THE ROLES OF FINANCIAL INSTITUTION TO DATA SECURITY AND PRIVACY

PRESENTED BY MR. HARUNA BALA MUSTAFA

DIRECTOR, BANKING SUPERVISION DEPARTMENT, CENTRAL BANK OF NIGERIA

December 9, 2021

TABLE OF CONTENTS

INTRODUCTION

Data security and privacy are at the front-burner of discussion by Regulatory Authorities, despite the economic rage caused by the COVID-19 pandemic.

Today, organizations that manage data are charged with the responsibility of protecting the data collected and the information that can be inferred from such data.

Without securing these data/information, cybercriminals and other malicious actors would take advantage of this gap and adverse impacts such as fraud, identity theft, denial of service, etc., may crystallize

Data Security and Privacy are, however, sub-components of Data Protection; which is primarily concerned with the proper handling of sensitive data to meet regulatory and other security requirements.

Typically, in the field of data protection, there are at least two (2) parties: Data Owner/Subject and Data Custodian (keepers of data) e.g. Banks, Credit Bureau, Hospitals, Payment Service Providers, Agencies etc.

INTRODUCTION - CONT.

Too often, the terms Security and Privacy are used interchangeably, however the terms are quite different and it is pertinent to differentiate them as follows:

Data Security is achieved using policies, tools, and technology solutions such as firewalls, user authentication, network limitations. Data Privacy is, however, achieved through measures that prevent data inference and linking of sensitive data to its data owner/subject

Data Security can be met without satisfying Data Privacy requirements. However, one cannot address Data Privacy concerns without first employing effective Data Security practices

Data Security is about protecting data from malicious threats, whereas Data Privacy is about using it responsibly and following the consent of the customer or data owners

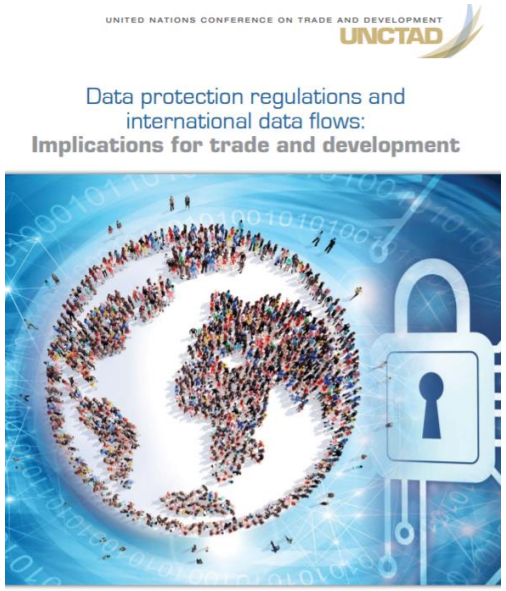
Data security is primarily focused on preventing unauthorized access to data, via breaches or leaks, regardless of who the unauthorized party is while Data Privacy is concerned with ensuring that the sensitive data an organization processes, stores, or transmits is consented to by the data owner of the sensitive data.

INTRODUCTION - CONT.

Consequently, as more and more social, and economic activities happen online, the importance of privacy and data protection is increasingly recognized. For instance, a publication by the United Nations Conference on Trade and Development (UNCTAD), on Data Protection and Privacy Legislation Worldwide (February 2020), stated that:

- About 66% of countries globally have data protection legislation (over 50% of African countries have data protection legislation); this includes Nigeria.

- 10% of countries have draft data protection legislation



- Approx. 15% of countries have no evidence to determine whether they have data protection legislations or not.

- 10% of countries have no data protection legislation

APPROACH OF THE CBN TO SECURITY AND PRIVACY OF DATA

One of the mandates of the CBN is to promote a sound financial system in Nigeria. To however, achieve this mandate, the security and privacy of financial data is a major requirement. In this vein, the CBN has issued several frameworks and guidelines to ensure the security and privacy of financial data in Nigeria; which include but are not limited to:

1. ***Regulatory Framework for Open Banking in Nigeria, 2021.***

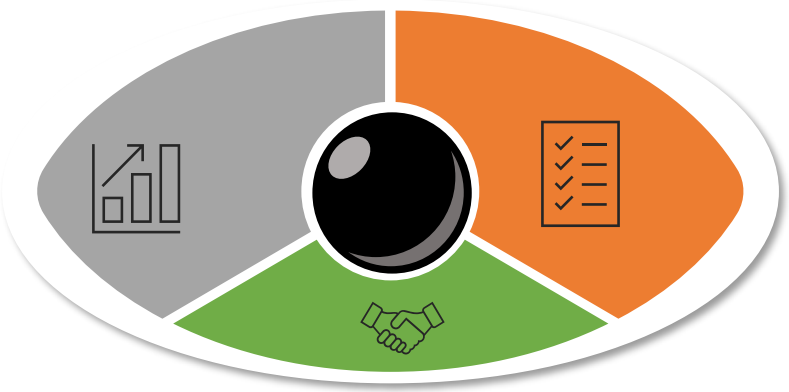
2. ***The CBN Risk-based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018***

3. ***Consumer Protection Regulation, 2019***

BENEFITS OF SECURITY AND PRIVACY OF DATA

It is imperative to say that any organization that implements data security and privacy measures stand a chance of having:

- Enhanced organization reputation.
- May lead to Increase In Revenue



- Improved Customer Loyalty and Confidence

- Assured data integrity and availability.
- Reduction in regulatory risks and penalties resulting from data protection and privacy breaches.
- Reduced unauthorized access.

