

# **CYBERSECURITY AND DATA PROTECTION IN ACCOUNTING: BEST PRACTICES**

**By**

**Prof Fatima Alfa Tahir (BSc, MBA, MSc, PhD, FCNA)**

**Department of Accounting, University of Maiduguri**

## **Introduction**

In today's digital era, organizations are increasingly seeking best practices that prioritize data security. In order to achieve this, organizations need to understand the criticality of safeguarding their sensitive information. Accounting professionals are custodians of financial data. They collect, process, summarize and report sensitive financial information in their roles as finance officers, accountants, tax consultants and auditors. Hence, safeguarding client information is not only vital but also mandatory in line with professional codes of conduct. Professional accountants in organizations may also be employees that are part of the risk mitigation mechanisms. As such, Knowledge of cybersecurity and data governance is essential for ensuring financial data integrity, due diligence and safeguarding the reputation of the profession.

In recent times, advancements in information and communication technology continues to have a massive impact in the way humans relate to their environment. This encompasses all aspects of social interaction from commerce, education, health, hospitality, travel, leisure among others Gordon et al. (2003). Coupled with these changes, the COVID 19 pandemic forced nations and organizations to device alternative ways of doing business requiring minimal physical human interaction. As a result, the digital economy blossomed with commercial banks and fintech companies as major stakeholders championing financial intermediation between buyers and sellers through providing innovative financial interphases and products. However, expansion of the digital economy came with attendant risks related to cybersecurity and cybercrimes (Islam et al., 2018).

## **Major global Cyberattack Incidents**

According to Stedman (2024) some recent major cyberattack incidents include:

- In 2023, Movelt file transfer application was breached and allowed unauthenticated hackers gain unauthorized access to its database
- A file transfer tool sold by Progress Software, that is believed to have led to breaches involving more than 2,700 organizations and 94 million people.
- In 2021 hackers scraped about 533 million Facebook users' data and leaked it into a hacking forum
- Microsoft reported a breach in 2020 when 250 million customer service and support records over a 14-year period was exposed online.
- A consistent security breach at Marriott International Inc. across several years compromised personal data of about 383 million guests in total.
- Yahoo suffered two major breaches that exposed 500 million users accounts in 2014 and all 3 billion accounts in 2013.

### **Major Local (Nigeria) Cyberattack Incidents**

Even though industry players are hesitant to disclose threats incidence (Udi, 2023) some include;

- Nigerian Inter-Banks Settlement Systems Plc (NIBSS) as at January 2019, reported at least N46, 000, 000 million Naira lost to cyber criminals in 2018
- Sophos- a cyber security firm reported by Nairametrics, 71% of Nigerian firms were hit with ransomware in 2021.
- Nigerian businesses paid as much as \$706,452 as ransom to cyber-criminals in 2021.
- Cyber Security Expert Association of Nigeria (CSEAN) report Small and Medium Scale Enterprises (SMEs) were the most hit by cyber-attacks in 2022, recording an increase in phishing attacks from 37% in 2021 to 87% in 2022.

### **Paper Objectives**

Against this background, this paper seeks to explore the following objectives:

- Explain the concept of Cybersecurity
- Highlight the Importance of Safeguarding Financial Data in the Digital Age
- Explain the Relevance of Cybersecurity to Organizations and Financial Officers
- Discuss Common Cyber Security Threats Affecting Data/Financial Information
- Provide an Overview of Nigeria Data Protection Act (NDPA) 2023 and Cyber Security

- ✓ Principles of Processing Personal Data
- ✓ Key considerations for Processing of Personal Data
- ✓ NDPA ACT Enforcement and Penalties
- ✓ Challenges to the NDPA 2023
- Explain the Concept of Cybersecurity Planning for Organizations and Businesses
- Discuss Contemporary Cybersecurity tips and Best Practices for Data Protection
- Discuss the Concept of Cybersecurity Risk Management
- Explain Cybersecurity Risk Management Strategy (Map, Monitor, Mitigate & Manage)
- Discuss the Role of Accountants/Finance Professionals in Cybersecurity Management
- Highlight Key Cyber Risk Challenges
- Discuss the Critical Security Requirements in choosing Cloud Service Providers

