SERIANU

Nigeria Cyber Security Report 2017

Demystifying Africa's Cyber Security Poverty Line

United States International University-Africa

ISACA
Trust in, and value from, information systems
Lagos Chapter

DEMADIUR

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

The **Africa Cyber Immersion Centre** is a state-of-the-art research, innovation and training facility that seeks to address Africa's ongoing and long-term future needs through unique education, training, research, and practical applications.

For more information contact:

Serianu Limited
info@serianu.com • http://www.serianu.com

Content

Editor's Note and Acknowledgement

We are extremely pleased to publish the 2nd Edition of the Nigeria Cyber Security Report. This report contains content from a variety of sources and covers highly critical topics in Cyber intelligence, Cyber security trends, industry risk ranking as well as home security.

Over the last 5 years, we have consistently strived to demystify the state of Cyber security in Africa. In this edition themed **Demystifying Africa's Cyber Security Poverty Line**, we take a deeper look at the financial limitations impacting many Nigerian organisations. Our research is broken down into the following key areas:

Top Trends: We analysed incidents that occurred in 2017 and compiled a list of top trends that had a huge impact on the economic and social well-being of organisations and Nigerian citizens. This section provides an in-depth analysis of these trends.

Cyber Intelligence: This section highlights various Cyber-attacks, technical methodologies, tools, and tactics that attackers leverage to compromise organisations. The compromise statistics and indicators provided in this section empower organisations to develop a proactive Cyber security posture and bolster overall risk.

Survey Analysis: This section analyses the responses we received from over 700 organisations surveyed across Africa. It measures the challenges facing Nigerian organisations, including low Cyber security budgets and inadequate security impact awareness that eventually translates to limited capabilities to anticipate, detect, respond and contain threats.

Cost of Cyber Crime Analysis: Here we closely examine the cost of Cybercrime in Nigerian organisations and in particular, to gain a better appreciation of the costs to the local economy. We provide an estimate of this cost, which includes direct damage plus post-attack disruption to the normal course of business.

Sector Risk Ranking: The risk appetite for organisations varies. In this section, we rank different sectors based on their risk appetite, number of previous attacks reported, likelihood and impact of a successful attack.

Anatomy of a Cyber Heist: This section provides a wealth of intelligence about how Cybercriminals operate, from reconnaissance, gaining access, attacking and covering their tracks. This section is tailored to assist Security managers identify pain points within the organisation.

Home Security: In light of the increased residential internet penetration, smart phone use and cases of Cyber bullying, it has become necessary to raise awareness on Cyber security matters at a non-corporate level. This section highlights key challenges in the modern smart home and sheds light on the growing issue of Cyber bullying.

Africa Cyber Security Framework (ACSF): In order to assist businesses in Africa, especially SMEs, we developed the Africa Cyber Security Framework (ACSF). This section highlights the four (4) key domains of ACSF which serves to help businesses identify and prioritize specific risks plus steps that can be taken to address these risks in a cost effective manner.

Brencil Kaimba
Editor-in-chief

What can our readers look forward to in this report?

THIS REPORT GIVES INSIGHTFUL ANALYSIS OF CYBER SECURITY ISSUES, TRENDS AND THREATS IN AFRICA. ITS SECTIONS ARE WELL RESEARCHED AND STRUCTURED TO CATER FOR THE NEEDS OF ALL ORGANISATIONAL STAFF INCLUDING BOARD DIRECTORS. THE ANATOMY OF A CYBER-HEIST WAS COMPILED WITH SECURITY IMPLEMENTERS AND FORENSIC INVESTIGATORS IN MIND WHILE THE TOP PRIORITIES SECTION CATERS FOR DIRECTORS AND SENIOR EXECUTIVES.

We have also highlighted other social issues such as home security that plays an important role away from the corporate standpoint.

Appreciation

In developing the Nigeria Cyber Security Report 2017, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;

We partnered with Demadiur Systems Limited, a servicing company founded to focus on providing innovative telecommunication and engineering services to the African Continent. Demadiur provided immense support through research and provision of statistics, survey responses, local intelligence on top issues and trends highlighted in the report.

The USIU's Centre for Informatics Research and Innovation (CIRI) at the School of Science and Technology has been our key research partner. They provided the necessary facilities, research analysts and technical resources to carry out the extensive work that made this report possible.

The ISACA-Lagos Chapter provided immense support through its network of members spread across the country. Key statistics, survey responses, local intelligence on top issues and trends highlighted in the report were as a result of our interaction with ISACA-Lagos chapter members.

The Serianu CyberThreat Intelligence Team

We would like to single out individuals who worked tirelessly and put in long hours to deliver the document.

Keston Agboro - Demadiur - Researcher, Cyber Attacks and Trends
Ikenna Azorji – Demadiur – Researcher, Cyber Attacks and Trends
Beatrice Inkoom - Demadiur - Researcher Survey
Babatunde Olaleke - EPPAN - Researcher Survey
Lucy Akokoku - EPPAB - Researcher Survey
Martin Ekpeke – IT Pulse – Researcher, Survey
Barbara Munyendo – Researcher, Cyber Intelligence
Kevin Kimani – Researcher, Anatomy of a Cyber Heist
George Kiio – Researcher, Home Security Researcher
Margaret Ndung'u – Data Analyst
Morris Ndung'u – Data Analyst
Mark Muema – Data Analyst
Nabihah Rishad – Line Editor

USIU Team

Ms. Paula Musuva Kigen
Folarin Adefemi Isaac
Zamzam Hassan
Gaurav Bhatnagar

Commentaries

Engr. Haru Al Hassan
Director, New Media and Information Security Department,
Nigeria Communications Commission (NCC)

Ibrahim Lamorde
Commissioner of Police,
Police Special Fraud Unit, Lagos

Olusola Teniola
President,
Association of Telecommunications Operating Companies of Nigeria (ATCON)

Onajite Regha
Chief Executive Officer,
Electronic Payment Association of Nigeria (E-PPAN)

Abiodun Aderoju
Chief Inspector of Internal Audit and Deputy General Manager,
Sterling Bank Plc

Ben Roberts
Chief Technical Officer,
Liquid Telecom Group

Babatunde Ajiboye
Manager, Governor's Department,
Central Bank of Nigeria, Headquarters, Abuja

Sunday Folayan
President,
Nigeria Internet Registration Agency (NiRA)

Dr. Peter Tobin
Privacy and Compliance Expert,
BDO Consulting, Mauritius

Joseph Mathenge
Chief Operational Officer,
Serianu Limited

Olufemi Ake
Country Manager, Nigeria | Ghana
ESET

Abdul-Hakeem Ajijola
Chairman,
Consultancy Support Services Limited

Akinpelu Oluleke
Manager, Cybersecurity Engineering,
FirstBank Nigeria

Oluseyi Akindeinde
Chief Technology Officer, Digital Encode

Building Data Partnerships

In an effort to enrich the data we are collecting, Serianu continues to build corporate relationships with like-minded institutions. Recently, we partnered with The Honeynet Project ™ and other global Cyber intelligence organisations that share our vision to strengthen the continental resilience to cyber threats and attacks. As a result, Serianu has a regular pulse feeds on malicious activity into and across the continent. Through these collaborative efforts and using our Intelligent Analysis Engine, we are able to anticipate, detect and identify new and emerging threats. The analysis engine enables us identify new patterns and trends in the Cyber threat sphere that are unique to Nigeria.

Our new Serianu CyberThreat Command Centre (SC^3) Initiative serves as an excellent platform in our mission to improve the state of Cyber security in Africa. It opens up collaborative opportunities for Cyber security projects in academia, industrial, commercial and government institutions.

For details on how to become a partner and how your organisation or institution can benefit from this initiative, email us at **info@serianu.com**

Design, layout and production: Tonn Kriation

Disclaimer

The views and opinions expressed in this report are those of the authors and do not necessarily reflect the official position of any specific organisation or government.

As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers should therefore also rely on their own experience and knowledge in evaluating and using any information described herein.

For more information contact:

Demadiur Systems Limited
8A Saka Tinubu Street,
Victoria Island, Lagos, Nigeria

Tel: +234 803 347 1283

contact@demadiur.com | www.demadiur.com | www.serianu.com

Foreword

FORTIFYING THE HOME FRONT – NEED FOR LOCAL EXPERTISE IN CURBING CYBER SECURITY THREATS

Ikechukwu Nnamani

President
Demadiur Systems Limited;

Board Member
Nigerian Internet Registration Agency (NIRA);

Board Member
Association of Telecommunications Companies of Nigeria (ATCON)

As the world gets more connected and the digital divide that has long separated Nigeria from other technologically more advanced countries are gradually bridge, the possibility of a major cyber attack within Nigeria, crippling the critical national infrastructure becomes more apparent. Nigeria cannot be isolated from the current global cyber threat facing the rest of the world. From electioneering infrastructure, financial institutions, power systems, manufacturing systems, telecommunications networks, to the media and entertainment industry, no sector is spared from the current cyber security threats.

One glaring fact from the most recent global cyber attacks is that each country and region must be able to defend themselves with internal resources. Each country places priority on securing and restoring its own infrastructure before consideration is given to other countries. The Nigerian 2016 Cyber Security Report indicated that Nigeria lags behind several African countries like Kenya, Ghana, Uganda, and Tanzania, in the number of cyber security experts per citizen. This is a worrisome development that needs urgent attention to address.

Nigerian-specific cyber security program that takes into consideration the peculiarities of our environment and unique threats we face as a country need to be developed across all sectors of the society. Expertise has to be developed on how to identify potential security breaches, detect breaches when they occur in a timely manner, remedy the breaches, and develop mechanism against future similar occurrences.

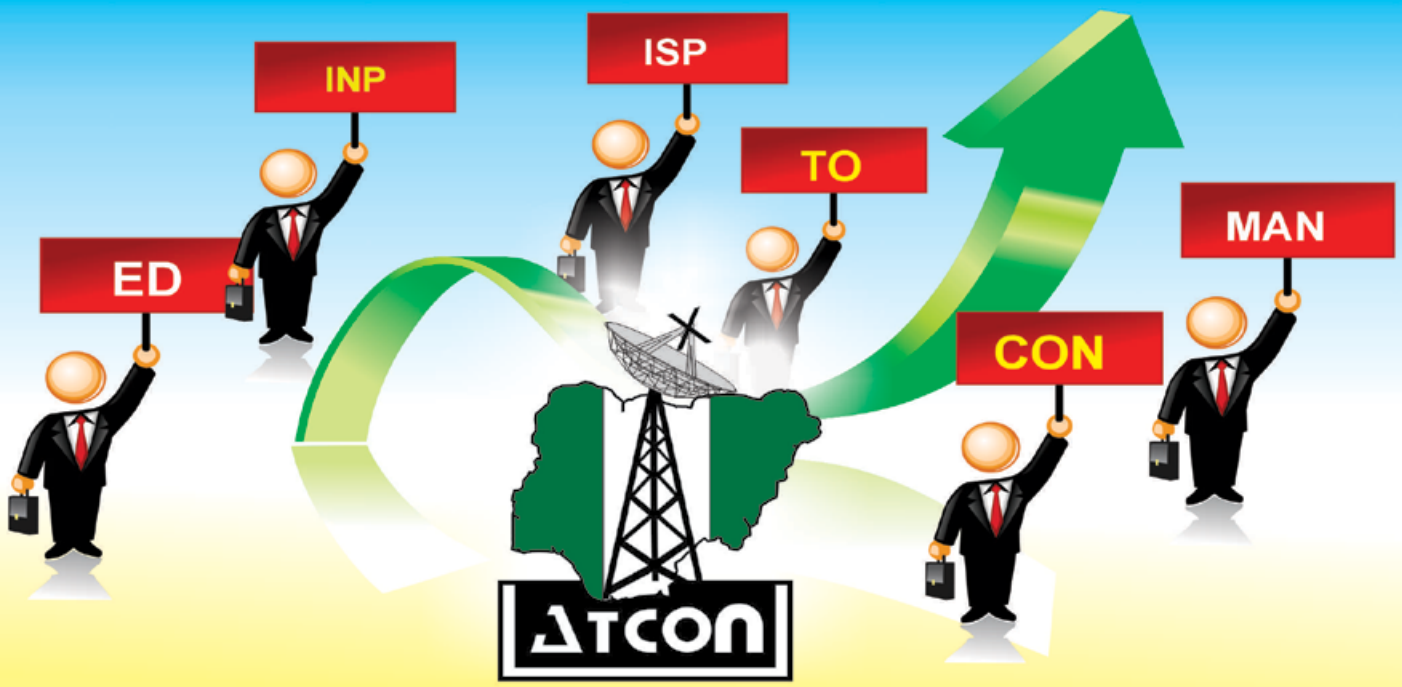
This calls for efforts in both formal and informal educational systems with respect to cyber security. On the formal sector, the youths must be thought the basics of cyber security as an integral part of the educational curriculum. The risks posed by cyber criminals' affects every member of the society hence being cyber security literate is a key component in building a progressive society. Cyber security needs to be demystified so the current mindset that it can only be understood by those with expertise in the sciences need to be reversed. Industry specific subject matter experts need to be trained to ensure that the appropriate security needed for each sub sector of the society is put in place.

On the informal front, constant dissemination of information to the general public on best cyber security practices is essential to keeping the populace safe and will minimize impact of consistent cyber attacks.

Weekly updates on cyber risks and preventive measures to be adopted should be sent to the populace using various means including social media apps, print media, various electronic communications, bill boards and posters. Various languages easily understood by the populace should be adopted so the concept of cyber security will be well understood and its successful implementation assured.

The theme of the Nigerian 2017 Cyber Security Report – **Demystifying Nigeria's Cyber Security Poverty Line**, and the content of the well researched report on the state of cyber security in Nigeria creates a good platform to keeping the Nigerian state safe from Cyber Criminals.

