Deloitte.

Nigeria Cybersecurity Outlook 2022

January 2022

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

The year 2021 was exciting in the cybersecurity space both locally and internationally. Cyber breaches and attacks were experienced in the economy's public, private, financial, and non-financial sectors. A significant trend was that no organisation appeared immune to cyber-attacks. Even Financial Institutions that had made significant investments in cybersecurity experienced high-profile attacks. This may have been due to some predictions in the Nigeria Cyber Outlook that we released in January 2021. It was noted that there would be a spotlight on Nigeria, and attackers would have more tools, skills, and ground to play. See Nigeria Cyber Outlook 2021 for more details. In addition, 2021 saw an increase in cybersecurity regulations across different sectors.

We envisage that the Nigeria Cybersecurity Landscape in 2022 would be interesting for both sides of the divide (i.e., the threat actors and the "defenders"). Organisations would need to re-strategise to catch up and protect themselves. Some of the specific events we are likely to witness include:

Paid Collaboration between Insiders and Threat Actors will Surge

According to Threat Post and Krebs reports, in 2021, cybersecurity threat actors advertised profit-sharing incentives for company employees willing to help them distribute malicious software within their organisations. In Nigeria specifically, these threat actors sent out an open communique to employees willing to cause their organisations harm.

While it is difficult to establish if any employee took up the offer in 2021, we envisage that this would be a major area of concern. There could be a surge in cyber-attacks if there is a successful collaboration between external threat actors and malicious insiders/employees. It may also be challenging to detect such instances since the attackers use valid credentials/access to perform their activities.
Organisations can stall this by ensuring that their systems are configured to keep logs of activities. These logs should be stored locally and remotely to prevent tampering. Organisations should also invest in mechanisms that perform 24/7 monitoring of the logs to detect quickly when malicious activities happen. Improving the working conditions and performing cybersecurity awareness for employees may also help keep employees motivated while informing them of the tactics of the malicious attackers.

Third-Party Risks to Become a Front Burner Issue in Managing Cybersecurity

Today's businesses operate globally, and many business processes are powered by technology. To remain relevant in business and continue to deliver services that meet customers' needs, companies are beginning to explore local and international partnerships. They seek to leverage these platforms to provide innovative technology solutions to customers. While this would create more business value, there is also the risk of being exposed, especially when connecting to a third party with low cybersecurity hygiene practices.

Last year, cybercriminals exploited the Accellion file transfer appliance, allowing enterprises to transfer large files. They had access to private information such as Social Security Number (SSN) and banking information. Nigeria was not left out; we witnessed cases where unprotected technology interfaces between companies were used to perpetrate fraud and divulge sensitive customer information.