## Cybersecurity

Cybersecurity involves safeguarding systems, networks, and software from digital threats or cybercrimes. These threats typically seek unauthorized access, alteration, misuse or destroy valuable information. They also serve as medium to among others:

- extort money through ransomware
- identity theft
- corrupt sensitive data
- steal sensitive information
- spy on activities
- steal personal effects, copyrights or patents
- disrupt regular business operations
- gather insider information for other unethical businesses

Implementing effective cybersecurity measures is an issue that affects all organizations, particularly challenging today because attackers are becoming more innovative (Kahyaoglu & Caliyurt, 2018). Securing financial data covers an elaborate harmonization of the systems component parts such as the technologies, policies, procedures and physical safeguards deployed to protect sensitive financial data. An effective cybersecurity strategy involves employing various layers of protection distributed across computers, networks, programs, or data to ensure asset and information security

(Haapamäki & Sihvonen, 2019). Additionally, it is crucial that there is synergy between people, processes, and technology to reinforce each component, thus forming a robust defence against cyber-attacks. The main objective of securing financial data is to safeguard information from unauthorized access, corruption, and theft throughout its lifecycle. So, what constitute sensitive financial information? Sensitive financial information varies across organizations and may include bank account or verification numbers, security passwords, ATM card numbers, date of birth, OTPs, transaction data, payroll etc

### **Importance of Safeguarding Financial Data in the Digital Age**

The financial sector is a prime target for hackers aiming to access sensitive information or disrupt operations. However, safeguarding financial data extends beyond protection against cyber threats as there are also natural disasters, hardware failures, or human errors that can pose substantial risks. Cloud providers mitigate these concerns by incorporating strong data redundancy and disaster recovery mechanisms. Financial institutions can utilize the cloud's distributed nature to store data across multiple geographically diverse data centers. This redundancy guarantees that in the event of an outage or data loss in one center, the information remains accessible from other locations. This strategy enhances the overall resilience of financial systems and mitigates the impact of unforeseen events. Even though initial costs are high, the consequences of failing to safeguard all data, especially financial data are enormous ranging from:

- potential loss of job/business
- bad publicity
- damaged customer relationships
- significant financial losses to entities and their customers or ransom payments
- prosecution, fines and restitution to victims of data breach and recovery costs

Hence, it becomes imperative to inculcate best practices that mitigate risk exposures and safeguard financial data from cybercriminals (Gansler & Lucyshyn, 2005). This will not only ensure data and financial security but will also reinforce trust and confidence of users of financial technologies as well as compliance with legal requirements. This paper discusses the risks

associated with digitalization, importance of safeguarding accounting data and provide invaluable tips to enable stakeholders protect their data.

### **Cybersecurity Challenges of Entities and Businesses**

- Evolving security threats and attack methodologies
- Increased vulnerability to attacks due to data volumes, digital operations and remote working.
- Wider attack surface resulting from the proliferation of systems, applications, mobile devices, and other endpoint technologies.
- Emerging security requirements driven by the widespread adoption of cloud and IoT technologies.
- Formidable adversaries with advanced capabilities and substantial financial backing, including state-sponsored cybercrime initiatives.
- The utilization of AI and machine learning technologies, including generative AI tools, for automating attacks.
- Challenges related to budget constraints, staffing limitations, and resource availability.
- Shortage of cybersecurity experts with requisite skills.
- Poor cybersecurity awareness among individuals, entities and business users.

### **Relevance of Cybersecurity to Organizations and Financial Officers**

Accountants process financial data into information at the close of specified financial period when books are closed to enable accurate financial reporting. During the closing period, they reconcile accounts, adjust entries and ensure appropriate posting of entries. In the courses of their duties, they need to ensure sensitive information is secured from unauthorized access, modification, use, disclosure, or loss using tools such as encryption, firewalls, access controls or monitoring. Closing Period and data security are intricately linked as good financial reporting relies on the integrity and confidentiality of financial data. Implementing data security measures like encryption, access controls, and monitoring plays a vital role in safeguarding financial data, preventing unauthorized access, utilization, or disclosure, and thereby minimizing the potential for data breaches and financial fraud. Saxena (2023) identified the following benefits:

- Securing computer systems and networks from an unauthorized attack or access
- protecting individual/organizational assets and data from hackers
- Ensuring consistent integrity, completeness and quality of financial information

- Protecting personal and organizational data from manipulation or misuse
- Preserving individual and firm reputation through brand quality and reliable financial information
- Enhancing productivity through uninterrupted seamless operations (backups)
- Assists remote workspaces by securing central sources from hackers (IoT, wifi)
- Enables regulatory compliance and avoiding penalties for noncompliance
- Improves cyber posture by enabling inclusive digital protection and response
- Better data management through effective monitoring and operational efficiency
- Helps educate and train workforce on potential risks and exposures to reduce susceptibility
- Helps maintain trust and credibility through trust building amongst customers and investors
- Enables streamlining access by controlling internal and external processes so that individuals and companies can focus on other relevant tasks to establish accountability for strategic management
- Supports the IT team to keep up with evolving changes in cyberspace by equipping them with tools, techniques, and comprehensive knowledge to skillfully handle even advanced cybercrimes
- Regulatory compliance
- Cost of ignorance is high (negative costs)
- Long-run return on security investment

### **Common Cyber Security Threats Affecting Data/Financial Information**

Many organizations, businesses, individuals and even Countries in recent times, have suffered high-profile cyberattacks with devastating consequences (Gansler & Lucyshyn, 2005). These attacks have brought to fore the relevance of having strong cybersecurity systems. Some of the most common cyber threats encountered by stakeholders include:

- **Phishing:** refers to tricking users into clicking on malicious links or attachments, leading to the theft of sensitive information, such as financial data or login credentials
- **Malware:** spreading malicious software that infects computers and devices to hijack devices, steal information, or launch attacks on other systems
- **Denial-of-service attacks:** This is a type of threat that prohibits users from accessing their system or service because it has been damaged or flooded with requests or traffic thereby affecting its functionality

- **Ransomware:** installing a malware that corrupts systems or files, enabling hackers to demand a ransom to decrypt them. In some cases, sensitive data is entirely lost or worse, a complete shutdown of operations.
- **Man-in-the-middle (MitM):** Occurs when a hacker intercepts private communications between two parties by redirecting traffic to a malicious server or eavesdropping on a network connection.
- **SQL injection:** This occurs when a malicious SQL code is injected into the database by taking advantage of system weaknesses. This code takes control of systems server and modifies, views, or deletes data in the database thereby harming the system with other malicious activities.

### **Overview of Nigeria Data Protection Act (NDPA) 2023 and Cyber Security**

Following the boom in the digital economy and the widespread migration of public and private business dealings to online systems, the need to regulate and safeguard information systems and infrastructure against atrocious breaches becomes paramount. Data has assumed a crucial role in influencing decisions, prompting governments and regulators to prioritize safeguarding information, particularly containing personal data, to prevent misuse. As a result, many countries, including Nigeria, have enacted laws recognizing data protection as a fundamental human right. Nigeria's dedication to individual privacy is evident in Section 37 of its Constitution, which guarantees citizens the right to privacy. This constitutional provision forms the basis for Nigeria's legal framework on data privacy and protection.

In Nigeria, the National Information Technology Development Agency (NITDA) was the primary government body authorized by the NITDA Act (2007) to establish regulations for electronic governance before the Nigeria Data Protection Commission was established. NITDA played a crucial role in facilitating the effective exchange of data and information through electronic communication methods. In 2019, the Nigerian Data Protection Regulation (NDPR) was adopted and four years later, replaced by the Nigeria Data Protection Act, (NDPA) 2023 following the signing into law of the Nigeria Data Protection Bill, 2023 by President Tinubu. The NDPA 2023 sets the legal framework for regulating personal data in Nigeria and replaces all existing frameworks (NDPR, 2019 and NDPR Implementation Framework 2019).

The primary objectives of the Act include among others to:

- i. Protect the interests of data subjects and safeguarding their fundamental rights and freedoms in line with the 1999 Constitution
- ii. Regulate the processing of all personal data.
- iii. Encourage best practices in data processing that ensure the security of personal data as well as privacy of individuals.
- iv. Ensure the protection of the rights of data subjects by providing avenues for recourse and remedies in case of any violation of their rights
- v. Ensure that data controllers or processors carry out their responsibilities to data subjects.
- vi. Reinforce the legal structures of the national digital economy.
- vii. Ensure Nigeria participates effectively in regional and global economies through the beneficial and trusted utilization of personal data.

