Nigeria Cyber Security Outlook 2020 –
The Year of Shifts

January 2020
Welcome to 2020, the beginning of a new decade that will witness unprecedented cyber-attacks and cyber security solutions. We have named it the “year of shifts”, as we expect significant changes in cybercrime and counter-measures. We also expect “cyber” to be one of the top news headlines throughout this decade in Nigeria and across the globe.

In our 2019 Cyber Security Outlook we made a number of predictions that came to pass. For the year 2020, we envisage a number of shifts that will affect the Nigerian Cyberspace – shifts in attack targets; attack magnitude; identification and authentication; monitoring; awareness and education; regulatory oversight; collaboration; and a shift in the way organisations deal with cyber-attacks.
Shift in
Attack target

Many attacks in 2020 will move from big “well prepared” organisations to the seemingly unlikely targets, especially companies who are of the notion that they are not prone to cyber-attacks or do not have enough resources to attract any attack. The main targets for cyber-attackers will be the cloud-based systems, user mobile devices, IOTs and Small & Medium Enterprises (SMEs) as well as organisations in the non-financial sector. Organisations with cloud based infrastructure will be exposed due to misconfigured cloud-infrastructures, mobile devices will be exposed to more sophisticated phishing attacks that could convince even the most security conscious individuals and lastly, SMEs will be exposed due to their unpreparedness. 2020 will also see organizations liable to exposure through unprotected third party vendors and suppliers.

Shift in
Attack Magnitude:

Organizations in Nigeria are becoming more cyber security conscious through the implementation of protective and security monitoring mechanisms. This has led to organizations becoming more successful at detecting and responding to attacks and breaches within the shortest possible times. Despite the efforts of organizations, cyber-attacks are becoming more focused. There are indications from reports of the Nigerian Interbank Settlement Scheme (NIBSS) that mobile fraud cases would likely rise above those of automated teller machines (ATM) by 2020. 2019 saw fewer successful attacks but resulted in higher losses and impact on the affected organizations. Phishing and Business Email Compromise (BEC) were the most common and successful as they prey on human emotions and give rise to higher profits for the attackers. The year 2020 will likely witness a sharp rise in this trend. Organizations will need to be proactive to stay ahead of the attackers.
Shift of identification and authentication:

With the recent data breaches happening globally, compromised passwords obtained via credential harvesting is the leading cause of data breaches. Obtaining user credentials is one of the easiest ways to gain access to a system, so it stands to reason that attackers will try and exploit the path of least resistance. Human error also contributes to a huge amount of security breaches.

In 2020, more organizations will move towards the “Zero Trust” security model, where security strategy begins with: Never trust, always verify. Zero trust architecture ensures that data and access across the network are secure and based on parameters like user identity and location. It inspects and logs all traffic, learns and monitors network patterns, and adds authentication methods into the security mix, all with the goal of seeing every user and device connected to the network at any moment. There will also be a rise in the adoption of biometric technologies for authentication and identification in computer systems, ATM machines and physical access controls.

Shift in monitoring:

In 2019, organisations took strategic decisions by implementing or subscribing to Security Operation Centres to monitor and defend their firms from existing and emerging threats. Consequently, we saw a rise in cyber threat monitoring services which has helped many organisations secure their most priced data.

Time is crucial when protecting an organisation’s assets from cyber threats and attack elements as it is important for the security measures to work fast to keep pace with the hackers and cybersecurity threats. Safeguarding data is critical for businesses and so they require faster detection, response and recovery from imminent threats.

Artificial Intelligence (AI) and machine learning is now an effective tool in threat monitoring to gain serious advantage against fraudsters and hackers. In 2020, Cyber threat monitoring and intelligence would take a new direction as many organisations (outside the banks) will begin to rely on AI and machine learning monitoring to help uncover attacks before they happen.
Shift in awareness and education:

2020 will see a shift in security awareness thereby creating more impact which will ultimately protect the populace. We will see more local, grassroots, pidgin and native language awareness to reach low income users or targets. We will also see security awareness that is adaptable to the user’s lifestyle instead of the generic traditional awareness mechanism. Cyber Security will also be included in the curriculum of schools as a way to increase awareness and develop the scarce skills around cyber security.

Shift in regulatory oversight:

2019 witnessed an increase in the number and sophistication of data breaches which has been a continuous trend for the past decade. This trend has led to increased regulatory oversight initiatives across the world with prominent examples like the Nigerian data protection regulation, General data protection regulation, Asia pacific data protection and cyber security guide, German’s IT security act of 2015 amongst many more.

2020 will see many regulators including government agencies release guidelines around Cyber Security, with new focus on data privacy. We already have the Nigeria Data Protection Regulation (NDPR) released by NITDA and The Central Bank of Nigeria will soon be releasing more guidelines for Fintechs and banks during the course of the year with strict penalties attached for non-compliance. We also expect better enforcements of the existing cyber security and data protection regulations.
Shift in collaboration:

Historically, government establishments in the country have worked in silos, with each establishment fully responsible for all its security operations. Due to recent events, it is evident now more than ever that collaboration is needed in the security landscape most especially in the threat intelligence front. The expansion of cyber threat intelligence (CTI) all over the world is largely credited to information sharing and establishments in Nigeria will begin to embrace this idea. Cyber Threat alliance is an important factor for the advancement of security operations. It has become obvious that the wider the scope and insights into threats that can be created, processed and shared across these organizations, the easier it becomes for new and emerging threats to be identified and promptly mitigated. As a result of the benefits associated with cyber threat alliance, 2020 will see collaborations between regulators, private organizations, government parastatals, security agencies, as well as collaboration among countries.

Shift in bearing the Consequences:

As the cyber insurance market is fast becoming a common tool for risk management, the cybersecurity insurance market is predicted to reach an astounding mark of $7.5 billion in the year 2020 as reported by Tripwire. Organizations will start to push for cyber insurance as a means to safeguard against the implications of a cyber-breach. Though cyber insurance as a product has been around for a long period of time, it has certainly not yet matured. 2020 will see an increase in organizations in Nigeria exploring cyber insurance as against focusing efforts solely on preventive measures for detecting and blocking potential attacks as well as practices around disaster recovery to enable appropriate response. Insurance cover will include but not limited to cyber-attacks, data breaches and other incidents that affect third parties or supply chains.
Conclusion

As the past decade has proven, attackers are willing to explore known and unknown tactics to exploit organisations. By combining the cyber security lessons and practices from the past decade, we can develop better strategies for the next decade of cyber defence.

While we have focused on some shifts and changes that can cyber-secure our 2020, we must prepare our environment for adaptation. This involves adaptation to new cyber security regulations, adaptations to new attack vectors, and most importantly adaptation to collaboration between technologies, processes and intelligence. As always, we wish you a Cyber Secure 2020

Tope Aladenusi
Cyber Risk Services Leader,
Deloitte West Africa

+234 1 9041730
taladenusi@deloitte.com.ng