | 5 | Low- Multiple cloud facilities usually cater for natural disasters. |
| NIMC- Databases | Ransomwares | 2- Requires a high level of tech savviness, so, rarely occurs in Nigeria | 5- An attack will render the NIMC useless as this inaccessibility is dangerous | 10 | Medium- Regular multiple backups and redundancy is employed efficiently |
| NIMC- Customers | Phishing | 5- Phishing is one of the oldest tricks in the book, so, it is rampant even in Nigeria | 2- Phishing attacks rarely catch a large amount of people | 10 | Medium- public sensitization and awareness are efficiently employed here |
| NIMC-Websites | Distributed Denial Of Service | 2- Nigeria is an emerging market and while it is low right now, the future holds potential danger. | 3- Most Nigerians have been verified so a short period of inaccessibility will barely affect process. | 6 | Medium- More focus should be placed on intelligent security that can ban specific IP threats and use of load balancers should be enhanced. |

ASSETS

“Assets” are valuable resources an organization must protect from threats. These include data, hardware, software, networks, personnel, intellectual property, and physical facilities. Proper identification and management of these assets are crucial for risk assessment, prioritization, and incident response, ensuring that critical assets are safeguarded against potential threats.

Effective asset management involves maintaining an up-to-date inventory, classifying assets based on importance, implementing access controls, and conducting regular audits. This helps organizations allocate resources efficiently, comply with regulations, and protect their operations from security breaches.

By prioritizing and protecting assets, organizations can mitigate risks, ensure business continuity, and maintain stakeholder trust. Understanding and managing assets is key to a robust cybersecurity strategy, as it enables organizations to respond effectively to threats and safeguard their most critical resources.

THREATS

Cyber threats are malicious activities aimed at disrupting, damaging or gaining unauthorized access to computers, networks, personnel and data. Common types of cyber threats include malware, phishing attacks, denial-of-service (DoS) attacks, and ransomware. Each of these can cause significant harm to an organization's operations, data integrity, and reputation.

Threats are constantly evolving, with attackers developing new tactics and techniques to bypass security measures. Organizations must continuously monitor, assess, and mitigate threats to protect their assets and maintain operational resilience. This involves implementing robust security measures, conducting regular threat assessments, and staying informed about emerging threats. Proactive threat management, including threat intelligence and incident response planning, is essential to minimize the impact of potential attacks and safeguard the organization's critical infrastructure and data.

VULNERABILITIES

Vulnerabilities are weaknesses or flaws in systems, networks, physical buildings or applications that can be exploited by attackers to gain unauthorized access, cause harm, or perform malicious activities. Vulnerabilities are categorized under network, software, hardware and physical vulnerabilities as will be examined in this report. Attackers often seek out these weaknesses to launch cyberattacks, such as data breaches, ransomware attacks, or denial-of-service (DoS) attacks. This report will identify and mitigate vulnerabilities through risk assessments as is crucial to maintaining the security and integrity of an organization's systems. These vulnerabilities range from software bugs, misconfigurations, outdated software, or inadequate security measures in physical buildings such as lack of fire escape or fire extinguishers.

LIKELIHOOD

“Likelihood” refers to the probability or chance that a specific threat will successfully exploit a vulnerability within a system, network, or application. Factors influencing likelihood include the presence of vulnerabilities, the motivation and capability of attackers, and the effectiveness of existing security controls.

IMPACT

“Impact” is primarily justified by the effect that a threat will have if it occurs, not just the likelihood of it happening. While the likelihood or possibility of a threat occurring is important for risk assessment, the impact is about the severity of the consequences if the threat materializes.

RISKS

In cybersecurity, risks refer to the potential for loss or damage when a threat successfully exploits a vulnerability. Risk is a combination of the likelihood that a threat will occur and the impact it will have if it does. Effective risk management involves identifying vulnerabilities, assessing the associated risks, and implementing measures to mitigate or reduce those risks. This approach helps organizations prioritize their security efforts, protect critical assets, and minimize potential damage from cyber threats.

Risk is mathematically defined as the product of likelihood and impact. This means that risk is determined by both the probability that a threat will exploit a vulnerability (likelihood) and the potential consequences or damage that would result from that exploitation (impact). By quantifying both factors, organizations can assess the overall risk associated with specific vulnerabilities and prioritize their security measures accordingly to mitigate the most significant risks.

In conclusion, the cybersecurity landscape in the public sector is increasingly complex and demands a proactive, comprehensive approach to mitigate potential risks. The case of NIMC's management of the NIN underscores the critical need for robust security measures to protect sensitive data and maintain public trust. By addressing vulnerabilities, enhancing security protocols, and fostering a culture of awareness, government institutions can safeguard their operations against both internal and external threats, ensuring the resilience and integrity of their systems in the face of evolving cyber threats.