The NDPA 2023 focuses on data controllers and data processors who process personal data of people or entities operating in Nigeria or processors outside Nigeria that control or process personal data of Nigerian data subjects. However, the Act does not apply to the processing of personal information by individuals solely for personal or household use, as long as such processing for personal or household purposes does not infringe upon the fundamental right to privacy of the individual whose data is involved.

Moreover, the 1999 Constitution stipulates that a data controller or data processor is exempted from the Act's provisions if the processing is:

- conducted by a competent authority for the purposes of preventing, investigating, detecting, prosecuting, or adjudicating criminal offenses, executing criminal penalties, controlling national public health emergencies, or safeguarding national security;
- for public interest publications, such as journalism, education, art, or literature, to the extent that it conflicts with the obligations and rights of data subjects;
- deemed necessary for establishing, exercising, or defending legal claims in court, administrative, or out-of-court proceedings.



## Principles of Processing Personal Data

As professional accountants play an integral role in processing data for individuals, businesses and Government, it becomes necessary to understand how the NDPA 2023 Act applies to them as data processors/controllers and businesses which they serve within or outside Nigeria. The Act stipulates **six (6) major principles** to be observed by data controller and data processors when processing of personal data:

- i. Processing data should be done in a **fair, lawful, and transparent** manner where businesses/individuals clearly communicate intent, purpose and method of processing data to data subjects.
- ii. Data collection must be for **specific, clear, and lawful purposes**, and should not undergo any subsequent processing that deviates from the **initial intent**. This guideline necessitates businesses to be more meticulous and transparent in data collection
- iii. Personal data should be **sufficient, relevant, and appropriately limited for** the intended **purpose** it was obtained for. As such, individuals/companies must ensure they are focused and proactive in obtaining only essentially required information for the designated purpose, thus reducing exposure to unnecessary and sensitive data.
- iv. The **duration** for which **personal data is retained** should not exceed the time required to fulfil its lawful purposes. This requires companies to have explicit data **retention and deletion policies** where data becomes unnecessary.
- v. Data must remain **accurate, non-deceptive, and current** so businesses, have to incorporate data validation procedures and regular evaluations of stored data to sustain accuracy and completeness.
- vi. In line with the objectives of the Act, businesses/individuals must handle data in a way that guarantees **effective protection against unauthorized or unlawful processing, access, loss, destruction, damage, or breaches**. This necessitates data controllers and processors to implement strong security measures, including encryption, access controls, and other protective mechanisms, to ensure the complete security of the collected and/or processed data.

## **Key considerations for Processing of Personal Data**

### **i. Consent**

The Act requires that consent must be gained from data subjects which must be freely given, specific, informed, clear, affirmative and not based on pre-selected confirmations. The consent can be given orally, in writing or even electronically, but unambiguous. In relation to digital transactions, the Act prohibits the automation of consent resulting from automated decisions or obtaining consent from children that lack legal capacity, but have recourse to parents or guardian.

### **ii. Data Protection Impact Assessment**

The NDPA 2023 Act identifies the need for a Data Protection Impact Assessment (DPIA) process that assesses risks and impact of processing personal data. This risk management process ascertains:

- envisaged processing and its purpose
- determining the necessity and extent of the processing
- evaluating risks to the rights and freedoms of a data subject; and
- defining measures to mitigate identified risks and applicable safeguards and mechanisms for data protection.

Where the assessment indicates a high-risk potential to rights and freedoms of data subjects, data controllers must consult the NDPC before proceeding with the processing. This provision underscores the legislators' commitment to data protection and privacy rights.

### **iii. Data Protection Officers/ Data Protection Compliance Experts**

The Act provides for the appointment of data processing officers (DPO) in Nigeria equipped with requisite knowledge of data protection laws and practices who will be responsible for providing expert opinion and guidance on data protection matters to their organisation while serving as intermediary between institutions and regulators. The Act also authorizes the Nigeria Data Protection Commission to license data protection experts to monitor, audit and report on compliance to the NDPA (2023) Act for continuous regulatory oversight.