ASSOCIATION OF TELECOMMUNICATIONS COMPANIES OF NIGERIA



ATCON works in partnership with all stakeholders in the telecommunications industry to take Nigeria's economy to the next level.

- **TELEPHONE OPERATORS**
  Fixed, Mobile
- **MANUFACTURERS**
  Equipment & Accessories Manufacturers,
  Manufacturers' Representatives, etc.
- **INFRASTRUCTURE PROVIDERS**
  Colocation, VSAT, Trunking,
  Microwave Radio, Optic Fiber, Cabling,
  Interconnect, Long Distance Carrier, etc.
- **EQUIPMENT DEALERS**
  Sales, Supply, Installation & Maintenance of Mobile Phones,
  Two-Way Radios, Pagers, Telephone Handsets,
  Customer Premise Equipment, PABX, Network Installation, System Integrators,
  etc.
- **INTERNET SERVICE PROVIDERS (ISP)**
  Internet and related services
- **CONSULTING**

ASSOCIATION OF TELECOMMUNICATIONS COMPANIES OF NIGERIA
10 Mojidi St., Off Toyin St.,Ikeja, Lagos
Tel: 01 769369; 018963488; 08066629111
secretariat@atcon.org.ng ; www.atcon.org.ng

www.atcon.org.ng

...Partnering for Telecom Development!

Executive Summary

THE GLOBAL LANDSCAPE OF CYBER THREATS IS QUICKLY CHANGING. THE 2017 CYBER SECURITY REPORT IS PART OF OUR CONTRIBUTION TO THIS SHIFT AS WE HELP CUSTOMERS AND THE PUBLIC BETTER UNDERSTAND THE NATURE OF THE THREATS IN AFRICA.

Our research is broken down into 8 key areas:

- Top Attacks
- Cyber Intelligence
- Survey Analysis
- Home Security
- Top Trends
- Sector Risk Ranking
- Industry Analysis
- Anatomy of a Cyber Heist

As more business models move away from physical to cyber operations, it's become evident that the African cyber health is poor. The 2017 Cyber security survey shockingly reveals that **over 90% of African businesses are operating below the cyber 'security poverty line'.**

What is the cyber security poverty line?

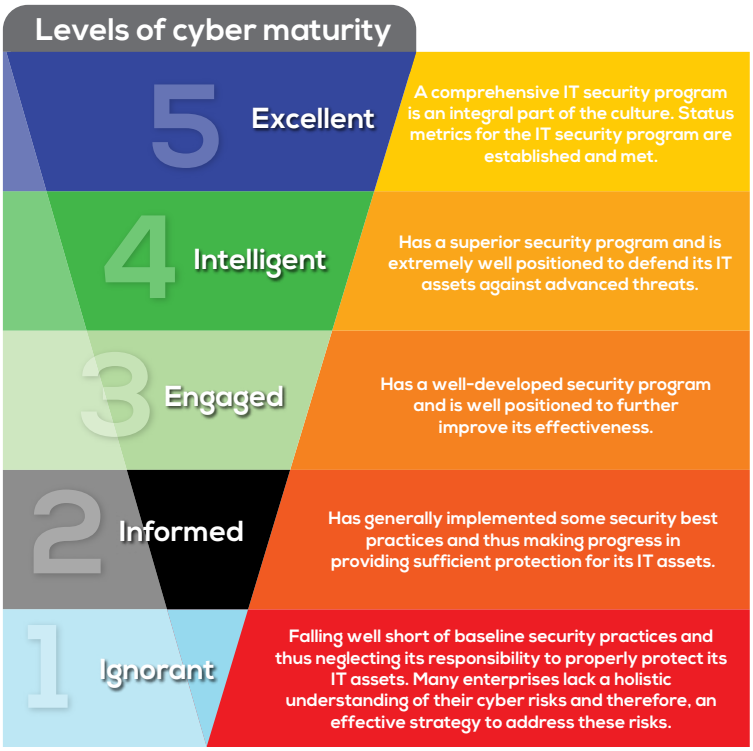
Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

In the context of a cyber-security poverty line there are still numerous organisations particularly SMEs that do not have the skills, resources or funding to protect, detect and respond to cyber security threats. Many organisations and individuals fall below this line. We aim to demystify the cyber security poverty line within Africa.

What are the characteristics of organisations operating below the poverty line?

Firms rated their own capabilities by responding to 24 questions that covered the four key functions outlined in the Africa Cyber Security Framework: Anticipate, Detect, Respond, and Contain.

Using the Africa Cyber Security Maturity Framework, we were able to establish the maturity levels of these organisations.



What is the impact of operating below the poverty line?

The overall survey results found about 90% of respondents in Africa have significant Cyber security risk exposure (with overall capabilities falling below under Ignorant capability).

General characteristics of organisations operating below the Cyber security poverty line are:

- Lack the minimum requirement for fending off an opportunistic adversary.
- Are essentially waiting to get taken down by an attack.
- There's also the idea of technical debt as a result of postponing important system updates.
- Lack in-house expertise to maintain a decent level of security controls and monitoring
- Tremendously dependent on third parties hence have less direct control over the security of the systems they use.
- They also end up relinquishing risk decisions to third parties that they ideally should be making themselves.
- Lack resources to implement separate systems for different tasks, or different personnel to achieve segregation of duties.
- They'll use the cheapest software they can find regardless of its quality or security.
- They'll have all sorts of back doors to make administration easier for whoever they can convince to do it.

What does the future hold for this problem?

As cyber-attacks continue to evolve, it's paramount that organisations rise above the cyber security poverty line. In a world where buying a tool is considered a silver bullet to solving cyber security issues, it's critical that we ask ourselves key questions:

- What are my organisations top risks?
- What is the worst that can happen to my business?
- What do I need to do to ensure that I have secured my systems against these threats?

This approach creates room for dialogue between business and IT. Years of experience in the Cyber security field has shown that organisations with little budgets can still maintain reasonable security levels granted they understand the few critical areas that need to be protected the most.

Key Highlights

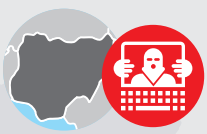
Breakdown of key statistics for different countries:

	Population (2017 Est.)	GDP (2017) in USD	Internet Penetration % Population (2017)	Estimated Cost of cyber-crime (2017)	Estimated No. of Certified Professionals
Africa	1,300,000,000	$3.3T	35%	$3.5B	10,000
Nigeria	195,875,237	$405B	50%	$649M	1800
Tanzania	59,091,392	$47B	39%	$99.5M	300
Kenya	50,950,879	$70.5B	85%	$210M	1600
Uganda	44,270,563	$24B	43%	$67M	350
Ghana	29,463,643	$43B	34%	$54M	500
Namibia	2,587,801	$11B	31%	*	75
Botswana	2,333,201	$15.6B	40%	*	60
Lesotho	2,263,010	$2.3B	28%	*	30
Mauritius	1,268,315	$12.2B	63%	*	125

*Certified Professionals is limited to the following certifications: CISA, CISM, GIAC, SANS, CISSP, CEH, ISO 27001, PCI DSS QA and other relevant courses.
*Economic and internet usage data extracted from respective country Internet regulator reports and World Bank site.

The past year was a particularly tough period for local organisations with respect to cyber security. The number of threats and data breaches increased with clear evidence that home grown cyber criminals are becoming more skilled and targeted.

over 90% of Nigerian organisations are operating below the security poverty line significantly exposing themselves to Cyber security risks



Cost of cyber-attacks $649M annually

Fake News has hit Nigeria's media streams as we increasingly see unverified and often elaborate disinformation being circulated through various mediums

over 90% The people affected by Cyber bullying ranged from the common citizen to media personalities and even government officials.

Banking Sector is still the most targeted industry in Nigeria

Most organisations' Cyber security programs are Tool Oriented

81% Cyber security incidents either go unreported or unsolved

Engr. Haru Al Hassan

Director, New Media and Information Security Department

Nigerian Communications Commission (NCC)

What is fake news?

Written and published news with the intent to mislead in order to damage an entity or person and/or gain financially.

How did fake news become such a big problem?

People believe what they see in the public domain, especially on popular information sharing sites. Because it was designed to instigate outrage and shock, some readers share it on Facebook, twitter, or other types of social media without questioning it or with the purpose of helping others.

Fake news is a problem because it is aided by speed and large number of audience in the social media domain.

What will ultimately get brands to fight fake news?

Google now work with international fact-checking network, IFCN, in three main ways: increasing the number of verified fact checking in the world, expanding the code of principles into new regions, and offering free fact checking tools. It should be encouraged in other climes too, countries should enter into partnership with content providers to find solutions to this problem.

Should regulators force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

Yes, though both companies already have strict policies for their ad networks, it is also important to reach an agreement with these companies on what to remove as fake news. By removing a potential revenue stream, it makes the business of fake news a bit less lucrative. It's clear that it's not just about influencing people's conviction, they also take advantage of social networks to make money using fake news. If Facebook, Twitter, Google News and other website flagged inappropriate content, then there would be no reason to create fake news sites in the first place.

What happens when fake news spreads?

What actions can people take to verify news stories, photographs and of online information?

It is very difficult to verify information on the internet, preventive and proactive measures taken through collaboration with all relevant stakeholders would be the best way to prevent the spread of fake news. Counter narratives using the same media, but indicating authentic or credible sources may help in certain circumstances.

We do everything online - book doctors' appointments, manage our bank accounts and find dates. Do you think we are ready to vote from our PCs or smartphones? Explain.

No. The stakes are higher in the case of voting as compared to other online endeavors. Moreover, availability of network services in most remote areas will be a challenge to contend with. Even where there are services and people have smart phones, we have to make sure that the people are in control of their own computers as far as security is concerned.

There are two major concerns when it comes to security: the vulnerabilities of voters' personal computers, and the vulnerabilities of the servers and back-end systems that would power the online voting infrastructure and host the websites for particular jurisdictions.

The fears on the server side concern hackers. The biggest fears there revolve around users being redirected to fake sites and servers, thus causing a vote to go to the wrong place and leading to inaccurate tallying. But the security of those systems are easier to control than citizens' computers.

What is the highest risk that we face by moving to electronic voting?

In any elections, verification or validation and anonymity of votes is very important. Voting away from polls also raises the spectra of vote manipulation. The major issue at stake will be ignorance and lack of awareness, which can lead to one internet savvy 'expert' voting on behalf of many.

What are some of the pros?

- It will make collation of election results much easier.
- People can vote from anywhere.
- Ransomware.

Why is Ransomware so effective?

Ransomware displays intimidating messages that will induce a victim not to ask for help, it is done in such a way that a victim is meant to believe the only option he/she has is to pay the ransom, in order to disinfect your system. The authors of Ransomware tend to instill fear and panic into their victims, causing them to click on a link or pay a ransom, and users systems can become infected with malware. Social engineering concepts are also used in some cases to convince a target to succumb to ransomware attack.

What is the possible impact of Ransomware?

Ransomware not only targets home users; businesses can also become infected with Ransomware, leading to negative consequences, including;

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organisation's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Have you or know someone you know been affected by Ransomware?

No.

How often do you transact using your mobile phone?

Daily.

Have you ever been a victim of online/ mobile scam?

No.

Why does the cyber skills shortage need immediate attention?

- To help in the combat against cyber criminals in the country.
- To enhance security and confidence in the use of cyberspace.

How many unfilled security jobs are estimated to exist today?

The low availability of professionals with specialized cyber skills is one of the biggest issues facing organisations looking to defend their core business systems against cyber-attacks. A recent report from Information Systems Audit and Control Association (ISACA) one of our important stakeholders, titled "The Growing Cyber Security Skill Crisis," estimated that there are as many as 1 million unfilled security jobs worldwide.

How does collaboration help enrich the students' learning?

It serves as an avenue for knowledge sharing - learning new concepts, techniques, solutions and services rendered by relevant stakeholders.

In the year 2017, what were the key Cyber security consultancy services that the industry need the most?

- Vulnerability Assessments
- Forensics
- Audit Services
- Risk Management Programs

Based on your experience, approximately how many times do organisations within the country carry out comprehensive Cyber security audits annually?

Once a year, albeit rarely.

Where would you rate the Cyber security maturity levels of the organisations you have interacted with?

- High
- Medium
- Low

In your opinion were there more cyber-attacks in the year 2017 as compared to previous years?

Yes.

Which categories of Cyber security should organisations be most keen on?

- Vulnerability assessment and penetration testing services.
- Cybersecurity risk audit services.
- Forensics and investigations services.
- Managed security services.

Which sector releases the highest number of cyber security tenders within the country?

- Financial sector
- Manufacturing sector
- Hospitality
- Government institutions
- Others

Based on your previous experience, what are the most critical Cyber security challenges being faced by local market?

- Budget or Management buy-in.
- Lack of awareness.

Top Trends

Fake News: Vulnerability of truth

The inception of Facebook, Twitter and Instagram have revolutionized the way we consume information with SPEED being a key selling point. Individuals now have a constant need to 'be in the know'. Through features like feeds, profiles and groups we get instantaneous access to information from any location.

In 2017 however, these platforms were overwhelmed by rogue politics, misinformation and dubious claims. In 2017, the editors and directors of one of Nigeria's most popular tabloid newspapers were detained over what authorities called a fake news story about a political plot implicating the president. The real impact of the growing interest in fake news has been the realization that the public might not be well-equipped to separate truthful information from false information.

Its paramount that governments and social media owner's lay down stringent measures to clamp down on fake news, none the less, we appreciate that fabricated stories are not likely to go away as they have become a means for some writers to push their agendas, manipulate emotions, make money and potentially influence public opinion.

