Deloitte.

Nigeria Cybersecurity Outlook 2024

MAKING AN IMPACT THAT MATTERS since 1845

January 2024

Introduction

The year 2023 was significant for Nigeria with the conduct of the general elections. Beyond the fact that it was an election year, it was also characterized by several high-profile cyber incidents ranging from ransomware attacks, third-party attacks, phishing attacks, and insider-enabled attacks. As predicted, there was a high spate of cyber-attacks during the elections, as stated by the Minister of Communications and Digital Economy.

Given the current economic situation in the country, we anticipate more attacks to occur in 2024 if organizations fail to take the right measures to address cybersecurity gaps in their processes, people, and technology infrastructure. This article delves into the key cybersecurity predictions for Nigeria in 2024 and will equip you with insights to navigate the evolving threat landscape and build resilience against potential attacks.

The following are some of the events we anticipate will happen in 2024:

1 Integration between Cloud and on-premise defense

As cloud adoption increases with more sensitive services being migrated to the Cloud, the delineation between "on-premise" and "cloud" infrastructure is gradually fading away. Traditionally, the protection mechanisms in both cloud and on-premises infrastructure exist in silos and are managed independently of each other. We will see a drive towards a more holistic approach to security defense (Cloud and On-premise). This will result in integrated security solutions being deployed to create a single experience for users.

Consequently, organizations will begin to employ a combined approach to manage security between the cloud infrastructure and on-premises infrastructure.

This integrated approach may lead to an increased complexity in configuration, monitoring, and maintenance, potentially creating more points of failure or misconfiguration. Compatibility issues between legacy on-premise infrastructure and cloud systems could impact security, and organizations may require additional skills to manage this new approach. Organizations will need to expand their cybersecurity strategy beyond traditional infrastructure to encompass the cloud and mitigate potential threats effectively. A comprehensive security strategy that encompasses both on-premise and cloud environments will be crucial for effective cyber risk management.

2 Economic Downturn and Heightened Insider Threat

The recent economic situation in the country caused by the high exchange rates, inflation, and low disposable income will present unique cybersecurity challenges in Nigeria. We envisage that if the economic situation continues, the hardship may incentivize disgruntled employees to engage in malicious activities for financial gain. Insider-supported attacks may increase astronomically due to the quest to make money, leading to an increase in cyber-related financial crimes.

The increase in internal-external collusion will pose significant risks to both small and large enterprises, increasing the likelihood of data breaches, unauthorised access, and other malicious activities.

On the other hand, the exchange rate debacle would increase product and license costs and may push organisations to start exploring alternative and cheaper solutions/services which may not necessarily address their risk exposure. Some may even deprioritise cybersecurity investments and divert the funds to other areas of the business. This could expose them to significant risks.

Organisations must proactively address insider threats by implementing robust security measures such as making user access more stringent and continued monitoring and analysis of the activities and behaviours of users, applications, servers, and computers on the network. They also need to develop strategies to optimise existing security investments while ensuring they are adapting to the changing threat landscape to mitigate the growing attacks. Investments in security should be done not from a reactive (knee-jerk) approach but from a well-thought-through strategic standpoint that would support the business objectives.

3 Escalation of Ransomware Attacks

Ransomware attacks will continue to evolve in scale and complexity, leveraging Artificial Intelligence (AI) and Machine Learning (ML) to evade detection by traditional security tools. Ransomware actors will continue targeting critical infrastructure such as financial institutions, healthcare, and government, leading to disruptions and higher demands for ransom payments.

The economic and societal impact of ransomware attacks will intensify, underscoring the need for organisations to implement comprehensive cybersecurity measures. This includes robust backup and recovery strategies, employee training, and collaboration with law enforcement agencies to combat increasingly sophisticated ransomware threats.