#### **iv. Rights of a Data subject**

The NDPA 2023 Act establishes the rights of data subjects in relation to access, request for and acquire insights on the processing of their personal data. This mandates data controllers to immediately respond to such request for access, and provide comprehensive details to data subjects. This underscores the need for businesses to invest in efficient data management systems adequately equipped to handle and process such requests by data subjects. In the event of any breach of the rights of a data subject by data controller or data processor, data subjects can seek redress by contest data processing, revoking their consent to access or process their personal data at any time or even initiating legal proceedings. Hence, data processors/controllers who violate any rights of data subjects, could face potential consequences such as financial penalties, civil lawsuits, or even the revocation of their licenses. There is a likelihood that these sanctions will become increasingly stringent.

#### **NDPA 2023 AND Data Security**

Part VII of the NDPA 2023 Act stipulates vital provisions regarding data security, and how fundamental it is for businesses to manage data of subjects. The Act makes data controllers/processors responsible for implementing appropriate technical and organisational measures to secure the integrity, accessibility and confidentiality of customers or data subjects' personal data. Hence, entities should implement measures to reduce potential harm to individuals in case of a breach through measures such as encryption, pseudonymization, routine risk assessments, and testing of security protocols to address emerging threats. Data controllers and processors are required to employ security measures (such as firewalls, data encryption technologies, etc.) to safeguard data against theft, cyberattacks, manipulations, environmental hazards, and similar risks.

In the event of a data breach, the Act imposes strict requirements that businesses must adhere to for addressing such incidents. For instance, data processors must promptly notify other data controller of any breach and provide necessary information to fulfill data breach obligations. Additionally, data controllers are obligated to report significant breaches that pose risks to individuals' rights and freedoms to the NDPC within 72 hours of the occurrence. When a breach is considered high risk, immediate notification to the data subjects is required. The potential

consequences of data breaches among others include damage to reputation, legal penalties, financial risks, and loss of client trust. These underscore the need for businesses to prioritize investments in robust cybersecurity infrastructure, encryption tools, data breach response plans, staff training, and awareness initiatives to cultivate a resilient data security culture within the organization.

### **NDPA 2003 Enforcement**

The Act advocates strong measures for enforcing data protection compliance within businesses through establishing a complaint system that enables data subjects to report breaches to the commission. The NDPC is empowered to investigate these complaints and initiate independent inquiries when there are suspicions of violations, aiming to ensure transparency and accountability for businesses managing personal data. Penalties for breaching the Act or subsidiary regulations differ based on the significance of the data controllers or processors. This implies that entities handling larger volumes of personal data will be held to higher standards of data protection and accountability. Specifically, the maximum fine for:

- data controller or data processor of major importance may be the greater of ₦10,000,000 and 2% of the annual gross revenue in the preceding financial year
- data controllers or processors not of major importance, the maximum fine may be the greater of ₦2,000,000 and 2% of their annual gross revenue in the preceding financial year

The penalties are stiffer than those stipulated in the NDPR 2019 which pegged the breach to 10,000 or more data subjects.

### **Challenges with the NDPA**

In order to ensure absolute compliance with the NDPA 2023, Government needs to take all measures to ensure citizens are adequately informed and enlightened about the Act. Some challenges identified by researchers that may inhibit compliance include:

- Poor Data Protection Sensitization
- Poor enlightenment of citizens
- Lack of entrenchment of Act in organizational cultures
- Enforcement of Penalties to serve as deterrent to non-compliance

## Cybersecurity planning for Organizations and Businesses

A cybersecurity plan serves as a digital shield or armour for safeguarding entities in the vast digital space. Planning is an integral step before implementation. The first step in Cybersecurity planning is risk evaluation. According to Stedman (2024) the risk assessment involves:

### 1. Risk Assessment

- **Scoping the assessment** (Identifying and prioritising the key aspects of operations to be assessed the extent of work to be undertaken)
- **Risk identification** (Identifying weak points in order to create robust defense mechanisms to shield your business)
- **Risk analysis** (vulnerabilities/weaknesses; outdated software, weak passwords, staff knowledge gap)
- **Risk evaluation and prioritization** (extent of cover versus need; data privacy, accessibility, integrity, reporting mechanisms, compliance to regulations)
- **Documentation of risk scenarios** (structure/framework)

### 2. Cybersecurity strategy details the strategy for the next 3-5 years. The process of strategy development encompasses:

- appraisal of the threat landscape
- evaluating the existing and desired levels of cybersecurity maturity
- determining actions to enhance cybersecurity, and
- documenting precise plans, policies, guidelines, and procedures.