Insider Threat: The enemy within

Insider threats still top our list when it comes to high risks. From the numerous cases reported this year, it is clear that the group most implicated is administrators and other privileged users, who are in the best position to carry out a malicious breach, and whose mistakes or negligence could have the most severe effects to the organisation. The key contributors to the success of these attacks were inadequate data protection strategies or solutions and a lack of privilege account monitoring.

Top insider threats:

- Administrator accounts
- Privileged users accounts
- Contractors, consultants and temporary workers.

Ransomware: I don't WannaCry

Worldwide attack map

Throughout the first half of 2017, one thing still stands: ransomware is here to stay. We have seen an explosion of new variants, new attack tactics.

The level of sophistication in distribution methods and attack vectors have expanded and it is no longer enough to just rely on signatures and antiviruses, because, unfortunately, the data also shows no one is immune.

The Polymorphic technique with minor changes leads to unknown malware and greater obfuscation. For example, there is a PowerPoint malware that spreads by simply hovering a mouse pointer over a tainted PowerPoint slide, WannaCry which spread itself within corporate networks without user interaction, by exploiting known vulnerabilities in Microsoft Windows.

Dr. Ibrahim Lamorde

Commissioner of Police,

Police Special Fraud Unit, Lagos

What is fake news?

This in our view is false or distorted information, or stories usually initiated on electronic media mostly to smear targeted individuals or entities, gain financially or politically advantage, or influence public opinion. Significant information available on Nigerian social media contains such deliberate, unsubstantiated and often negative content.

How did fake news become such a big problem?

The problem has assumed alarming proportion in Nigeria due to the easy access to smartphones and Internet. There are over 147 million registered GSM phones (mostly Internet capable) to quickly spread any scandalous fake news.

Some print and electronic media do not confirm information before publication, thus falling prey to planted stories, which the undiscerning public, fascinated with melodrama circulate. Sensational headlines improve numbers of active online visitors to blogs and websites, thus boosting their advertisement income.

Industry regulators do not check the vicious circle of fake news, online followers and advertisement income, as practically no sanction or deterrence has been recorded.

Some online and print journalism are controlled and financed by non-professionals, whose primary goal is to promote personal interests not obliged to follow any ethical standard, such as editing and confirmation of stories.

Anonymity of fake news purveyors is further enhanced by the overseas location of platforms, website owners and domain name providers, while local regulators and law enforcement agencies possess inadequate technical capacity to track origins of fake news posts.

What will ultimately get brands to fight fake news?

Public apathy, consumer resistance and mass platform boycott.

Should regulator force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

This concern is not completely applicable to the Nigerian context, as all level 3 Internet platforms – Google, LinkedIn, Yahoo, Facebook, Twitter, Instagram, WhatsApp etc. are conveniently located outside Nigeria to avoid national oversight by our regulators. There is no available evidence that they have shared direct investigation related information with Nigerian regulators or law enforcement.

They and their users are also greatly averse to any regulation or control, to sustain the concept of freedom of the Internet.

However, victims in other Countries with strong Internet legislation have recourse to civil action against originators of fake news and the platform providers in specific cases. Public apologies, takedown of injurious publications and even damages have been awarded in favor victims.

What happens when fake news spreads?

What actions can people takes to varify news stories, photographs and other sources of online information?

Once fake news appears on any medium, it is inevitable that it is swiftly disseminated electronically to millions of people through any of the available mainstream or social media. The story is copies and pasted on other websites, becoming amorphous and uncontrollable. Intellectual property rights or original source becomes opaque. The more scandalous, disastrous or fantastic the story appears; the faster it spreads.

Verification cannot be done through any online platform at this stage, since all search engines will only replicate the same negative story in their top searches. Credible verification, confirmation or corroboration can only be safely done manually through hard copy document reviews and comparison, direct interviews, visitations and physical checks with concerned entities.

We do everything online - book doctors' appointments, manage our bank accounts and find dates - Do you think we are ready to vote from our PCs or smartphones? Explain

The electronic verification through the digital card readers at the 2015 general elections clearly demonstrates that the Independent National Electoral Commission will be able to conduct online voting through voting machines, PCs and smartphones in the near future.

It is however imperative to improvethe technical capacity of the national and state electoral bodies to transmit, secure, authenticate or repudiate digital signatures that electronic voting entails.

Development of indigenous software and servers required for such critical endeavor will prevent remote backdoor access by foreign parties.

Our telecommunication and power infrastructure also needs to be upgraded to support nationwide electronic voting.

Citizens' education is key towards public acceptability of electronic voting system.

What is the highest risk that we face by moving to electronic voting?

- Hacking
- Rejection of electoral result by skeptical voters
- Disenfranchisement of illiterate voters who are unable to utilize computers, tablets and smart phones to vote
- Technical issue such as malfunctioning of portal, software, Internet connectivity and servers during voting exercise

What are some of the pros?

Digital bulk data is always easier to store, retrieve, process, analyze and protect against theft or destruction.

Why is ransomware so effective?

Targets sometime want to pay the money demanded quickly, and avoid contact with law enforcement.

We believe that ransomewareattacks in Nigeria are grossly under reported.

What is the possible impact of Ransomware?

Financial and personal data loss.

Have you or know someone you know been affected by Ransomware?

No.

How often do you transact using your mobile phone?

Rarely.

Have you ever been a victim of online or mobile scam?

No.

Why does the cyber skills shortage need immediate attention?

For law enforcement, critical mass is urgently needed to design vital disruption, intelligence, investigation and public education strategies, as well as criminal databases archiving.

How many unfilled security jobs are estimated to exist today?

Unknown.

How does collaboration help enrich the students' learning?

- Practical skill acquisition for successful field operations.
- Focusing on specialized areas of comparative advantage.
- Task de-confliction.

Skill Gap: What you don't know will hurt you

Cost of Cybercrime in 2017 grew by 20% but the skill gap is still gaping wide. No one knows what they're doing, a lot of IT and security staff are downloading templates from the internet and applying these in their organisations. From our analysis, a key contributor to this is that organisations tend to look for people with traditional technology credentials – IT, Computer Science etc. But when you look at the matter, we need Technology analysts, Cyber Risk Engineers, data analysts, Risk experts most of which do not necessarily warrant a technology course. Most firms encourage their IT teams to take up courses that don't necessarily add value to the security of the organisations.

It is also concerning that companies would rather poach talent from each other and from training providers, rather than develop it pointing to the sad fact that: businesses are thinking in the short term. Rather than cultivating the needed talent, organisations are continuously relying on ready-made talent.

It is critical that we develop the right skills for our IT team that will enhance the ability to Anticipate, Detect, Respond and Contain cyber threats.

Mobile and Internet Related Services. Battery is low is no longer the only warning

This has become necessary as mobile money (MoMo) transfer is gaining grounds as a fast and easy way to transact business but criminals try to swindle unsuspecting victims.

Our statistics reveal that half of the banking users are using internet banking and three quarters use mobile banking services.

This year, several attacks reported indicated that hackers used dormant accounts to channel huge sums of money from banks. Most of the attackers also leveraged on the no-limit vulnerability present in most internet banking systems to channel out money.

There is a clear need to bridge the knowledge gap on mobile money operations among law enforcement officers and to identify common security, fraud and money laundering challenges confronting MoMo operations.

Network Architecture: Defense In-depth

Defense in depth means, applying multiple countermeasures in a layered or stepwise manner. Because there are ways around traditional protective systems such as firewall, it is imperative that individual systems be hardened from the Network, Application, Endpoint and Database levels. This means, putting controls in place for Access (Remote and Privilege), Change and vulnerability management.

The success of most attacks in 2017 were in one way or another linked to one critical issue: Weak Security Architecture. Successful ransomware attacks were mainly due to missing patches (Wannacry) and for most cases, inadequate privilege account monitoring/third party risk management. Yet these organisations have invested heavily in the latest Antivirus programs or SIEM solutions. High technology solutions, installed on top of weak architecture only equals one thing = A WHITE ELEPHANT. Most organisations focus most of their IT budgets on acquiring high end technologies but forget to set the foundation on which these technologies will effectively operate.

A SIEM tool is a useless investment if auditing is not enabled in network devices, no expertise exists for continuously analyzing and refining the alerts

Phishing: The weakest Link

Phishing is one of the attacks that leverages the inadequacies of humans and it remains worryingly effective. The number of phishing emails sent in 2017 was overwhelming and over 20% of these attacks targeted banks and other credit and financial organizations. With the evolution of phishing, it has become clear that basic awareness training may not be sufficient to safeguard your organisation. 2017 proved that we need to leverage technology especially since education programs, awareness campaigns and product innovation on their own have failed.

Cyber Pyramid Schemes: Easy come, Easy go

In an economy where it is so difficult to earn a living, many Nigerians try out pyramid schemes with the hope of making a huge, quick profit. Today's crypto currency scams in Nigeria seem to have taken over the old fashioned 419 scam.

The government has put in efforts in fighting electronic fraud within the Nigerian financial ecosystem. However, Bitcoin and other cryptocurrency scams are spreading so fast that the government is playing catch up.

In 2017 private sectors users were the greatest victims and initiatives like the "Nigeria Blockchain Alliance" (NBA) which brings together law enforcement agents, legal practitioners, forensic investigators and government agencies among others to collaborate in the fight against cryptocurrency related crimes within the country.

These schemes rely on a constant flow of new investments to continue to provide returns to older investors. When this flow runs out, the scheme falls apart. In recent times, we have seen these schemes evolve to now include crypto currencies.

System Integrity: Eroding Public Trust

Government has automated many processes including Passport Application, Voters Registration etc. However these automated systems have become a target for hackers seeking to make news or disrupt service delivery. As such tighter controls need to be in place to ensure that the confidentiality, integrity and availability of these systems are maintained. As such tighter controls need to be in place to ensure that the confidentiality, integrity and availability of these systems are maintained.

Website Defacement:

A number of Nigerian websites have been defaced including:

- Nigeria Security & Civil Defence Corps website hacked and hackers went on to dupe innocent and desperate job seekers online.
- West African Examination Council website hacked and hackers illegally gained access and printed questions meant for the May/June 2017 Secondary School Certificate Examination, and sold them to students.
- Joint Admissions and Matriculation Board (JAMB) website hacked – The hackers' deployed fake biometric capturing mechanisms and super-imposed registration slips just to satisfy the curiosity of innocent candidates that their registration was successful. And on the day of examination, such candidates' data would either be edited, or not found on the JAMB data base

Olusola Teniola

President,

Association Of Telecommunications Operating Companies of Nigeria (ATCON)

What is fake news?

Is news that may be considered unreliable and deliberately pushed out to create damage, propaganda, misinformation to the reader, so that the reader believes and may make informed decisions and draw conclusions that may negatively impact them or the target of fake news.

How did fake news become such a big problem?

The easy availability of online material and wider access to the World Wide Web has meant that bad news is easier to sale to the online user who is not readily informed and due to the nature of the information being misrepresented can be an avenue for those peddling fake news to make money on the back of ignorance. Generally, online blogs are areas where fake news is highest as there isn't any robust manner for fake news to be verified and challenged where generally it is easier for 'group thinking' to dominate the minds of the participants in the blog.

What will ultimately get brands to fight fake news?

Unfortunately, fake news in the form of propaganda has been in existence for centuries and the only reasonable way for brands to fight this is the through the adoption of AI and countering information in real-time to protect their brands. Public Relationship experts and consultants are traditional sources for brands to defend their image and with the growth in expert systems, big data there is an evolution in the methods used to counter the market and image risk that the bigger brands face (i.e. supply chain management has had many cases of fake news to destroy value).

Should regulators force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

This is a very sensitive area and subject to legal rights issues that will still need regional jurisdiction support, in the case of the European Union for instance, they are enforcing data privacy legislation to force the big OTT players mentioned to adopt rules to protect European citizen data considered private to not be propagated. This may be easier technically in search engines, however, parsing real-time Instant Messaging apps like WhatsApp that maybe used to spread fake news raises an interesting scenario that still needs to be explored under the current encryptions deployed by these services – how do you police this kind of thing?

What happens when fake news spreads?

What actions can people take to verify news stories, photographs and other sources of online information? Basic stuff, as consider the source, check the author, ask experts, check your bias and read beyond may be tactics that can be used by the lay person to manage this new reality.

We do everything online – book doctors' appointments, manage our bank accounts and find dates – Do you think we are ready to vote from our PCs or smartphones?

Explain. As a country, such as Nigeria, Definitely, not. The electronic systems are not fully embedded into our society, we are still not digitally literate to capture e-votes in a manner that is fully transparent and until we have fully resolved citizen data such as KYC across all our different National databases, it is premature to rely on voting systems that can be done from a PC or smartphone.

What is the highest risk that we face by moving to electronic voting?

Glitches in connectivity, poor level of veracity of data (Garbage-in-Garbage-out) and unavailability of voters campaign to educate the masses on how this will improve the current voting system and what needs to be put in place to achieve a fair and free election.

What are some of the pros?

No need to queue in the sun or rain. Improve security of lives – from voters' box snatchers and speedy declaration of elected officers, typically within 24hrs!

Why is Ransomware so effective?

A malware (software, firmware) written to threaten damage to a computer system unless the owner of the computer system yields to the threat and pays or preforms a favour to the writer of the malware to remove it, so that the threat is no longer there

What is the possible impact of Ransomware?

Lost productivity whilst negotiating to get the Ransomware removed and embarrassment

Have you or know someone you know been affected by Ransomware?

Fortunately, no one has owned up to being a victim that I know.

How often do you transact using your mobile phone?

At least once every other day.

Have you ever been a victim of online or mobile scam?

No, not personally.

Why does the cyber skills shortage need immediate attention?