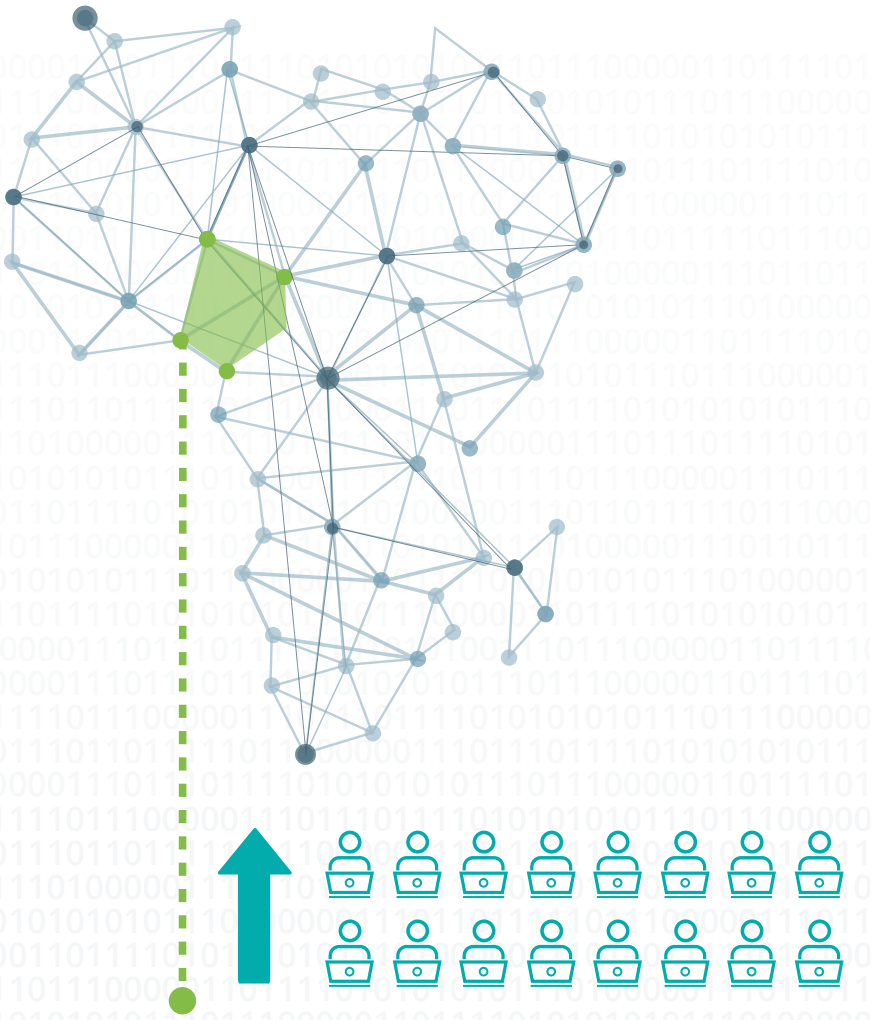
As partnerships among businesses increase in 2022 and beyond, we envision that Third-Party Risks will be one of the items on the front burner for many organisations in Nigeria when planning on how to manage cybersecurity. To properly manage the risks associated with third parties, organisations should consider business continuity, interface security and integrity, personnel security, and information security hygiene.

To remain relevant in business, companies are beginning to explore local and international partnerships.