### 3. Cybersecurity budgeting involves committing resources smartly and effectively by identifying critical areas in plans that need financial attention such as:

- Strong security software
- Staff training
- Hiring experts to ensure a safer digital environment

Good budgeting ensures there is a balance in addressing both immediate and future security needs without compromising other business objectives.

## **Cybersecurity Tips for Record Protection**

According to Scarfone (2024) a principal consultant at Scarfone Cybersecurity, best practices for cybersecurity teams or tips for entities and users for record protection are:

1. Update cybersecurity policies and practices as necessarily needed
2. Implement robust authentication methods for all users by implementing additional security measures for individuals working remotely, and reinforcing policies for safeguarding data
3. Update network security and access controls regularly to ensure their effectiveness
4. Establish readiness for security compromises and response plan in the event of breach, outlining necessary steps, roles and responsibilities, communication protocols, and coordination with relevant authorities to minimize the impact
5. Stay abreast with current security topics and technologies
6. Enhance security awareness among employees by initiating a broader cultural shift of understanding relevance of cybersecurity and the need for everyone to do their bit.
7. Regular Auditing and Monitoring by ensuring continuous monitoring and auditing system for financial data to identify potential breaches, or unauthorized access in order to respond promptly
8. Implement regular backup procedures to secure financial data in secure locations to safeguard against data loss due to unforeseen events like natural disasters or hardware failures and regular testing to ensuring data integrity.

## **Cybersecurity Risk Management**

Managing cybersecurity risks involves the identification of an organization's digital assets, the assessment of current security measures, and the implementation of solutions to either maintain effective practices or address potential security risks that could endanger a business. This continuous process of vulnerability risk management (VRM) is essential to adapt to the evolving dynamics of the organization and the external threat landscape. Vulnerability risk management (VRM) entails a continuous appraisal of every aspect of a business's operations. As new vulnerabilities are identified, patches are developed and released to rectify them. The ongoing addition of potentially susceptible devices to the network, particularly with the substantial proliferation of Internet of Things (IoT) devices and sensors in various physical locations, further accentuates the need for vigilance in this process.

## Cybersecurity Risk Management Strategy

A cybersecurity risk management strategy implements four quadrants that deliver comprehensive and continuous Digital Risk Protection (DRP). DRP platforms use multiple reconnaissance methods to find, track, and analyze threats in real time. Using both indicators of compromise (IOCs) and indicators of attack (IOAs) intelligence, a DRP solution can analyze risks and warn of attacks. Let's take a look at the four quadrants:

A cybersecurity risk management strategy seeks to provide robust Digital Risk Protection against real-time threats by focusing on four key areas or four Ms:

- ❖ **Map:** Uncover and chart all digital assets to quantify the potential points of attack and utilize the map as a basis for monitoring cybercrimes.
- ❖ **Monitor:** Explore the web for references of threats targeting your digital assets so that they can be transformed into actionable intelligence.
- ❖ **Mitigate:** Implement automated measures to obstruct and eliminate recognized threats to digital assets using a blend of integrated security initiatives.
- ❖ **Manage:** Coordinate the procedure employed in the Mapping, Monitoring, and Mitigating aspects quadrants in order to strengthen indicators of compromise (IOCs) and prioritize vulnerabilities for effective digital risk protection.

## Role of Accountants and Finance Professionals in Cybersecurity Management

Finance professionals have integral roles to play to ensure a robust cybersecurity system. Accountants are primary collectors, processors and custodians of financial data which is an irresistible target of cybercriminals. As such, they must justify the confidence reposed in them in protecting the public interest by keeping abreast with latest security solutions, understand legal frameworks within which they operate and integrate new technologies in the conduct of their assignments.