4 5G Network Exploitation

The widespread adoption of 5G networks will unlock new possibilities for faster connectivity and also introduce new cyber exploitation opportunities. We will see a rise in the adoption of emerging technologies like smart homes, connected cars, and connected personal devices. On the flip side, with the proliferation of 5G technologies, malicious persons will have a faster means of conducting attacks. There will be an increase of denial of service attacks due to the increased connection speed offered by the 5G technology. Similarly, data exfiltration will be made faster, thereby shortening the time it will take to complete a data breach.

Organisations will need to fortify their networks against potential threats exploiting the increased bandwidth and connection speed. There will be a need to collaborate and develop cyber security strategies that will address the unique challenges posed by 5G networks, including the potential for increased attack vectors.

5 Adoption of Zero Trust Security Models

With the increase in insider threats and constant compromise of user account credentials, organisations will adopt “zero trust” security models. Many organisations will move away from traditional perimeter-based security and seek to achieve micro-segmentation within the network to reduce risk and exposure. Continuous authentication and strict access controls will become foundational principles. Zero trust will move from being a buzzword to becoming a business priority due to increased insider threat.

The implementation of zero trust models will enhance the overall security posture, reducing the risk of unauthorised access and lateral movement within networks. However, organisations will need to invest in advanced identity and access management solutions and educate employees on the principles of zero-trust security.

6 Cybersecurity Representation at Board Level

As cybersecurity risks continue to be a major business concern, organisations and regulators will prioritise the inclusion of dedicated cybersecurity experts as board members.

The presence of cybersecurity-focused board members will ensure that decisions taken at the highest level provide a robust cybersecurity steer, creating a proactive approach to safeguarding organisational assets and maintaining stakeholder trust.

7 Partnership Against Cybercrime

There will be an increased drive towards industry collaboration and the establishment of centralized incident reporting and response capabilities both at private, state, national, and international levels to facilitate information sharing to combat cyber crimes. The partnership will bring together coordinated and concerted efforts towards information sharing. This objective will be driven by the need to form a guided coalition to combat Cybercrime by sharing relevant and timely information among stakeholders to help in the detection and quick response to threats to reduce the incidents of Cybercrimes.

8 Cybersecurity Inexperience

As the wind of emigration becomes more boisterous, it will continue to cause a deep cut in the number of skilled cybersecurity specialists available for employment in Nigeria. The ISC2 Cybersecurity Workforce Study 2023 currently estimates the global cybersecurity workforce gap to be approximately 4 million. As more organisations face a shortage of experienced cybersecurity professionals, there will be an increased risk of reliance on practitioners who do not have adequate levels of experience to manage the security of their organisations.

This may result in increased numbers of successful cyber attacks and slower incident response/detection rates. Some malicious persons can also capitalize on the dire need for resources and implant themselves in organisations to perpetuate their activities.

Organisations need to up their ante regarding screening of potential employees, especially those that would handle sensitive functions; they also need to verify the real identity of the individuals they are dealing with and ensure controls are in place to implement zero trust. There is also the need for more investment in training/skill development to shorten the learning curve and enable new employees to adapt quickly. Other strategies like co-sourcing will be important to bridge short-medium term skill gaps.

Conclusion

As the business and threat landscape continues to evolve, organisations must stay atop to address rising cybersecurity concerns. Both small and large corporations are subject to cyber attacks, and organisations that fail to prioritise cyber protection will be forced to battle their reputation and finances when the risk crystallises. Establishing a good security culture, prioritising security investments, revising security strategy, and implementing the right controls are some of the strategies forward-looking organisations should put in place to reduce the risk of cyber-attacks and consequently minimise business disruptions.

Cybersecurity has become a major business imperative and must be discussed at the highest levels within the organisation to ensure the preservation of shareholders' value. Enjoy a safe 2024

Contacts

Tope Aladenusi

Risk Advisory Leader,
Deloitte West Africa
+234 1 9041730
taladenusi@deloitte.com.ng

Funmilola Odumuboni

Partner, Cyber Risk Services,
Deloitte West Africa
+234 19041882
fodumuboni@deloitte.com.ng

www.facebook.com/DeloitteNigeria www.twitter.com/DeloitteNigeria