Cyber Insurance to Gain Popularity

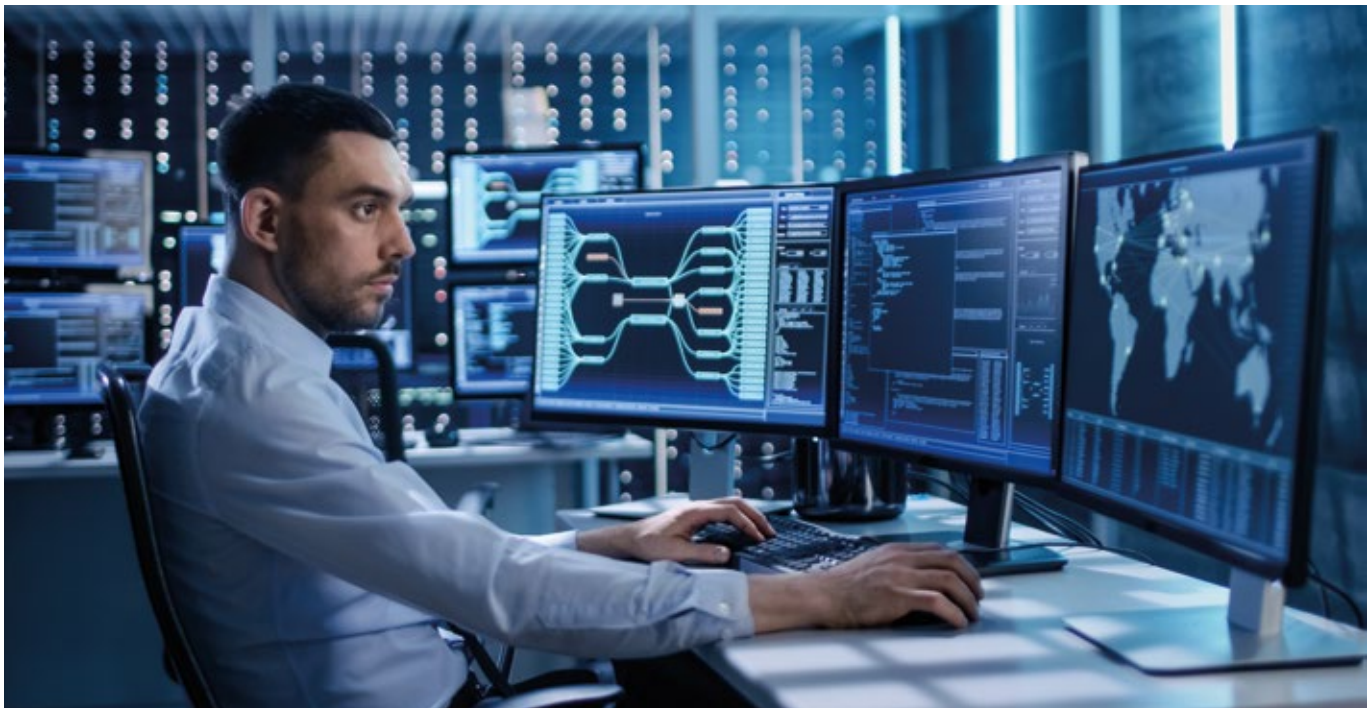
It is no longer news that cybercrime is increasing in Nigeria, even though some of these crimes go unreported. Nigeria was ranked 16th among the countries most affected by internet crime in the world in 2020, according to the Federal Bureau of Investigation (FBI) in its 2020 internet crime report. These crimes come with associated costs to organisations. In 2021, the Special Fraud Unit (SFU) of the Nigerian Police Force (NPF) arrested a man for allegedly hacking into the server of a Nigerian bank to steal N1.87 billion.