In recent times, they are not only about numbers and spreadsheets anymore but also:

- ❖ **Digital gatekeepers** who should safeguard financial data and digital assets of their organizations
- ❖ **Keep the financial health** of their organization by collaborating with other unit specialists (such as Chief Information Officer, Chief Technology Officer, Compliance and Risk Officers, Internal Audit teams, Chief Information Security Officer, HR and Operations) to deploy

cybersecurity measures that are strong digital defenders and ensuring virtual walls are solid. Each unit plays their role as interdependent parts of the system to ensure robust cyber defense.

- ❖ **Update their knowledge, skill and competence** on cybersecurity to enhance their role as professional accountants
- ❖ **Ensure financial data is complete** has integrity and inaccessible to unauthorized personnel
- ❖ **Have Open communication** with the CISO to clearly understand the financial risks and implications of data breaches, and measures available to protect data.
- ❖ **Create a cybersecurity budget** that comprehensively considers financial constraints and appropriate cybersecurity investments that balances cost and security needs.
- ❖ **Inculcate the organizational culture of cybersecurity** by communicating the financial implications of cyber threats and receiving training and resources to improve relevant cybersecurity practices.

## Key Cyber Risk Challenges

Businesses today encounter the challenge of proactively addressing potential threats before these threats exploit the system. These challenges include:

- **Lack of visibility:** Unsuspecting ransomware and phishing attacks have limited visibility. How do you resist threats that you do not even know exist? Hence the need for threat intelligence and real-time protection across several layers of security from suspected locations.
- **Prioritizing cyber risks:** Addressing the risk of cyber threats real-time in the face of resource constraint. What do you do first? To what extent? At what costs? Staying proactive in the face of changing cyber risks, business conditions, business goals, and technological updates.
- **Communicating cyber risks to the board and management:** Justifying the significance of security and how security initiatives can help in cost effectiveness, damage prevention and control as well as time savings from budget allocation.
- **Sophisticated ransomware:** The frequency and evolution of ransomware attacks is increasing steadily, requiring business leaders and IT professionals to establish a resilient



recovery plan against such threats for safeguarding their enterprises. The ongoing war between cybercriminals seeking to evade detection, and security measures striving to block threats. Rather than indiscriminately encrypting data, perpetrators are specifically targeting high-value business data for encryption and subsequent ransom demands.

- **Cloud risks:** Businesses are migrating their sensitive data from traditional data centers to the cloud due to the cost-effectiveness and flexibility. However, the transition to the cloud necessitates proper configuration and security protocols; otherwise, businesses may be susceptible to potential pitfalls especially since cloud service providers only ensure security of their own platforms. The responsibility of safeguarding a company's infrastructure on the cloud from theft and deletion rests with the company itself. Hence, management must assess their teams regarding their readiness and capability to monitor and respond to security breaches in the cloud.
- **Staff and skills shortage:** cyber risks continue to evolve in sophistication, leading to a recurring trend of excessive reliance on individual security products to fend off threats. Additionally, the digitization accompanied by shortage in dedicated cybersecurity personnel, complexity across business environment and industry has expanded the risk to even remote devices used at-home and small businesses,
- **Perpetually evolving risks:** As malware continue to evolve raising susceptibility concerns to data breaches through harmful computer software like viruses, worms, or spyware, that can alter their structure, the importance for organizations to be proactive by incorporating extra layers of protection (identify, block access and data leakage) to enhance defense systems becomes vital.

### **Factors To Consider When Evaluating Cloud Service Providers**

- **Security and Data Protection:** Organizations need to establish their data is protected against cyber threats when selecting cloud service providers. Hence, they should consider ability to provide diverse security measures such as multi-factor authentication, strong encryption, routine backups, and comprehensive disaster recovery plans as well as adherence to industry standards and regulations.
- **Scalability and Flexibility:** As businesses develop and expand, their requirements for cloud computing may vary. Hence, selecting an appropriate cloud service provider that

provides scalability and flexibility is crucial so that they accommodate demands for expanded storage and computing resources seamlessly, without causing disruptions to operations. This will enable them to customize their cloud solutions based on specific requirements.