The prevalence of IT systems in our day-to-day life means that criminals are more focused on hacking into these systems for maximum pay-day and hence, it means that each one of us is vulnerable to hacking. Cybersecurity skills is critical to solving this menace

How many unfilled security jobs are estimated to exist today?

More than 24% of the unemployed youth in Nigeria

How does collaboration help enrich the students' learning?

Collaboration in between University, SMEs, Corporates and Government is key to the application of student knowledge and deep experience of how Cybercrimes can be solved and society a better place for these students entering a digital world.

Nigeria's TOP 10 priorities for 2018

TRANSITIONING FROM 2017 TO 2018, THE JOURNEY OF ATTAINING A SECURE CYBER ECOSYSTEM IS A LONG BUT OPTIMISTIC ONE. CYBER-ATTACKS WILL CONTINUE TO GROW AND ONLY THE INFORMED AND PREPARED WOULD SURVIVE WITH MINIMAL LOSSES. IN 2018, CYBER THREATS AND COUNTERMEASURES ARE LIKELY TO TAKE THE FOLLOWING DIMENSIONS:

1 Database Security: Secure the vault

Database (DB) security concerns the protection of data contained within databases from accidental or intentional but unauthorized access, view, modification or deletion.Top priority for security teams is to gain visibility on activities on the databases particularly, direct and remote access to DB by privileged users. Fine grained auditing of these activities is essential to ensure integrity of data. Going to 2018, database security should be a top priority that focuses on ensuring that access to the database is based on a specific role, limited to specific time and that auditing and continuous monitoring is enabled to provide visibility.

2 Privileged User Management: Who has access to the crown jewels

The main obstacle between your organisation's crown jewels and hackers are privileged accounts.

These accounts are found in every networked device, database, application, server and social media account and as such are a lucrative target for attackers. More often, privileged accounts go unmonitored and unreported and therefore unsecured. We anticipate that in 2018, abuse of privileged accounts will worsen and it is therefore critical that organisations inventory all their privileged accounts, continuously review the users with these privileges and monitor their activities.

Organisations must adopt a privileged account security strategy that includes proactive protection and monitoring of all privileged credentials, including both passwords and SSH keys.

3 Patch Management: To patch or not to patch

75% of vulnerabilities identified within local organisations were missing patches. In 2017 alone, we have seen vendors such as Microsoft releasing over 300 patches for their windows systems. This presents two obvious lessons:

- The increased number of released patches are choking organisations
- Organisations have not developed comprehensive patch management strategies and procedures.

Now more than ever, organisations need to narrow down to one critical thing: What do we patch?

Not all of the vulnerabilities that exist in products or technologies will affect you, 2018 presents a great opportunity for organisations to strategize, focus more energy on identifying testing and applying critical patches released. This may require adoption of an automated patch management system.

4 Unstructured Data Management: There is no one size fits all

Unstructured data is information that either does not have a pre-defined data model or is not organized in a pre-defined manner.

Emails, medical records and contracts are a few examples of unstructured data that exist in the organisation. Whereas most institutions have some form of unstructured data, it is the healthcare and insurance industries that top this list with terabytes of data in file shares and home directories. The security of this data however remains an under-recognized problem as these files and folders are left unsecured. This has resulted in often-unnecessary data exposure and unauthorized access. To help secure against the security risks of unstructured data it is necessary that we;

- Identify critical unstructured information assets
- Identify which employees possess critical unstructured data
- Implement technology and process controls to protect data assets eg DLP, Email Monitoring

5 Endpoint Security: Cyber security front-line

Often defined as end-user devices – such as mobile devices and laptops, endpoint devices are receiving more attention because of the profound change in the way computer networks are attacked. With so many pluggable devices in the network, this creates new areas of exposure.

- Unsecured USB devices leading to leakage of critical data, spread of malware.
- Missing security agents and patches accounts for 70% of all misconfigurations within the network allowing attackers to exploit well known vulnerabilities.

- Unauthorized remote control software giving attackers full control of the endpoint.
- Unauthorized modems/wireless access points

It is critical that before endpoints are granted network access, they should meet minimum security standards. Beyond this, organisations should invest in endpoint security tools that provide capabilities such as monitoring for and blocking risky or malicious activities. Focus areas:

- DISCOVER all devices that are connected to a company's network. Including new or suspicious connections,
- INVENTORY the OS, firmware and software versions running on each endpoint. This information can also help prioritize patching
- MONITOR endpoints, files and the entire network for changes and indicators of compromise.
- PROTECT the endpoints using technologies such as Antivirus

6 **Employee Security Awareness:** Ignorance is not Bliss

If infrastructure is the engine, staff awareness is the oil that ensures the life of the engine. Uninformed staff or employees not familiar with basic IT security best practices can become the weak link for hackers to compromise your company's security. Staff awareness is key.

7 **Vendor/Third party security:** Bring Your Own Vulnerability

In 2017, several attacks were launched against organisations and these had one thing in common; vendor involvement. Be it directly or indirectly, vendors introduce risks to organisations through their interactions with critical data. We anticipate that in 2018, cases involving rogue vendors will increase; we will see rogue vendors:

- Use privileged accounts to access other network systems,
- Use remote access tools (RDP, Teamviewer, Toad) to access critical applications and databases
- Manipulate source code for critical applications in order to perform malicious activities

Organisations need to evaluate their potential vendor's risk posture, ability to protect information and provision of service level agreement. At the end of the day, when a breach occurs on your vendor's watch, regardless of fault, you shoulder the resulting legal obligations and cost.

8 **The Board's Changing Role:** Security begins at the top

The traditional role of boards in providing oversight continues to evolve. The impact of Cyber attacks now requires board member level participation. This proactive and resilient approach requires those at the highest level of the organisation or government to prioritize the importance of avoiding and proactively mitigating risks.

Key questions that modern board members should be asking themselves are:

ANTICIPATE
What are our risks and how do we mitigate them?
DETECT
Should these risks materialize, are we able to detect them?
RESPOND
What would we do if we were hacked today?
CONTAIN
What strategies do we have in place to ensure damage issues don't reoccur?

9 **Security Architecture/Engineer Skill Set:** Widen your employee gaze

Majority of IT staff are tool analysts focusing on understanding a tool instead of data processed within the tool.

10 **Continuous Monitoring:** Police Vigilance

There is need for continuous monitoring. The predicted increased number of attacks in 2018 demand for a mechanism to detect and respond to threats and incidents. Even though most organisations cannot adopt a real-time round the clock monitoring and reporting it is necessary that these organisations look for alternate solutions and practices including managed services and day long monitoring.

Onajite Regha

Chief Executive Officer,

Electronic Payment Association Of Nigeria (E-PPAN)

Leveraging On Big Data As An Industry Tool To Combat Fraud

E-PPAN annually hosts the E-Fraud Conference as an advocacy tool in combating payment system fraud. This year the conference concluded that fraud must be fought collaboratively using big data.

Today's world is more connected than ever, with the internet of Thing (IoTs) promising a more personalized and automated services, making the lives of people much easier. Yet, for all its advantages, many of these devices are not properly secured - giving rise to cyber threat. Cyber actors exploit these vulnerabilities to steal information and money. Experts estimate $450 billion was lost to the economy in 2016 as a result of cybercrime, and that number is expected to increase to $1 trillion by 2021. This shows that cybercrime is growing quickly and the stakes are rising as well.

Since the internet knows no physical or virtual border, it has become the perfect covers for cyber criminals to be anonymous and perpetuate their crimes. Fraudsters are smart and they are always inventing new ways to dupe the system and get through the defenses. They rapidly evolve their methods to complex tactics in other to swing online assault from hacks, attacks, ransoms, and even extortion attempts. So far in the year 2017, we have seen so many recent data breaches, from Uber, Equifax, and HBO, millions of data were stolen. A lot of these data breaches were targeted at fintechs, showing that they are an attractive target, since it's a universal knowledge that cybercriminals will always follow the money. The only way to prevent a cyber breach is for businesses and governments to change the way they think about cyber security otherwise there will be nothing to cyber-defend.

Many organizations are still not taking fraud prevention seriously. While some simple hope that they won't get hit, others believe the notion that if it does happen, they have defensive mechanism to fight it forgetting that these breaches come at a cost. It is not enough to own security solutions but to ensure that they are in the best possible position to respond to cyber-attack and navigate the aftermath.

Cybersecurity should be top most on the minds of individuals and companies alike in other to stay ahead in this 'cat and mouse game with fraudsters. They should focus on protecting themselves and their data from these increasingly advanced and complex threats and this cannot be done in silos; it needs the collaboration of everybody.

One of such collaborative platform was the 8th Annual Payment Systems and Fraud conference 2017 organized yearly by the E-Payment Providers Association of Nigeria (E-PPAN) where security experts from the financial sector, law enforcement agencies and industry key players met to discuss a head way out of the rise in fraudulent transactions. The conference revealed that 237 billion (Two Hundred and Thirty Seven Billion) naira has been lost to fraud in banks since 2007. Fraud has certainly been on the rise, and experts are bracing for worse. Hence, Security experts will need to think out of the box and start using sophisticated data analysis technology to fight fraud.

When it comes to effective fraud management, data is the key for this seeming daunting challenge. Big data is used to detach patterns and send signals which make it difficult for a fraudster to mimic the behavior. Leveraging on the use of data analytics technology, in a collaborative approach, can further promote the continued growth of the

industry and mitigate the ugly trend of payment fraud while boosting the economy at large. Insights from big Data can be used to stem cybercrime as the technology looks at data available to detect fraud patterns, allowing for better risk decisions to be made and thereby lowering fraud. The key word here is big data which we do not have. Many organizations have data in silos but not in a central place where it can easily be harnessed, analyzed and used to detect fraud.

The conference called for the need to have a strategic collaboration with other relevant data collecting agencies in Nigeria so as to harmonize all available database and set appropriate standards and protocols for people to access it. If we must stay ahead in this war against cybercrime, we need to fight fraud from a collective front. The payment industry stakeholders has to align together in other to beat cyber criminals at their game as the growth of the economy depend on a stable, safe, and resilient cyberspace.

One area the conference felt has not fully reached its potential is the inter-relationship between the different law enforcement agencies locally and across borders. Criminals are not being brought to justice swiftly because the law enforcement agencies are bugged down by bureaucracies of cross border investigations and prosecution. An improved cross border relationship liaise with law enforcement agencies, will improves the speed of investigation of cyber crime without the restrictions placed by geographical location.

With improved synergy between all stakeholders in the system and leveraging on Swe can hope for better adoption and faster growth of the National Payment System and minimized payment fraud.

E-PPAN

E-Payment Providers Association of Nigeria

Our **Objectives:**

- To assist members in influencing the development of appropriate standards for the common benefit of the electronic payment industry, end-users, consumers and regulatory authorities.
- To be the source of credible information in public policies that affects e-payment and self service adoption and implementation.
- To serve as an educational resource to our members and the industry.
- To provide a forum for cutting edge discussions and projects on issues surrounding e-payment and self service.

Our **Vision:**

To become the most authoritative and respected industry forum for promoting e-payment and self service businesses in Nigeria.

Overarching **Goals:**

To enhance institutional frameworks and processes for robust and effective E-payment systems in Nigeria.

Our Services

- **ADVOCACY**
- **CAPACITY BUILDING**
- **NETWORKING**
- **RESEARCH**
- **CONSULTING**

E-PAYMENT PROVIDERS ASSOCIATION OF NIGERIA

1, Racheal Nwangwu Close, Lekki Phase 1, Lagos.

01-3426493, 08033013614; eppan@e-ppan.org, info@e-ppan.org

@eProviders Electronic Payment Providers Association of Nigeria

www.e-ppan.org

Cyber Intelligence Statistics, Analysis, & Trends

FOR THE PURPOSES OF THIS REPORT, WE INSPECTED NETWORK TRAFFIC INSIDE A REPRESENTATIVE OF NIGERIAN ORGANISATIONS, REVIEWED CONTENTS OF ONLINE NETWORK MONITORING SITES SUCH AS PROJECT HONEYNET AND REVIEWED INFORMATION FROM SEVERAL SENSORS DEPLOYED IN NIGERIA. THE SENSORS PERFORM THE FUNCTION OF MONITORING AN ORGANISATION'S NETWORK FOR MALWARE AND CYBER THREAT ATTACKS SUCH AS BRUTE-FORCE ATTACKS AGAINST THE ORGANISATION'S SERVERS. IN AN EFFORT TO ENRICH THE DATA WE COLLECTED, WE PARTNERED WITH THE HONEYNET PROJECT AND OTHER GLOBAL CYBER INTELLIGENCE PARTNERS TO RECEIVE REGULAR FEEDS ON MALICIOUS ACTIVITY WITHIN THE CONTINENT.

In this section, we highlight the malicious activity observed in the period under review. This data represents malicious activity captured by our sensors and publicly available intelligence.

Project Honeypot Intelligence Analysis

This section covers data from the honeynet project, a global database of malicious IP addresses.

Cyber Attack Timeline

2017

FEB

Fraudsters hack Nigeria Security and Civil Defence Corps (NSCDC's) website

MAR

A four-man syndicate who specialize in defrauding foreigners using names of high profile politicians arrested

APR

North Korea-linked hackers are attacking banks worldwide

Alleged hacking of JAMB website

MAY

3 Nigerian Scammers Get 235 Years of Total Jail Sentence in U.S.

JUN

Maersk apm terminal systems hacked operations grounded

JUL

West African Examinations Council (WAEC) website hacked

AUG

Lone Nigerian hackers behind attempted hacks at 4,000 organisations

3 men allegedly hack bank account, steal N39m

Nigerian Man Hacked Thousands of Global Oil & Gas and Energy Firms

Check Point's researchers reveal a Nigerian cyber-criminal who attacked more than 4,000 organisations.