Given the increasing rate of cybercrimes and attendant losses, several organisations have started looking at cyber insurance as a means to manage the risks and losses due to cybercrime. Cyber Insurance is an insurance policy that covers financial losses resulting from data breaches and other cyber-attacks. We expect more companies in the Nigerian insurance space to partner with foreign counterparts to deliver cyber insurance products to organisations in Nigeria.



Cybercrime is increasing in Nigeria. The country was ranked 16th among the countries most affected by internet crime in the world in 2020

Increased Focus and Investment in Incident Response



Obtaining the right skills and tools to respond to cyber incidents is critical to help significantly reduce response time and attendant losses. Many organisations are now exploring automated mechanisms for incident response; this is in addition to obtaining the right skills and training for their team.

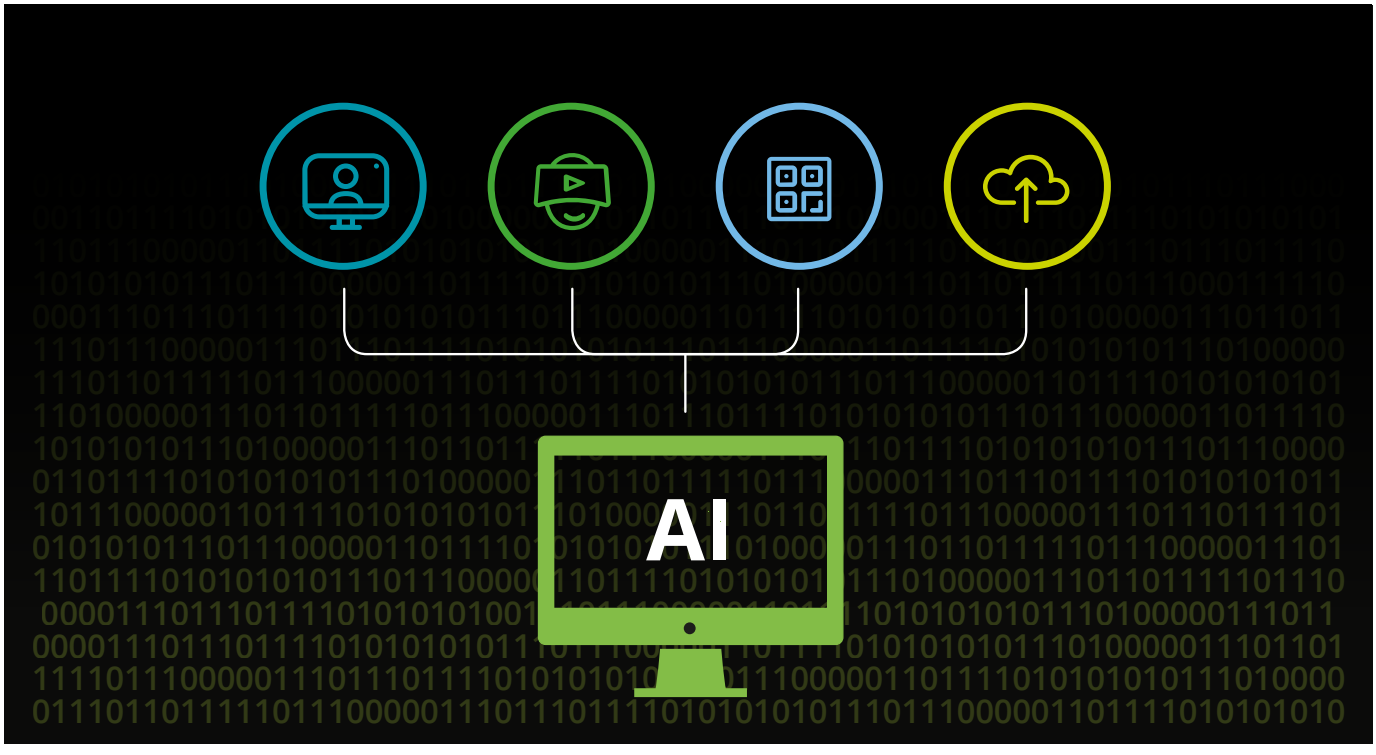
This year, we envisage that there will be a significant increase in focus/investment in detection and response capabilities. Since the attacks would be more, it would be better to ensure the right tools and skills to respond and contain those attacks are in place.

Artificial Intelligence (AI) Fused Cybersecurity Solutions to Become More Popular

Cyber-attacks are becoming more sophisticated, and organisations are struggling to keep up with this level of sophistication. Cybercriminals use Artificial Intelligence (AI) and Machine Learning (ML) to break through the defences set up by organisations; hence, organisations need to utilise the same or higher techniques to combat them effectively.

AI and ML are being leveraged in cybersecurity to quickly analyse millions of events and identify different types of threats. Organisations also use tools that leverage AI and ML to support their cybersecurity team. For example, Security Orchestration Automation and Response (SOAR) tools are used by organisations to automatically correlate information from different sources and interact with security tools to remediate incidents with minimal human intervention. With the aid of sophisticated algorithms, AI systems are being trained to detect malicious software, run pattern recognition, and detect malware before they enter the network (e.g. via email).

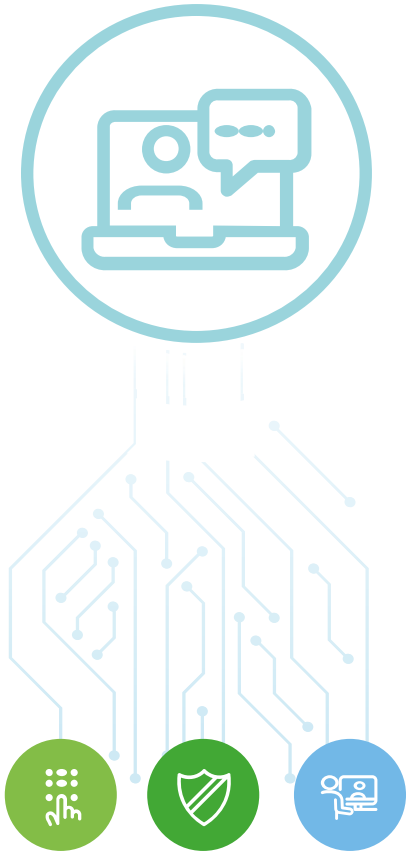
Organisations will invest more in security solutions with artificial intelligence capabilities to keep up with the fast-changing threat landscape and ensure proactivity in cybersecurity operations. Some of the considerations to look at when adopting AI-enabled solutions include the global acceptability and usability of the solution, the need to maintain privacy while consuming different types of data and the skill level of professionals required to implement the solution.



