DUALE, OVIA & ALEX-ADEDIPE

# Cybersecurity Requirements for Technology Platforms in Nigeria

**The landscape of cybersecurity has evolved from being a topic for tech enthusiasts and specialists to entrepreneurs and innovators who operate tech platforms in their business operations across industries.**

With the increase of data breaches, cyber-attacks, and privacy concerns, industry regulators have taken proactive steps to enforce stringent cybersecurity requirements for tech companies and operators of technological platforms. This TMT Thursday edition deals with some of these cybersecurity measures.

**doa-law.com**

## Introduction

**The landscape of cybersecurity has evolved from being a topic for tech enthusiasts and specialists to entrepreneurs and innovators who operate tech platforms in their business operations across industries.**

With the increase of data breaches, cyber-attacks, and privacy concerns, industry regulators have taken proactive steps to enforce stringent cybersecurity requirements for tech companies and operators of technological platforms. This TMT Thursday edition deals with some of these cybersecurity measures.

### 1. Comprehensive Risk Assessment:

Technology companies should conduct periodic comprehensive risk assessment on their platforms to identify potential vulnerabilities and threats. This assessment should encompass all aspects of the business, including networks, systems, applications, and data assets. By understanding their unique risk landscape, technology companies can develop targeted strategies to mitigate risks effectively.

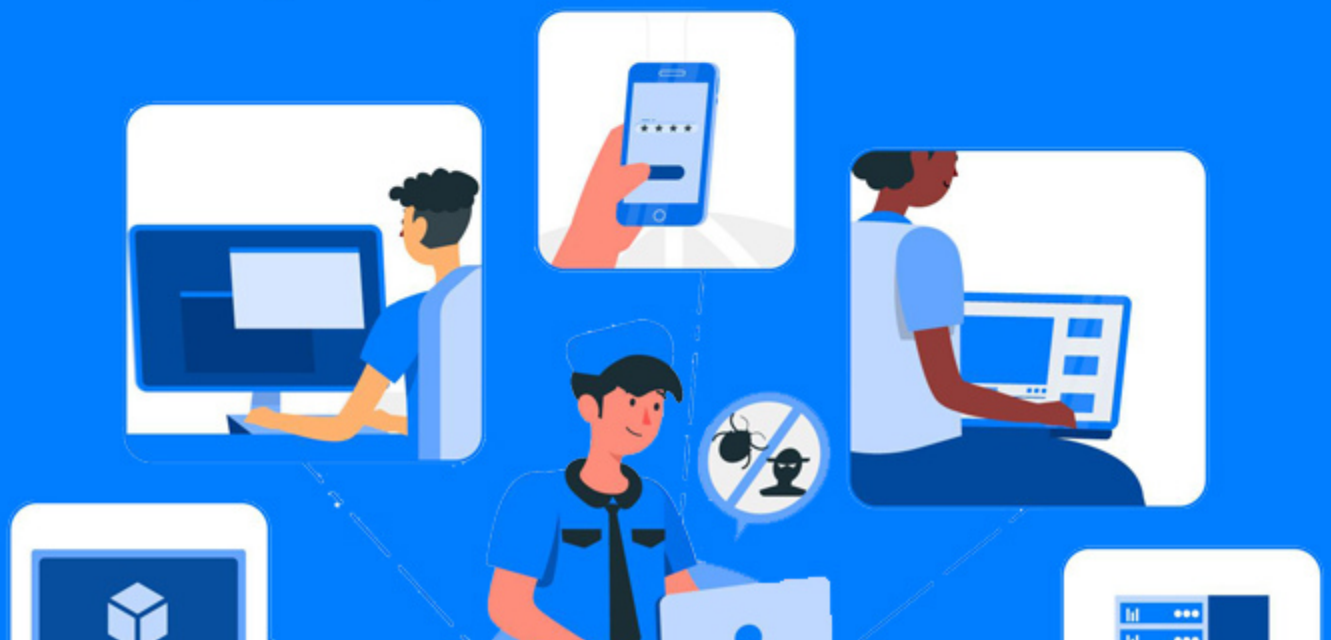
Technology companies should conduct periodic comprehensive risk assessment on their platforms to identify potential vulnerabilities and threats. This assessment should encompass all aspects of the business, including networks, systems, applications, and data assets. By understanding their unique risk landscape, technology companies can develop targeted strategies to mitigate risks effectively. [1]

## 2. Strong Access Controls:

Access control involve system features to verify a user's credentials, manage access, and monitor usage. Access controls are crucial to cyber security. Hackers develop sophisticated tools to take over computer systems including bots that search/mine valuable data. This can be contained through strong access controls.