Abiodun Aderoju

Chief Inspector of Internal Audit and Deputy General Manager

Sterling Bank Plc

What is fake news?

Any news that is not genuine or authentic.

How did fake news become such a big problem?

Because it misleads people.

What will ultimately get brands to fight fake news?

Because of the reputational damage that could be done to such brands.

Should regulators force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

Yes.

What happens when fake news spreads?

It misleads people.

What actions can people take to verify news stories, photographs and other sources of online information?

We do everything online – book doctors' appointments, manage our bank accounts and find dates – Do you think we are ready to vote from our PCs or smartphones? Explain.

Not yet ready as the country still has a lot of people that are not computer literate.

What is the highest risk that we face by moving to electronic voting?

Risk of disenfranchisement of genuine voters.

What are some of the pros?

If well managed, it will curb election rigging or malpractice.

Speedy or faster electoral results.

Why is Ransomware so effective?

A malicious software that "demobilized" the Victim until a ransom is paid.

What is the possible impact of Ransomware?

It is devastating - Monetary and otherwise.

Have you or know someone you know been affected by Ransomware?

No.

How often do you transact using your mobile phone?

Always.

Have you ever been a victim of online or mobile scam?

NO, I haven't been a victim. However, several attempts had been made on me.

Why does the cyber skills shortage need immediate attention?

Cybercrime has grown to be an industry on its own coupled with global adoption of Cloud Technology.

How many unfilled security jobs are estimated to exist today?

1.8M according to the recent survey by ISC2.

How does collaboration help enrich the students' learning?

It shortens learning curve and helpful for those with difficulty in social skills.

In the year 2017, what were the key Cybersecurity consultancy services that clients were looking for?

- Vulnerability Assessments
- Forensics
- Audit Services
- Risk Management Programs
- Managed Security Services

Based on your experience, approximately how many times do organizations within the country carry out comprehensive Cybersecurity audits annually?

On adhoc basis.

Where would you rate the Cybersecurity maturity levels of the organizations you have conducted audits at?

Medium.

In your opinion were there more Cyber-attacks in the year 2017 as compared to previous years?

Yes.

Which categories of Cybersecurity were organizations most keen on?

- Vulnerability Assessment and Penetration Testing Services.
- Forensics and Investigations Services.

Which sector releases the highest number of Cyber Security tenders within the country?

Financial Sector.

In the year 2017, what were the key Cybersecurity products that clients purchased?

Data Loss Prevention; IPS.

Based on your opinion, which products have higher market appetite?

- Data Loss Prevention Tools
- Anti-malware Tools

What are the clients' top priorities or needs to be addressed when purchasing Cybersecurity products?

Industry Credibility and Total Cost of Ownership.

What makes the local market unique when choosing what Cybersecurity products to invest in?

Nigeria is an Emerging Economy.

Based on your previous experience, what are the most critical Cybersecurity challenges being faced by the local market?

Skills gap.

What is your estimate of cyber crime in the year 2017 based on data or statistics available to you?

N127 Billion, about 0.08% of the country's Gross Domestic Products (GDP) as estimated by Federal Government of Nigeria.

2017 Nigeria Cybersecurity Outlook by Deloitte: https://www2.deloitte.com/ng/en/pages/risk/articles/2017-nigeria-cybersecurity-outlook.html

Malware Attacks

2017

JAN

New Variant of KillDisk is Ransomware

FEB

TeamSpy Malware transforms Teamviewer into a Spying software

MAR

Macro Malware for MacOS users

Torrent Locker Ransomware

DNSMessenger malware

New Ransom-ware-as-a-service Program, Dot Ransom-ware

APR

BankBot Trojan Targeting Over 420 Banking Apps

Hackers Steal Payment Card Data From Over 1,150 Inter Continental Hotels

New Malware strain targeting Linux-based systems

False Guide malware

MAY

PDF file containing Ransomware down-loader

PowerPoint Malicious Hover Vulnerability

Wannacry Ransomware affects more than 200,000 computers in 150 countries

Fireball Malware infects 250 million computers

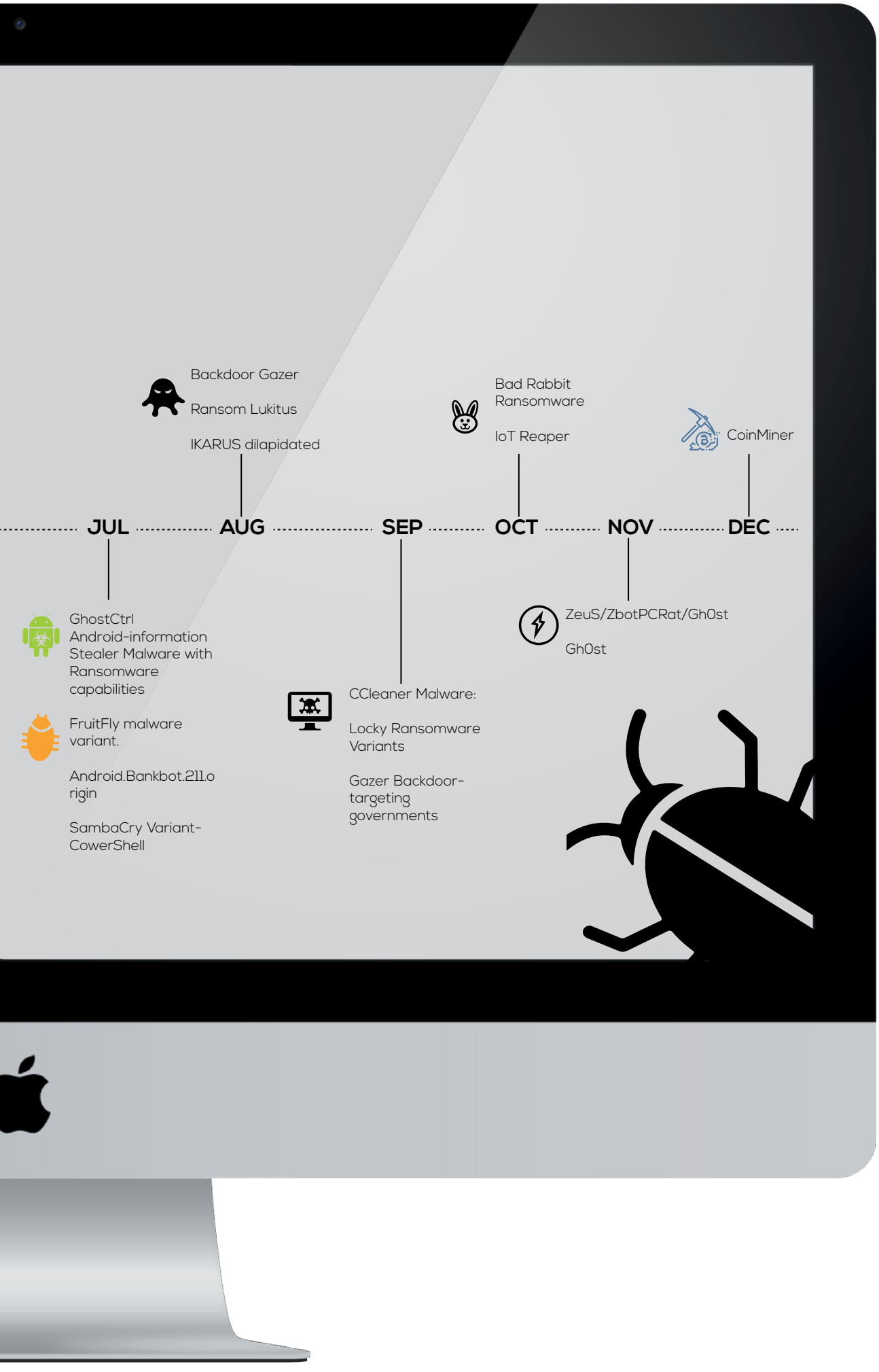
OakBot banking Trojan harvests financial information

JUN

Petya Ransomware has spread internationally, wreaking havoc.

A new variant of Marcher Android sophisticated banking malware disguised as

Major Malware 'Xavier' hits play store infecting 800 Android apps.


Backdoor Gazer
Ransom Lukitus
IKARUS dilapidated
Bad Rabbit Ransomware
IoT Reaper
CoinMiner
JUL
AUG
SEP
OCT
NOV
DEC
GhostCtrl Android-information Stealer Malware with Ransomware capabilities
FruitFly malware variant.
Android.Bankbot.211.origin
SambaCry Variant-CowerShell
CCleaner Malware:
Locky Ransomware Variants
Gazer Backdoor-targeting governments
ZeuS/ZbotPCRat/Gh0st
Gh0st

Ben Roberts

Chief Technical Officer,

Liquid Telecom Group

Kindly highlight some of the top Cyber security issues of 2017 and how these issues impacted you personally, your organisation or country.

Ransomware and particularly Wannacry have made the most noise in Cyber security in 2017. But from our own experience, it is social engineering, very sophisticated 'spear fishing' or 'whaling' (like phishing but aimed at bigger fish- senior execs) that has bothered us the most. This constant barrage of emails, instant messages, phone calls, to get people to give up their passwords voluntarily, is there all the time and is often good enough to fool very savvy smart people. An IT manager can secure his own company systems, only to find that people in the organisation are using personal Gmail, or Skype, they get hacked and causing damage within the corporate organisation. The motive for this kind of phishing is normally to conduct direct monetary theft.

Do you think fake news is a major problem in your country Africa?

Yes.

If yes, who should be responsible for controlling the creation and distribution of fake news (government, end users, Telcos or ISPs or content owners)?

Fake news has made headlines globally. But we need to distinguish between what's fake and what is not, and global leaders need to communicate responsibly. But yes, fake news in East Africa, particularly Nigeria (where I live) has been terrible this year, with the election season that has taken place. WhatsApp was the worst platform for circulating of completely fake news, but the traditional media did a poor job on responsible election coverage.

Should regulators force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

Regulators may not be well positioned to force takedowns on platforms that they do not regulate. Communication regulatory bodies in Africa regulate traditional media, but have no jurisdiction to regulate Facebook, a foreign company. So they can force local media houses to take down a fake story from their websites, but they cannot ask Facebook to take down a fake story. Communication service providers in East Africa are regulated by the Communication Authority (CA) of course, but the service providers are completely technically unable in any way to selectively block content, web pages, hashtags on any of the social media or international news sites. So the CA would be unable to force service providers to block content, since it is totally impossible to do so.

What can be done to improve the general user awareness on the detection of fake news in the country?

All of us are responsible to assess information before passing it on; think about the source and whether we trust it, and whether the information seems feasible. It is easy to blame media, or social media platforms for fake news, but in fact society is to blame. Just before the Nigerian elections, I came across really good campaign from Facebook about how to spot Fake news. It had 10 points of indicators that something might be fake news. It was a really good campaign from Facebook, and its targeting towards Nigerian audience was well meaning. I republished the campaign on Twitter under hashtag #dontfwdfakenews, the important message was, if it looks like fake news, it is probably fake news, and don't forward fake news.

Many governments in Africa are investing in e-services (e-government, e-voting, e-tax systems and many other portals.) Do you think the African citizenry is ready to consume and utilize these systems without the worry of privacy, security and fraud?

African society may not yet have gained full trust in e-services, from e-government to e-commerce. As they get used to using such services and noticing improved service delivery, then the trust will grow. E-government services are almost certain to be more accurate, more transparent and more efficient than existing manual systems which are often flawed with loopholes leading to inefficiency, corruption and financial loss.

What are some of the risks we face with the introduction of government driven e-services and do you have any examples of these cases in your country?

The main risk in implementing e-government is having pushback from cartels that are benefitting from corruption networks. If we look at the technologies, E-government, IoT, Blockchain and big data, they have the ability to totally transform and eradicate most forms of corruption, if implemented properly. But those cartels that profit right now may do their best to frustrate the implementation of technology that will cut off their income.

In 2017, we had several cases of Cyber security attacks including ransomware attacks across the world–were you impacted by these attacks?

If yes, how did you (company or country) respond to these cases?

Considering the shortage of skilled resources in Africa, how can we limit the impact of ransomware cases?

We were not impacted by ransomware at Liquid Telecom in 2017. But let us not pinpoint. I would consider myself a highly skilled experienced ICT professional, with long experience of leadership in technology. Yet in 2013 I picked up a ransomware from a downloaded Trojan and totally got my hard drive wiped. Just from my own carelessness, and lack of up to date antivirus tools employed by my highly skilled IT department in London.

Do you think organisations are spending enough money on combating Cybercrime and what can be done to encourage more spending on Cyber security issues?

Organisations are yet to understand what they should be spending on combatting Cyber-crime, and even where to spend it. Cyber Security and associated risks need to be understood at board level, since the average cost of the impact of a Cyber breach (estimated 1.3M$ per breach in US in 2017), is enough to bankrupt many companies. But there are ways to be smart about Cyber security spending. Deploying systems in trusted public cloud, may likely be more cost effective than managing the risks of deploying your own security on your premises. Cyber breach insurance will be a growing product that companies should consider.

Based on our research the Africa Cyber security market will be worth USD2 billion dollars by 2020. Despite this opportunity, Africa has not produced a single commercially viable Cyber security product/solution.

In your opinion, what should African countries and universities focus on to encourage innovation in the development of Cyber security solutions?

What role can the private sector and consumers of imported Cyber security products play to ensure we can encourage local players to start developing African grown Cyber security products and solutions or even services?

I would refute that statement.