Increased Focus on Application Programming Interface (API) Management and Security

There has been a proliferation of APIs across many organisations, and many were deployed in response to the growing demands of customers. However, in most cases, good API management and security practices were not followed during the design and development of the APIs. Many APIs were implemented without authentication, giving unauthorised access to sensitive data and breaching privacy requirements. In addition, many organisations had APIs exposed to the internet without encryption, allowing for theft of sensitive data through the internet. With this, there is likely to be an increase in API related attacks, especially ones that leak Personal Identifiable Information (PII). Organisations that are victims of these attacks would also need to contend with the Nigerian Data Protection Regulation (NDPR) dictates.

To address this risk, organisations would need to step back to perform some housekeeping activities such as API inventory, API documentation, security testing of APIs, code review, Web Application Firewall integration and API Distributed Denial of Service (DDoS) protection.



A New Wave of Cyberactivism in the Wake of the Upcoming Elections

Digital activism has transformed cybersecurity in the last two decades. Smartphones and the internet have changed the way political events, protests and movements are organised, helping to mobilise thousands of new supporters to a diverse range of causes. Digital activism has become more prominent in this era, with social media being its primary weapon. This could be attributed to the fact that many have considered social media a relatively safer and quicker space to run campaigns and protests, as there is a large base of internet users. In the last decade, Nigeria recorded several notable digital activisms via social media, such as the #BringBackOurGirls and the #ENDSARS movement of 2020 which raged across the world with nearly 30 million tweets in 48 hours. It is noteworthy that even the popular nationwide movement of 2012, "Occupy Nigeria", was greatly inspired by social media.

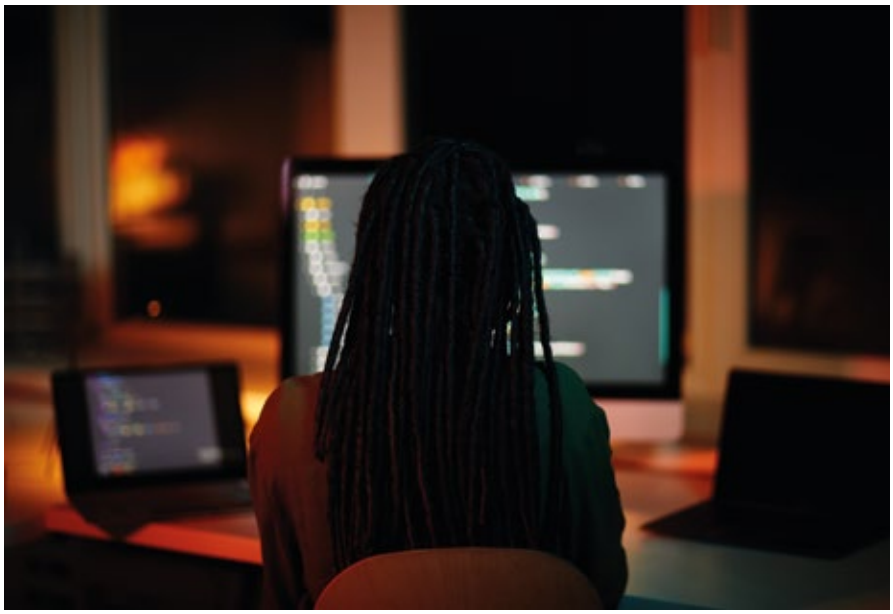
From BringBackOurGirls to NigeriaDecides in 2015, NigeriaDecides2019 in 2019, RevolutionNow and BuhariMustGo in the last quarter of 2021, it is apparent that this has been the paradigm during election periods in this past decade. Towards the end of 2022, this new wave of digital activism will become apparent and significant. In addition to social media activism, the Government and public institutions are likely to face cyber-attacks from hacktivists groups, mainly consisting of disgruntled Nigerian youths geared towards making loud statements against the current socio-economic issues they currently face, as in the case of the ENDSARS.