Implementing strong access controls involves measures such as user authentication, user authorization, role-based access permissions, and multi-factor authentication. These controls are aimed at significantly reducing the risk of unauthorized data breaches. These include the 2nd factor authentication ("**2FA**"). Financial institutions have been mandated to implement 2FA at login points for applications which facilitate transfers, withdrawal, deposit, standing order, and account maintenance and system maintenance processes.

[1] Section 39 (2) (e) of the Nigeria Data Protection Act 2023; Paragraph 3.3 of the Risk-Based Cybersecurity Framework and Guidelines for MDBs and PSPs 2018 (the "Cybersecurity Guidelines").



### 3. Regular Software Updates and Patch Management:

One of the most common entry points for cyber-attacks is through unpatched software vulnerabilities. This is because having outdated software on your systems can cause vulnerabilities and exposures in the operating system and allow cyber criminals to gain access to a user's system and their valuable information.

To mitigate this risk, technology platform operators must establish a robust patch management process to ensure that all software and systems are regularly updated with the latest security patches and fixes. This proactive approach helps close potential security gaps and strengthens the overall security posture of the organization.[2]

### 4. Data Encryption:

Technology companies use data encryption to protect digital data confidentiality using encryption algorithms. The algorithms provide confidentiality and enforce security initiatives such as authentication, integrity, and non-repudiation.

---

[2] Appendix III, Paragraph 1.6, and Appendix IV, Paragraph 6(a)(vii) and (viii) of the Cybersecurity Guidelines.

## 4. Data Encryption:

Encrypting sensitive data, both at rest and in transit, is essential for protecting it from unauthorized access or interception by cybercriminals. By employing strong encryption algorithms, technology platforms can ensure that even if data is compromised, it remains unintelligible to unauthorized parties. Implementing encryption protocols for data storage, communication channels, and mobile devices adds an extra layer of security to sensitive information.[3]

## 5. Pseudonymisation:

Pseudonymization strengthens the security of sensitive data by replacing identifying information with pseudonyms or aliases, reducing the risk of unauthorized access and data breaches.[4]

[3] Section 39(2) (b) of the Nigeria Data Protection Act 2023.
[4] Section 39(2) (a) of the Nigeria Data Protection Act 2023.

### 6. Cybersecurity Training and Awareness for Personnel:

Human error stands as a top cybersecurity risk for businesses. Employees, often unknowingly, open doors to cyber-attacks through phishing emails, social engineering, or weak passwords. Investing in thorough cybersecurity training, empowers staff, contractors, and customers to recognize threats, safeguard data, and report suspicious activity.[5]

### 7. Robust Incident Response Plan:

Even with proactive cybersecurity, every organization faces the risk of cyber-attacks. This highlights the need for an Incident Response Plan (IRP) which should outline steps for detecting, and mitigating security breaches. The IRP may also outline protocols for informing stakeholders and authorities. It is also important to establish a dedicated team to handle cyber-incidents for quick and effective responses.[6]

---

[5] Appendix 4, Paragraph 3 of the Cybersecurity Guidelines.
[6] Section 39(2) (d) of the Nigeria Data Protection Act 2023; Appendix IV, Paragraph 8 of the Cybersecurity Guidelines.

## 8. Continuous Monitoring and Threat Intelligence

Cyber threats are constantly evolving, requiring technology platform operators to adopt a proactive monitoring approach to cybersecurity. Continuous monitoring of network traffic, system logs, and user activities helps detect and respond to potential security incidents in real-time. Additionally, leveraging threat intelligence feeds, and security information and event management systems, enables organizations to stay ahead of emerging threats and adapt their defenses accordingly.[7]

## 9. Reporting Obligations:

The Cybercrimes (Prohibition and Prevention) Act 2021 requires platform operators to promptly notify the National Computer Emergency Response Team (CERT) Coordination Center of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues.

[7] Section 39(2) (f) and (g) of the Nigeria Data Protection Act 2023.

Similarly, under the Nigeria Data Protection Act 2023, data processors are required to report any breach of data processed or stored by it to the data controller, whom shall report all data breaches to the Nigeria Data Protection Commission and where possible, indicate the number of data subjects affected.

## Conclusion

In today's digital landscape, cybersecurity is both a legal and commercial necessity. By implementing robust cybersecurity measures, businesses can protect their valuable assets, maintain customer trust, and safeguard their reputation in the face of evolving cyber threats while achieving regulatory compliance.