Thawte, a security certificate company founded by South African Mark Shuttleworth in South Africa was a security company specializing in certificates for secure communications. Thawte was sold to Verisign for $575 million in 1999 making Thawte the first African tech Unicorn. African innovators should be inspired by Mark, and look to create Cyber security solutions that are well placed to deal with Cyber security issues in Africa at a price and service level that is good for the local market. What about a WhatsApp bot that you can add to your groups that will spot and delete fake news? African innovators need to start with a problem then go out and solve it.

In your opinion and from an African context, what are the top 2018 Cyber security priorities for African countries and organisations?

My top 3 priorities are, education, education and, education. All companies need to do their best to make sure the whole organisation understand and are aware of Cyber security, both at home and at work. IT departments and Infosec officers need to be educated to the highest level, but Cybersecurity, just like physical security, is the responsibility of every member of an organisation.

Threat Intelligence

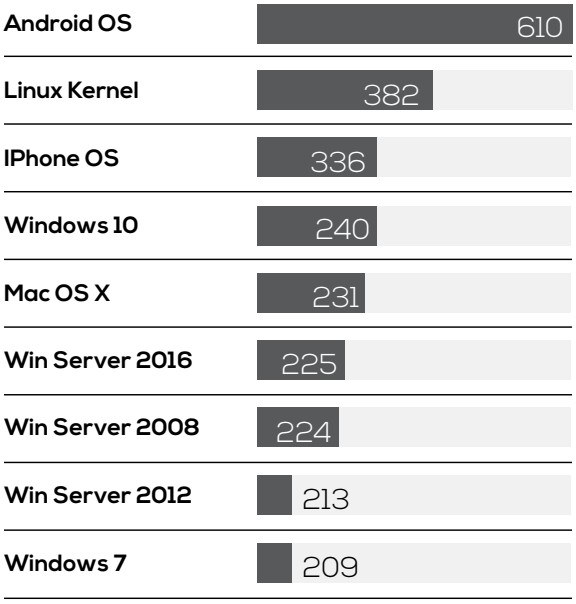
THE MAIN AIM OF THIS PHASE WAS TO IDENTIFY ACTIVE SYSTEMS EASILY ACCESSIBLE ONLINE AND USING THIS INFORMATION IDENTIFY AREAS OF WEAKNESSES AND ATTACK VECTORS THAT CAN BE LEVERAGED BY MALICIOUS PLAYERS TO CAUSE HARM.

We broke down the findings into the following sections:

- Open Ports
- Operating Systems
- Top Vulnerabilities by Application or Services

Vulnerabilities

OS with most Vulnerabilities



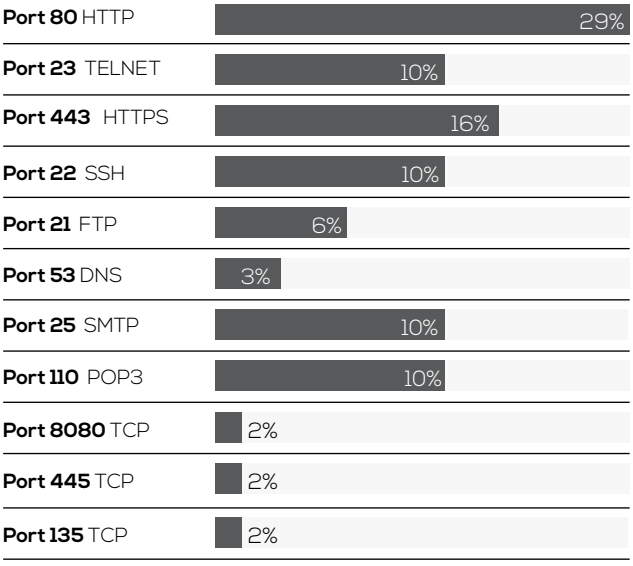
Open Ports

There is a total of 65,535 TCP ports and another 65,535 UDP ports, we examined risky network ports based on related applications, vulnerabilities, and attacks.

65,535 TCP ports

65,535 UDP ports

Top Open Ports



- TCP port 80, 8080 and 443 support web transmissions via HTTP and HTTPS respectively. HTTP transmits unencrypted data while HTTPS transmits encrypted data. Ports 25 and 143 also transmit unencrypted data therefore requiring the enforcement of encryption. These ports are commonly targeted as a means of gaining access to the application server and the database. Attacks commonly used include SQL injections, cross-site request forgeries, cross-site scripting, buffer overruns and Man-in-the-Middle attacks.
- TCP/UDP port 53 for DNS offers a good exit strategy for attackers. Since DNS is rarely monitored or filtered, an attacker simply turns data into DNS traffic and sends it through the DNS server
- TCP port 23 and 2323 is a legacy service that's fundamentally unsafe. Telnet sends data in clear text allowing attackers to listen in, watch for credentials, inject commands via [man-in-the-middle] attacks, and ultimately perform Remote Code Executions (RCE).
- UDP port 22 is a common target by attackers since its primary function is to manage network devices securely at the command level. Attackers commonly used brute-force and dictionary attacks to obtain the server credentials therefore gaining remote access to the server and deface websites or use the device as a botnet - a collection of compromised computers remotely controlled by an attacker.
- TCP port 21 connects FTP servers to the internet. FTP servers carry numerous vulnerabilities such as anonymous authentication capabilities, directory traversals, and cross-site scripting, making port 21 an ideal target.

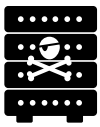
Top Operating Systems

Linux is considered more secure than Windows because of its architecture and the fact that most viruses and Trojan target windows systems.

However, as shown in the number of vulnerabilities discovered, linux users need to keep an eye for patches to the discovered vulnerabiliites.

Top Operating Systems

Linux	50%
Windows	45%
Others	5%



Top Harvester IPs

Harvester IPs

41.203.89.37	45%
41.203.93.115	45%
41.190.2.112	10%

Top Spam Servers

Spam Servers IPs

41.222.210.126	21%
217.14.88.242	16%
41.203.89.37	12%
41.203.93.115	12%
62.173.43.114	12%
62.173.32.85	6%
41.222.211.150	5%
41.190.17.13	3%
41.190.2.112	3%
62.173.32.5 | S	2%
41.222.208.65	2%

Total Count = 4,884

*Spam - Electronic junk mail
*A spam server- The computer used by a spammer ir order to send messages

Top Dictionary Attackers

Dictionary Attacker IPs

41.222.210.126	36%
217.14.88.242	20%
41.203.89.37	18%
41.203.93.115	18%
62.173.43.114	7%
62.173.32.85	4%
41.190.17.13	3%
41.190.2.112	3%
41.222.208.65	7%
212.100.73.4	4%

Total Count = 4,481

*Dictionary Attack - A dictionary attack involves making up a number of email addresses, sending mail to them, and seeing what is delivered.
Dictionary attackers typically send to common usernames

Vulnerabilities Discovered in Databases

Mysq<5.7	46%
MicrosoftSQL Server <13.0.1100.0	43%
Postgresq<9.2	8%
Oracle Web Logoic Admin HTTPD	3%
Oracle Glassfish <=3.1.2.2	1%
Mongo DB<3.0	0.3%

Babatunde Ajiboye

Manager, Governor's Department,

Central Bank of Nigeria, Headquarters, Abuja

Raising Consumer Awareness On E-Fraud: A Stich In Time

Nigeria has witnessed a lot of developments in the e-payments space since 2012. Several advances have equally cleaned up industry data on number of accounts and account holders through the introduction of the Bank Verification Number (BVN). Today, we have almost 31m account holders and when compared to the N56 Trillion moved on the NIBSS Instant Payment (NIP) platform, we will discover that an average of over N150,000 is moved per account holder every month or N5,000 daily. With the current efforts aimed at reducing Financial exclusion from 46.3% to 20% by 2020, we should therefore expect an additional 15 Million account holders, who will be on-boarded more with e-payment products as against the traditional banking products. Hence, a rise in transaction values should be expected.

Gladly, in our payments space we have not been ravaged with electronic fraud as current statistics show that the value of successful fraud cases has developed an inversely proportional relationship with the growth in e-payments highlighted earlier, as we have witnessed consecutive drops for three years straight in successful fraud cases in the light of the impressive growth in e-payments. This feat while being enough to part oneself on the back, it is also important to note that fraudsters are not sleeping but consistently looking for ways by which they can compromise a payment system that already has the world watching for its resilience, security and innovation.

It therefore requires that all Industry stakeholders should consistently be on the watch, especially around vulnerable areas of which the consumer of these e-payment products will be the focus of this paper. Developments in information and communications technology will no doubt significantly change the way we conduct business and conclude payments, a great part of this change will be driven via the mobile platform, thus increasing exposure of unsuspecting and unaware customers to do's and don'ts of the e-payment world.

On these new channels also comes unique vulnerabilities and most are directed at the consumer, however two that are considered major will be highlighted below;

1. Phishing and Social Engineering

Most payment platforms especially mobile phones are used for a mix of both personal and corporate usage. Mobile phones are gathering more and more information from the customer, which aggregated could help to carry out sophisticated attacks.

These attacks target the user by phishing emails and social engineering exploiting different communication channels (e.g. phone, email, SMS) and data about the user available in the public domain (e.g. social media sites, search engines). The data sought by attackers using social engineering are often payment card data and personal data (PINs) that the user should only know.

2. Installation of Rogue Applications and Malware

Fraudsters will find ways to install malware on the mobile device by phishing/social engineering a victim to open a malicious attachment in an email and by redirecting the user to a malicious URL.

Another possible channel for malware infection is insecure Wi-Fi hotspots (e.g. Internet cafes) that might allow an attacker to target the mobile device with Man-in-The-Middle. There is also the possibility of a network spoofing attack. That is when a malicious user setups a fake access point with same network name, as one that already exists, such as popular café

name or market chain. They might setup a fake website to "authenticate" users and this way collect data, then they can later use this data for next steps in their attack. It is not uncommon to see many people use same username and password for multiple different services, even for a mobile payment application, this is not recommended at all.

3. Possible Security Measures or Controls

If the Payments Industry must do something then it is the education of all consumers of e-payment products of their respective responsibilities using; "all effective means to educate consumers and business, including innovative techniques made possible by global networks" (OECD, 1999).

The Industry should as a matter of urgency embark on multi-agency and inter-governmental co-operation and co-ordination through the design of a methodology detailing guidelines for promoting safety in the e-payments space. Media (print, radio and TV) should be leveraged upon in the dissemination of this critical information to consumers.

The Nigeria electronic Fraud Forum (NeFF) has over the years provided a veritable platform for Industry collaboration in the fight against e-fraud, and the Forum again lends itself to realizing the success of this objective of rallying all stakeholders in executing this major frontier in the fight against e-fraud.

The Forum, under the amiable leadership of Mr. Dipo Fatokun, Director Banking and Payments System Department of the Central Bank of Nigeria, will seek to coordinate an industry response to this engagement, as we believe this initiative will be the proverbial stich in time that saves nine.

.ng

Your Nigerian Identity online

Domain Names are our identity on Cyberspace!

Claim yours today.

Domain Names are comparable to Real Estate

Contact
NiRA Accredited Registrars to register your Domain Names

www.nira.org.ng/ng

NiRA Office Address
8 Funsho Williams Avenue, Iponri,
Surulere, Lagos, Nigeria
Tel: +234-(0)8172004272, 0700CALLNIRA
Email: admin@nira.org.ng
Website: www.nira.org.ng

2017 Nigeria Cyber Security Survey


Nigeria

150
respondents

12
Industry Sectors

THE GOAL OF THE 2017 NIGERIAN REPORT WAS TO EXPLORE THE EVOLVING THREAT LANDSCAPE AND THE THOUSANDS OF CYBER-ATTACKS THAT HAVE BEEN FORGED AGAINST INDIVIDUALS, SMES AND LARGE ORGANISATIONS WITHIN NIGERIA. CYBERCRIMINALS CONTINUE TO TAKE ADVANTAGE OF THE VULNERABILITIES THAT EXIST WITHIN SYSTEMS IN NIGERIA AND THE LOW AWARENESS LEVELS. THIS SURVEY IDENTIFIES CURRENT AND FUTURE CYBER SECURITY NEEDS WITHIN ORGANISATIONS AND THE MOST PROMINENT THREATS THAT THEY FACE.

About the Survey

This survey was prepared based on data collected from over 150 respondents across organisations in Nigeria. They included companies from the following sectors:


Academic


Banking


Financial Services


Government


Healthcare Services


Insurance


Legal Advisory


Professional Services


Telecommunications


Others

The respondents who participated in this survey included technical respondents (predominantly chief information officers, chief information security officers, IT managers and IT directors) and non-technical respondents (procurement managers, senior executives, board members, finance professionals and office managers). The survey measures the challenges facing Nigerian organisations and the security awareness and expectations of their employees.

Summary of Findings

According to the survey findings, 99.4% of respondents have a general understanding of what Cybercrime is. With the many advances in information technology and the transition of social and economic interactions from the physical world to Cyberspace, it is expected that majority of individuals have a general idea of what Cybercrime is.

1. Cloud and IoT

We asked respondents whether or not they utilize Cloud services or Internet of Things and 65% of organisations surveyed responded affirmative showing that there is increased adoption of cloud and IoT usage within the continent with users mainly using services such as

The Mirai botnet exploited poorly secured IoT devices to perform the largest ever distributed denial-of-service attack.

Of concern, was the fact that majority of these individuals also indicated that they do not have policies in place to govern the usage of these emerging technologies.

Security concerns are evolving with the rapidly changing nature of cyber threats and our Cybersecurity research this year indicates a marked growth in the number of attacks and malware targeting cloud infrastructures and IoTs.

Does your organization allow or utilize Cloud Services or Internet of Things Tech (Big Data Analytics)?

Organisations that allow or utilize Cloud Services or IoTs Tech **65%**

Does your organization have a best practice policy for IoT and Cloud Services?