Likewise, just like in the US elections in 2020, where a lot of fake news were published to discredit the two leading contenders, we envisage a spike in the number of fake social media accounts that would be opened to propagate misinformation. The Nigerian Government would have to take case studies from the experiences of the US and other countries.

As we approach the 2023 elections, we can expect to see a new wave of various socio-political movements and hacktivism, and we expect public institutions to improve their cybersecurity posture in preparation for these.

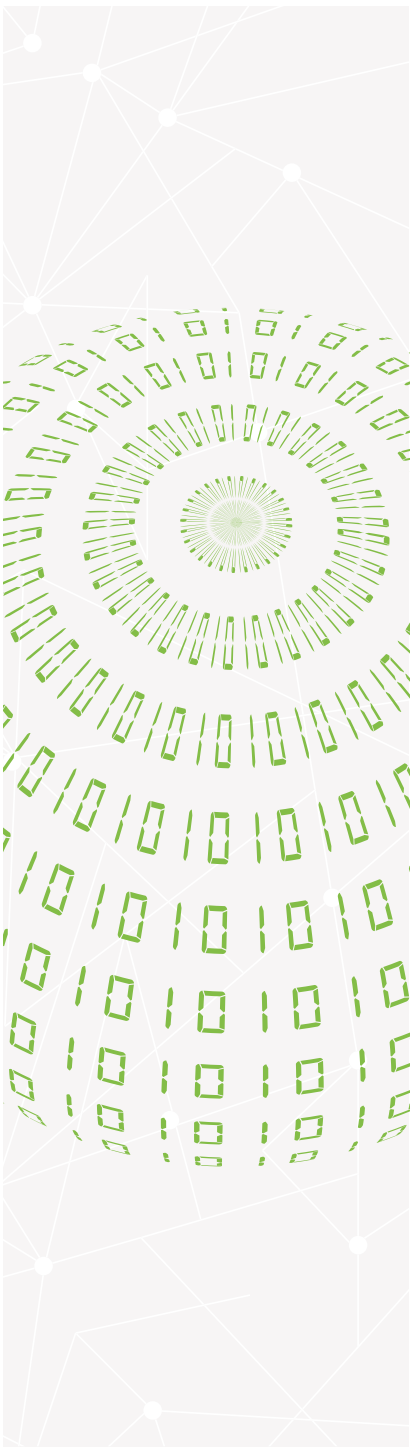
> Digital activism has become more prominent in this era, with social media being its primary weapon

Deepfake: Closer Home than You Think



Over the past few months and as predicted in our 2021 cybersecurity outlook, there has been a rise in the cases of deepfake manipulations where celebrities are seen in scandals only to realise they were never in the video or politicians are making inciting statements when they never said those words. Deepfakes are hyper-realistic, manipulated digital elements such as sounds, videos, and photos generated using artificial intelligence and machine learning tools. The technology supporting deepfakes are also improving, making it more difficult to detect them. In the past year, we have had cases of misinformation in Nigeria, from that of the presidency to the recent controversial revivalist popularly known as "Mummy GO". This goes to show that deepfake is closer home than we thought. In 2022, we expect to see more classic cases of deepfake manipulations, especially in the country's political space.

As the country prepares for the elections in 2023, we need to pay attention to the things we see, hear, and watch to ensure they have not been produced using deepfake technologies. Always ensure you get your information from trusted news sources and corroborate the information you receive with multiple trusted sources.



Conclusion

2022 is not a year to live in denial regarding the impact of cybersecurity on your businesses or organisations, as no organisation is too small or too big to be attacked. Organisations would need to invest unilaterally across their people, processes, and technology to stay afloat. Any area among the above found wanting/lacking proper attention would render other efforts useless. There is also the major mind shift from “defence-only” to “detect and respond”.

Wishing you a cyber-secure 2022!

Tope Aladenusi

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

Funmilola Odumuboni

Associate Director Risk Advisory,
Deloitte West Africa
+234 19041882
fodumuboni@deloitte.com.ng

Deloitte Nigeria