- **Pricing and Cost-Effectiveness:** Businesses place significant importance on cost when assessing potential cloud service providers. Understanding the pricing plans and overall structure of different providers is crucial, ensuring alignment with your budget and anticipated usage (e.g. pay-as-you-go models or fixed pricing plans based on service level or storage capacity). It is advisable to compare pricing among various service providers to maximize the value derived from your investment.
- **Compliance and Regulations:** As various industries have distinct regulatory requirements, it is crucial to identify applicable regulations and compliance standards relevant to individual entities and choosing cloud service providers who possess relevant certifications and attestations, including those related to industry-specific regulations or regional laws
- **Understand Data Privacy Laws:** Verify that the cloud provider adheres to the existing data privacy laws and regulations. They should provide data protection functionalities such as encryption, access controls, and options for data residency to assist entities in meeting their objectives.
- **Data Residency and Sovereignty:** Take into account the location of your data storage. Certain regulations mandate that data must be retained within designated countries or geographic boundaries. Confirm that the provider provides data center locations that align with your data residency specifications.
- **Audit and Reporting:** Ensure the service provider offers robust audit as well as reporting capabilities so that entities can track and verify compliance with their specific requirements and regulations.
- **Data Retention and Deletion:** Organizations need to understand how cloud providers manage their data (retention and deletion) as different norms may apply but data must be disposed securely when no longer needed.

## **Conclusion**

As digital financial data security solutions evolve in sophistication and versatility, so too ransomware and other sophisticated threats emerge seeking to infiltrate these solutions. Hence, financial data security will require a continuous mesh of solutions that provide consistent detection and mitigation mechanisms backed up by swift recovery where defenses are breached. All stakeholders need to be invested in ensuring adequate solutions are implemented to safeguard financial information. It is also important to understand safety in the use of anti-spam, content filters, wireless security and anti-viruses etc., so that information integrity, accessibility, and confidentiality is adequately assured. The NDPA 2023 Act is the framework for safeguarding data in Nigeria and may evolve over time due to weaknesses, experiences and complexities since data subject protection and privacy are key concerns. Until then, stakeholders all have roles to play in ensuring data subjects privacy is safeguarded and financial data is kept confidential, secured and reliable for users of financial information to make more informed decisions.

## REFERENCES

- Cybersecurity and Internal Control (2019). University of Hawai'i Maui College  
<https://maui.hawaii.edu/wp-content/uploads/sites/13/2019/01/ACC-124-Cybersecurity-and-Internal-Control-.pdf>
- Gordon, A.L. and Loeb, P.M. (2006), Managing Cybersecurity Resources: A Cost–Benefit Analysis, McGraw Hill, New York, NY, ISBN 0-07-145285-0.
- Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Sohail, T. (2006), “The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities”, *Journal of Accounting and Public Policy*, 25(5) 503-530.
- Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2018), “Empirical evidence on the determinants of cybersecurity investments in private sector firms”, *Journal of Information Security*, 9(2) 133-153.
- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808-834.
- Islam, M.S., Farah, N. and Stafford, T.S. (2018), “Factors associated with security/cybersecurity audit by internal audit function: an international study”, *Managerial Auditing Journal*, 33(4), 377-409.
- Johnson, k., (2022). Top 7 Types of Data Security Technology. TechTarget.  
<https://www.techtarget.com/searchsecurity/feature/Top-7-types-of-data-security-technology>
- Kahyaoglu, S.B. and Caliyurt, K. (2018), “Cyber security assurance process from the internal audit perspective”, *Managerial Auditing Journal*, 33(4) 360-376.
- Kelley, K., (2023). What is Cybersecurity and Why It is Important?  
<https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security>
- Malik, A., & Ullah, K. (2019). Risk and its mitigation techniques. *Introduction to Takaful: Theory and Practice*, 45-51.
- Saxena, A., (2023). Importance of cyber security: Benefits and Disadvantages  
<https://sprinto.com/blog/importance-of-cyber-security/>
- Udi, A., (2023). SMEs in Nigeria were major victims of cyber-attacks in 2022 – CSEAN.  
<https://nairametrics.com/2023/07/12/smes-in-nigeria-were-major-victims-of-cyber-attacks-in-2022-csea/>