50% lack policies to govern the usage of Cloud Services or IoTs Tech

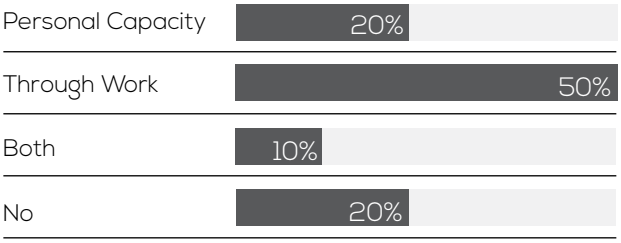
2. Cybercrime

The explosion in online fraud and cyber-crime affected almost 80% of all our respondents, most of them through work. This means majority of attackers are targeting organisations and people working for these organisations.

However an interesting fact is that 20% reported to not have experienced cyber-crime. From our analysis, majority of these people do not understand what qualifies as cyber-crime. As such, a huge percentage of people lack the ability to recognize a cyber-attack when it occurs.

Have you been a victim of any cybercriminal activity in the last 5 years? In what capacity?

80% of the respondents have been victims of Cybercriminal activities



3. Impact of Cybercrime

When asked about the business impact of cybercrime, loss of money and system downtime was highlighted as highest. Other significant consequences included loss of reputation, psychological harm and a combination of all the above.

This presents one conclusion- that majority of attacks in Africa are motivated by financial gain – suggesting reasons why financial institutions, Saccos

and organisations that deal primarily with transaction processing are major targets for the Cyber-attacks.

How has Cybercrime impacted on you?

Majority of the respondents have had an impact of cybercrime

System Downtime 30%

Money Lost 35%

Reputational Loss 15%

4. Reporting of Cybercrime

Internet-related crime, like any other crime, should be reported to the appropriate law enforcement or investigative authorities. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement.

If you have been a victim of cybercrime, what action followed?

4% reported cases were followed up to successful prosecution

Did not report to the police 77%

Reported to the police with no further action 9%

Reported to the police, who followed it up to successful prosecution 4%

Reported to the police, who followed it up but no successful prosecution 6%

Didn't know how to report to the Police 4%

5. Cyber security Spending

Cyber security spending is on the rise. From our analysis in 2016, 95% of respondents spent spend less than $5000 on cyber security annually. In 2017, we have seen a slight improvement of 7%. 88% of respondents reported to have spent less than $5000 on cyber security.

Further analysis also revealed that majority of organisations that spend over USD 10,000 came from the Banking and Financial sectors. This is not surprising since they are the most targeted.

Majority of companies which spent more than $5000 had 1000+ employees

Approximately how much does your organisation spend annually on cyber security?

organisations that spend less than US $5000 on cyber security

2016 95%

2017 88%

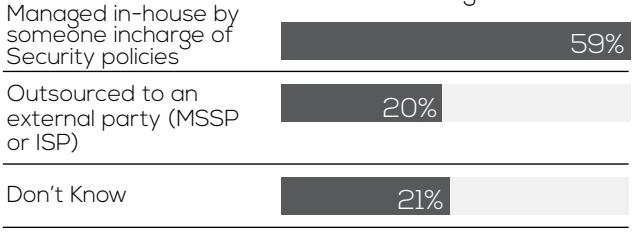
6. Managing Cyber Security

59% of organisations manage their cyber security inhouse while 20% have outsourced these services to an external party (MSSP or ISP). More companies, particularly Banking and financial institutions, are now developing inhouse capabilities to manage cyber security. Also key to note is that the number of organisations, most of which come from the banking, financial services, healthcare and insurance sectors now outsourcing the entire security function, has increased by 3% from last year.

Our survey also revealed that at 73%, Academic sector respondents did not know how their cyber security was managed. This was closely followed by 10% from the Manufacturing sector and 10% from the Health sector.

How is your organisation's cyber security managed?

20% of the respondents outsource the entire security function for their organisations

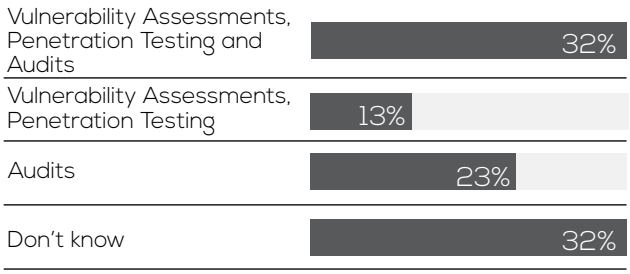


7. Cyber Security Testing Techniques

Security testing is a process performed to reveal flaws in security mechanisms and find the vulnerabilities or weaknesses in the environment. Recent security breaches of systems underscore the importance of ensuring that your security testing efforts are upto date. From the survey, only 32% of the respondents perform a combination of vulnerability assessments, penetration testing and audits. 13% perform penetration testing while 23% perform Audits. All these testing techniques are not independent and in fact work best when they are applied concurrently.

Which of the following security testing techniques does your organization use?

68% of the respondents carry out security testing techniques in their organisation



8. Cyber Security Awareness

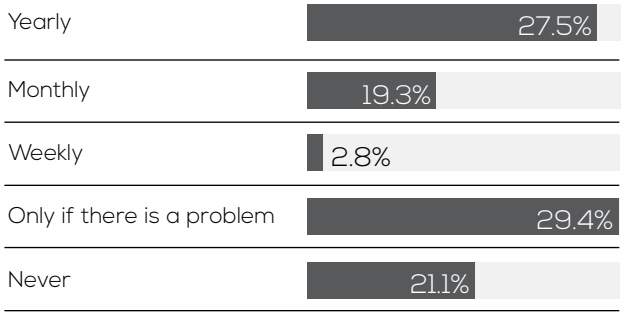
The level of awareness in Nigeria is still low with 21% of organisations missing an established cyber security training program.Many organisations (29.4%)are also still very reactive when it comes to cyber security training, only choosing to train their staff when there is an incident/problem. This is worrying considering 50% of all cyber attacks reported in the survey were through work. In 2017 alone, over 50% of the malware reported was spread through some form of social engineering.

On the other hand, it is important to point out that 50% of the respondents reported to have a regular training program in place. The importance of having regular security training for employees cannot be over emphasised.

How often are staff trained on cybersecurity risks?

49.6% of the respondents are regularly trained

while 21.1% of organisations DO NOT train their staff on cyber security



9. Information Sharing

Few organizations can really work in a vacuum and no organization can see all of the threats laying in wait on the internet. Despite this, our survey revealed that 40% of organisations do not keep up to date with cyber security trends and attacks.

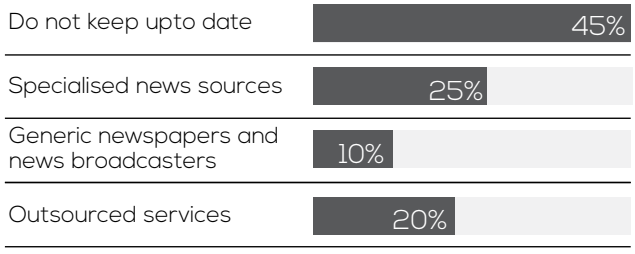
This has resulted in duplication of attacks across various industries as illustrated by the recent Wannacry and Petya Ransonware attacks.

On the other hand, many organizations are wary of sharing sensitive cybersecurity information, especially with government institutions, regulators and peers. Not only can such information jeopardize the security position of an organization, but it also can damage customer perceptions and even affect its stock market value.

Still, it is important for organisations and regulators to put in place infrastructure that will ensure safe sharing of information.

Is there a dedicated role or person within your organisation assigned to distributing or communicating latest cybersecurity updates?

55% of the respondents keep upto date with cyber security news from various sources



Revd. Sunday Folayan

President,

Nigerian Internet Registration Agency (NIRA)

The Need to Review the Nigerian Cybercrime Act 2015

Background

Whereas the Nigerian Cybercrime Act was passed by the 7th Assembly of the Senate in October 2014, the act was finally signed into law on the 15th of May 2015, it has not been given the necessary and full enforcement that it deserves.

The 2015 Act was made to contain the growing spate of Internet offences by seeking to arrest, prosecute and sentence anyone found guilty of committing cybercrime and allied offences but it lacks critical parts to make the Internet a safer place for Nigerians. One of the major challenges why this is so, is because the Act did not explicitly prescibe an agency that is responsible for the operation of the Act.

While this is not indeed a problem where cooperation is the norm, it leaves very deep holes in the administration of justice, because these holes can be exploited by Cybercriminals to an advantage. Similarly, Some stakeholders have alluded to the fact that while criminals move at the speed of light, Law enforcement continue to move at the speed of Law. The imperative is that the Law needs to be constantly updated to be able to deal with the various challenges posed by the rapid advances in technology.

It is therefore important to urgently review the Nigerian Cybercrime Act, so that it can remain relevant and useful in the administration of justice in Nigeria, with special emphasis on the Cyberspace.

The Existing Nigerian Cybercrime Legislation

The following are some of the challenges and or loop holes that have been identified in the existing legislation:

1. Though the Act is already two years old, it should have been tested by now.
2. The criminal provisions in the Act are generally adequate but need some refinement.
3. There are very obvious typographical errors in the Act
4. There is a weak or almost zero enfircement provisions in the Act
5. Some provisions in the act are too specific, and may give room for offenders to devise other means of committing crimes outside the specific definitions of the law.
6. There is the need to strengthen the provisions that deal with procedural rules in the act.
7. For some offences, some provisions in the act are very nebulous
8. A lot of provisions extraneous to both criminal law a very strict area of law, and cybercrime law as a technology field; wre erronously incorporated in the Act.
9. There is no clear agency responsible for the enforcemnt of the Act. Rather the Act uses the term "All relevant agencies".
10. There is nothing in the Act that defines what the Cybersecurity fund should be used for.
11. Indeed, it is not clear which agency administers the Cybersecurity Fund.
12. There is the need for the government to fully articulate a number of these issues and collaborate with the citizens to have a proper framework as to the workings of the Act.

13. The issue of the expertise of the Local Enforcement Agents in prosecuting cybercrime and related cases is also suspect

14. The Federal High Courts will be overburdened as they have been made the exclusive court to handle issues arising from cyber crime offences.

At different fora, some stakeholders have expressed opinions on what to do with the Cybercrime act and other similar ICT legislations, to make them more useful. These include:

1. Amending the act to create a directorate for Cybersecurity, that will be on the same level as the DSS, NIA, etc. The agency will be responsible for the coordination of all activities that have anything to do with Cybersecurity.

2. Amending the Act to create an agency, (just like NAFDAC for Pharmaceuticals, EFCC for Financial Crimes etc), to be conferred with the authority to enforce cybercrime and assure cybersecurity in the country.

3. Recognizing the fact that the Private sector is not in full support of ngCERT being in ONSA. They prefer the ONSA managing the Military cert (MilCERT) and NITDA managing the Government CERT (GovCERT), with all these CERTS feeding into the ngCERT.

4. The need to activate the National Cyber Security Coordination Center NCSC which will be at the apex of the Cybersecurity framework. This can best be rejuvenated moving forward, through a review of the 2015 act.

It is therefore a necessary to urgently and quickly review the existing Act to make it more relevant and useful as a law that will curtail the menance of Cybercrime in Nigeria.

The review will correct some obvious mistakes, give the existing Legislation an international face lift, harmonize the various positions that will make the Act more applicable for combating cybercrime in Nigeria and deliver an act that meets and exceeds the expectations of all stakeholders in Nigeria.

Finally, to enhance operational efficiencies for businesses. It is very important, and in fact inescapable, that Nigeria considers merging the three legal frameworks namely; Nigerian Communications Act; National Information Technology Development Agency Act; and the National Broadcasting Commission Act, into one "converged" legal and regulatory regime for ICT.

Summarized Findings Report – What are Cybersecurity Gaps in Nigeria?

*Reporting approach adopted from Cyberroad-project and survey

Theme	Scenario	Consequence(s)	Mitigation	Identified Gap(s)
Database Security	Limited visibility on activities on the databases.	**1. Fraudulent database postings!** **2. Loss of sensitive information!**	24/7 monitoring of activities within databases. Limit and monitor access to database. Audit and review privileged access to DB.	How can Nigerian companies improve visibility on DB activities at a cost effective and resource friendly manner?
Privileged User Management	Compromised administrator accounts.	**Unauthorized access to critical systems within the organisations!**	Audit the activities of privileged users within the network.	How can organisations implement segregation of duties when resources (staff) are limited?
Patch Management	Missing patches contribute 70% of vulnerabilities identified. 60% of these are never mitigated.	**Exploitation of missing patches to compromise confidentiality, integrity and availability of critical informational assets!**	Remediation roadmaps that ensure that critical patches are applied while medium and low risk vulnerabilities are fixed within a stipulated agreed upon period.	How can Nigerian organisations maintain a patch management program without exhausting resources?
	Employees are trained only after an incident.	**Employees fall victims of social engineering attacks!**	Regular employee training programs that have an effectiveness measuring metric.	How can organisations ensure employees understand the concepts taught during awareness workshops/ trainings?
Training and Awareness	IT Training is done on specific tools.	**IT teams lack the expertise for defensive and offensive security!**	Regular training on both defensive and offensive Cyber security concepts.	How can IT teams widen their gaze from being "tool analysts" to network engineers and architects?
	Board members lack Cyber security expertise and rely on standard audit reports to understand the security posture of organisations.	**Lack of visibility on actual Cyber security posture!** **No standard way of measuring progress and ROI on IT investments!**	Board training to involve reporting metrics for enhanced visibility that can provide a basis and guide on future decision making.	How can Board members shift from the traditional "oversight" role into the proactive Cyber security role?
Network Security Engineering	Limited expertise in the country on Security Architecture/ Engineering skill set.	**Networks are misconfigured to allow easy manipulation and system sabotage!**	Organisations to invest in or outsource security engineers/ architects for network design purposes.	Where can organisations get specialized training on security architecture/ Engineering?