SECURITY AND DATA PRIVACY REGULATIONS

Here are a few common regulations to help provide guidelines for maintaining security and data privacy

Sector

- Financial Industry: The Payment Card Industry Data Security Standard (PCI DSS) is a set of rules for protecting sensitive payment card information and cardholder data. It applies to banks, merchants, third parties, and other entities that handle cardholder data from the major payment card brands.
- Healthcare Industry: The Health Insurance Portability and Accountability Act (HIPAA) is concerned with protecting the sensitive health information of patients across the United States of America

Region

- The EU General Data Protection Regulation (GDPR) is among the world's toughest data protection laws protecting the privacy of EU citizens. Under the GDPR, the EU's data protection authorities can impose fines up to €20 million (roughly $20,372,000), or 4 percent of worldwide turnover for the preceding financial year - whichever is higher - if there is a breach of EU Citizen's data.
- Africa / Nigeria

Africa/Nigeria:

Here are a few common regulations to help provide guidelines for maintaining security and data privacy

Sector

- Healthcare Industry: The Health Insurance Portability and Accountability Act (HIPAA) is concerned with protecting the sensitive health information of patients across the United States of America

- Financial Industry: The Payment Card Industry Data Security Standard (PCI DSS) is a set of rules for protecting sensitive payment card information and cardholder data. It applies to banks, merchants, third parties, and other entities that handle cardholder data from the major payment card brands.

Region

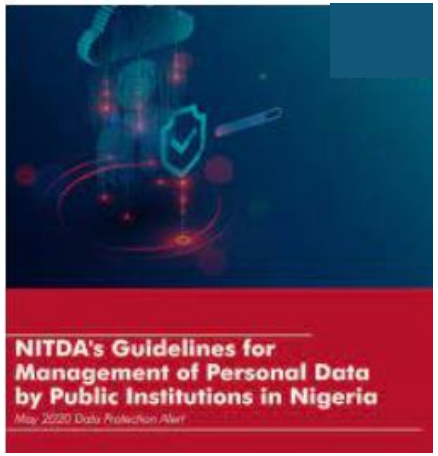
- The EU General Data Protection Regulation (GDPR) is among the world's toughest data protection laws protecting the privacy of EU citizens. Under the GDPR, the EU's data protection authorities can impose fines up to €20 million (roughly $20,372,000), or 4 percent of worldwide turnover for the preceding financial year - whichever is higher - if there is a breach of EU Citizen's data.

- Africa / Nigeria

Africa/Nigeria:

The Nigerian Data Protection Regulation (NDPR) 2019.

National Information Technology Development Agency (NITDA) issued the first data protection regulation in Nigeria to create awareness of data protection and privacy and to regulate those who have access to and control people's data.



Guidelines for The Management of Personal Data by Public Institutions in Nigeria, 2020.

Issued as a Guideline for the Implementation of the Nigeria Data Protection Regulation (NDPR), 2019, within Public Institutions in Nigeria.

Guidelines for The Management of Personal Data by Public Institutions in Nigeria, 2020.

Issued as a Guideline for the Implementation of the Nigeria Data Protection Regulation (NDPR), 2019, within Public Institutions in Nigeria.

IMPLICATION OF SECURITY AND DATA PRIVACY TO REGULATORS & DATA OWNERS

Regulators / Supervisors

- Regulators are required to issue directives, frameworks, and provide enabling environments that will engender the security and privacy of data.
- Supervisors are responsible for enforcing compliance with security and data privacy regulations.

Consumer/Data Owners

- They are mandated to know data security and privacy controls of data custodian, and check if it suits their requirements.
- A Data Owner is accountable for who has access to information assets within their functional areas

IMPLICATION OF SECURITY AND DATA PRIVACY TO FINANCIAL INSTITUTIONS

- Financial Institutions are responsible for the safe custody, transport, storage of the data, and implementation of business rules.
- They are the keepers of data, mandated to implement and administer controls over the information; according to instructions from owners and the law.
- They must understand the challenges of data security and privacy and devise strategies to address them.
- They must continually access compliance with applicable data protection laws and regulations.
- They must ensure that data protection is part of the organization culture, complimented with staff training and performance indicators.

TOP THREE (3) REGULATORY FINES FOR BREACH OF DATA SECURITY AND PRIVACY

Amazon

Amazon reported a penalty of €746 million in its July 2021 earning statement as a result of browser cookie consent and the way it collects and shares personal data via cookies. Similarly, in late 2020, France fined Amazon €35 million after the tech giant allegedly failed to get cookie consent on its website as customers shop online.

Google

In 2019 Google was fined €50 million because of how the tech giant provided privacy notice to its users and how the company requested their consent for personalized advertising and other types of data processing

H&M

On October 5, 2020, the Data Protection Authority of Hamburg, Germany, fined the clothing retailer H&M €35,258,707.95. H&M's GDPR violations involved the "monitoring of several hundred employees."

CHALLENGES TO SECURITY AND PRIVACY OF DATA

Data privacy and protection is not an easy task. It starts with classifying data and ensuring that the data (both sensitive and personally identifiable information) are protected according to their risk-level. However, security and data privacy come with several challenges

1. High Cost of Maintaining Data Privacy
2. The Growth of Data is Exponential
3. Human Error Creates a Level of Complexity
4. Increased Number of Open Vulnerabilities
5. Third-party Engagement in Data

CONCLUSION

Let me conclude by re-emphasizing the importance of data security and privacy.

- Financial services providers must continually ensure that security and data privacy controls are implemented in products and services offered to customers.

- During product design, consumer protection regulations and consumer consent should be paramount.

Concluding Remarks…….

Thank You!