Theme	Scenario	Consequence(s)	Mitigation	Identified Gap(s)
 **Insider Threats**	Greedy and Disgruntled employees are being recruited by cartels to launch attacks	**Compromise of administrator accounts** **Privilege escalation** **Malicious transaction posting** **Data exfiltration** **Sabotage of critical systems**	Audit and monitor activities of privileged accounts Segregation of duties Develop a user access matrix	How can Nigerian organisations share information on malicious insiders?
 **Continuous Monitoring**	**Multiplicity** - Remote Access to critical system after business hours goes undetected	**Compromise of confidentiality, Integrity and Availability**	Multiplicity as an Indicator of Compromise – Establish a baseline for what is normal.	
	Velocity – Multiple failed logins to critical system within a short period of time goes undetected by security teams	**Compromise of confidentiality, Integrity and Availability**	Velocity as an Indicator of Compromise - Establish a baseline for what frequency is normal for the organisations.	
	Volume – Bulk transactions go undetected by security teams	**Compromise of confidentiality, Integrity and Availability**	Volume as an Indicator of Compromise - Establish a baseline for what number, bandwidth or utilization metric is normal for the organisations.	How can Nigerian organisations establish a baseline for what "normal" is.
	Limits - Security personnel are unable to determine a baseline for understanding limits as an indicator of compromise.	**Malicious postings of transactions**	Limits as an Indicator of Compromise - Establish a baseline for what threshold is normal for the organisations	

Inter Industry Analysis - Africa

SECTOR	Banking and Financial Services		Government		Telecommu-nications		Other Industries	
YEAR	'16	'17	'16	'17	'16	'17	'16	'17
Been victims of any cybercriminal activity in the last 5 years; Through work	59% ↓	55%	63% ↑	67%	67% ↓	65%	48% ↑	51%
Organisations spending below $1,000 USD annually on cyber security	33% ↓	30%	45%	45%	30% ↓	27%	48% ↑	50%
Organisations with Cyber Security managed In-house	63% ↓	55%	58%	58%	71%	71%	40% ↑	48%
Yearly training staff on Cyber Security risks	39% ↑	45%	45% ↑	47%	55% ↑	57%	38% ↓	33%
Organisations that allow Bring Your Own Devices (BYODs) usage	20% ↑	26%	60% ↑	61%	49% ↓	40%	60%	60%
Organisations who lack BYOD policy	30% ↑	35%	74%	74%	60% ↓	56%	57% ↓	55%
Organisations utilizing Cloud Services or Internet of Things Tech (Big Data Analytics)	*	46%	*	43%	*	40%	*	58%
Organisations which lack an IoT and Cloud Policy	*	35%	*	71%	*	54%	*	54%

* No statistical analysis done in 2016 on this section.

Dr. Peter Tobin

Privacy and Compliance Expert

BDO IT Consulting Ltd

Mauritius

Love it or hate it, the GDPR is here to stay!

Historical context for the GDPR

Global recognition of the importance of data privacy can be traced back to the United Nations (UN) which has a long history of promoting the right to privacy through its Human Rights treaties. This includes article 12 of the Universal Declaration of Human Rights in 1948 and article 17 of the International Covenant on Civil and Political Rights in 1966. More recently in July 2015 the UN appointed a "Special Rapporteur on the right to privacy" to bring additional focus to the importance of data privacy. Supporting the UN is the Organisation for Economic Co-operation and Development (OECD) which in 1980 issued its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" which were revised and re-issued in 2013, just as the POPI Act (POPIA) was gazetted in South Africa, allowing that country to join the growing list of those forming part of the African community of nations that have embraced personal data protection legislation. Following the UN and OECD initiatives, nearly one hundred countries and territories have established or are developing data protection laws.

African personal data privacy and protection developments

In Africa, the African Union (AU) Commission and the Economic Commission for Africa have spearheaded the development of the AU Convention on Cybersecurity and Personal Data Protection, which was adopted by the AU Heads of States and Governments Summit in June 2014 in Malabo, Equatorial Guinea. Eight Countries had already signed the convention by July 2016 according to AU Commission: Benin, Chad, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia. At a regional level in Africa there are also several initiatives, notably the ECOWAS Cybersecurity guidelines and the SADC Model Law on data protection, e-transactions and cybercrime. There is also the HIPSSA initiative (Harmonization of the ICT Policies in Sub-Saharan Africa) which covers 30 countries across the continent. Latest estimates show that 16 African countries have data privacy legislation, with an additional 14 countries working on legislation, leaving a balance of 24 currently having taken no action so far. There are some leading examples in Africa, such as Mauritius which passed the Mauritius Data Protection Act (MDPA) in late 2017, swiftly brought the MDPA into full force in January 2018 and thus positioned itself as a leading nation in Africa and the Indian ocean island states in terms of alignment with the European Union and its General Data Protection Regulation (GDPR).

So what is the European Union GDPR?

During 2016 the General Data Protection Regulation – commonly known as the GDPR – was finalised, with a transition period to full compliance required by those organisations impacted - those processing directly (controllers) or indirectly (processors) the personal data or EU residents - by May 2018.

The GDPR has potentially wide-ranging implications for companies based outside the EU (increasingly often in Africa) trading with the EU member states. Of particular interest is the following extract from the GDPR document: "The [European] Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision." This opens the door to leading practice nations and sectors stealing a march over their competitors in the global marketplace for information services provision where personal data is processed.

So what, briefly, is the GDPR (www.eugdpr.org)?

The GDPR is a single regulation that automatically applies to all current and future European Union members states from May 2018.

In the case of the United Kingdom (UK), there were strong indications at the time of writing this article that the UK would fully align itself with the GDPR even post "BREXIT" (the exit of the UK from the EU). The GDPR has 173 introductory clauses (sometimes referred to as the recitals, a form of explanatory pre-amble), with the main regulation body comprising 11 chapters made up of 99 Articles which come to over 400 numbered paragraphs. It is important to remember that the GDPR works in conjunction with other EU directives and regulations at an EU level, and may be complemented by local legislation, whether in EU member states or in African countries that are seeking to align themselves to the GDPR.

After chapter 1 which contains a series of general provisions and definitions, chapter 2 covers the principles of data processing, which have been refined since the previous EU personal data protection directive of 1995. Chapter 3 addresses the "Rights of the Data Subject", those EU-resident individuals whose personal data may be processed by one of more the main parties who need to comply with the GDPR: the Controller (typically an organisation such as a business or arm of government) that determines and controls the processing of the personal data and the Processor, a service provider which renders personal data processing services to one or more Controllers. There are other Third Parties that may be involved, such as those organisations where the Controller shares personal data for a variety of legitimate reasons. Chapter 4 looks at the duties of the Controller and Processor.

Chapter 5 addresses the Transfer of Personal Data to 3rd Countries or International Organisations, an important consideration when dealing with countries in Africa that, for example, host outsourced personal data processing services for EU-based Controllers. Some of the chapters of the GDPR are really only of interest to the supervisory and regulatory authorities (such as chapters 6, 7, 10 and 11), whilst others discuss important issues such as remedies, liability and penalties (Chapter 8) which can have serious consequences for Controllers or Processors who do not meet the requirements of the GDPR.

Key changes in the GDPR

Compared to the earlier EU-wide directive of 1995, the GDPR contains a number of key changes. These include the increased territorial scope of the GDPR (extra-territorial or non-EU member state applicability; significant increases in potential penalties (rising to up to 2% to 4% of global turnover of either or both of the Controller or Processor found at fault by the supervisory authorities). There have also been changes to the nature of consent which can be used as a justification of lawful processing, including expanded requirements in terms of the record keeping for consent given, refused or withdrawn. Whilst some countries have already implemented strict rules around data breach notification, the GDPR emphasises to requirement to normally notify the supervisory authorities within 72 hours of a data breach being confirmed (perhaps after an initial check that the data breach is real and not imagined or only suspected). Data subject rights have also been clarified and expanded to include the much-discussed "right to be forgotten" (erasure of personal data) as well as the right to data portability, such as when moving between service providers. "Privacy by design and default" also represents not only a new requirement but one which addresses the approach to personal data privacy as "built-in" not just "added-on". The last major change highlighted by the EU is the enhanced and expanded (broader and deeper) role of the Data Protection Officer (DPO).

Beyond the vanilla GDPR

It is important to be aware that the GDPR in its basic format has already been complemented by a number publications by the group that will over time become the collective body for supervisory authorities in the EU (European Data Protection Board, established under Article 68 of the GDPR), although operating at the time of writing under the "Article 29 DPWP" branding (perhaps somewhat confusingly, that's Article 29 under the 1995 directive and not under the GDPR). Further guidance is already planned in areas such as consent, transparency, profiling, high risk processing, certification, administrative fines, breach notification and data transfers.

So how is your compliance status?

Here's a quick review of some of the key considerations when preparing for (or maintaining) compliance with the GDPR. Can you prove that:

1. You comply with the 6 principles relating to personal data processing? (Article 5: Principles relating to personal data processing)
2. You comply with the lawfulness of processing rules? (Article 6: Lawfulness of processing)
3. You have records of consent that meet the required conditions? (Article 7: Conditions for consent)
4. You have provided all necessary information at point of collection? (Article 13: Information to be provided)
5. You have a policy, process and procedures to ensure a) right of access; b) to rectification; c) to erasure; d) to restriction of processing; by the data subject? (Article 15 - 18: Right of access; to rectification; to erasure; to restriction of processing)
6. You are meeting all the responsibilities of the controller? (Article 24: Responsibility of the controller)
7. You have data protection by design and by default? (Article 25: Data protection by design and by default)
8. You have a representative in the EU? (Article 27: Representatives of controllers not established in the Union)
9. You have adequate records of processing? (Article 30: Records of processing activities)
10. You have adequate security of processing? (Article 32: Security of processing)
11. You have a policy, process and procedures for data breach notification to the supervisory authority? (Article 33: Notification of a personal data breach to the supervisory authority)
12. You have a policy, process and procedures for data breach notification to the data subject? (Article 34: Communication of a personal data breach to the data subject)
13. You have conducted data protection impact assessments where necessary according to the screening rules? (Article 35: Data protection impact assessment)
14. You have, where necessary, appointed an appropriate data protection officer following the EU requirements? (Article 39: Tasks of the data protection officer)
15. You have appropriate safeguards for cross-border transfers? (Article 46: Transfers subject to appropriate safeguards)
16. You have trained your staff in all of the above aspects and more (Article 39: Tasks of the data protection officer)

So maybe you didn't score full marks and are beginning to hate the idea of all the effort it might take to climb the GDPR mountain if you need to. But perhaps it's also time to look on the bright side, and learn to love the GDPR. It might just be that the next big contract you land with a client in Europe or service work you perform for an organisation outside the EU but with clients in the EU, provides the bonus you have been promising yourself all year.

One way or the other, love it or hate it, the GDPR is here to stay!

Cost of Cyber Crime

Analysis – 2017

IN THIS SECTION, WE LOOK MORE CLOSELY AT THE COST OF CYBERCRIME IN NIGERIA, IN PARTICULAR, TO GAIN A BETTER APPRECIATION OF THE COSTS TO THE LOCAL ECONOMY.

From our research and analysis, we estimate that Cyber-attacks cost Nigeria businesses around $649 million a year, which includes direct damage plus post-attack disruption to the normal course of business.

Nigeria

Cost of cyber-attacks

$649m annually

Methodology

Our assessments are, essentially, based on reported incidents of Cyber crime, our insider knowledge when handling cases of Cybercrime, estimates and assumptions.

We have drawn from information in the public domain, law enforcement and economics experts from a range of public and private-sector organisations and our tremendous knowledge of numerous incedents.

With this said, the boundary between traditional crime and Cybercrime remains fluid. Therefore for our research, the term Cyber-crime refers to:

> The traditional forms of crime committed over electronic communication networks and information systems and crimes unique to electronic networks, e.g. attacks against information systems, denial of service and hacking.

A significant proportion of this cost comes from the insider threat, which we estimate at $194M per annum. In all probability, and in line with our worst-case scenarios, the real impact of Cyber crime is likely to be much greater. As for measuring costs, this report decomposes the cost based on these 4 categories:

- **Costs in anticipation of Cybercrime,** such as antivirus software, insurance and compliance.
- **Costs as a consequence of Cybercrime**, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise.
- **Costs in response to Cybercrime,** such as compensation payments to victims and fines paid to regulatory bodies.
- **Indirect costs** such as reputational damage to firms, loss of confidence in Cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.

$649m annually

Type & Cost of Cyber Crime in Nigeria

Insider Threat	30%	$194M
Attacks on Computer Systems (Unauthorized Access and Malware)	20%	$130M
Social Engineering and Identity Theft	15%	$97M
Email Spam & Phishing	12%	$78M
Data Exfiltration	10%	$65M
Online Fraud Scams	8%	$52M
Ransomware	5%	$33M
	TOTAL	$649M

Joseph Mathenge

Chief Operational Officer

Serianu Limited

Approach in Raising Cyber Security Poverty Line

Poverty as is loosely defined is the inability to meet basic needs. Unfortunately here in Africa we have experienced the overwhelming sense of hopelessness in being unable to meet any one life basic needs.

In our report we build on the concept of the Security poverty line in which an organization is seen to be unable to effectively protect itself from a cyber threat.

In 2018 all organization needs to measure whether they have adequately invested to protect, detect, respond and recover to cyber events. So in discussing poverty in cyber security one will need to understand what are basic cyber security needs. In no order of priority, basic cyber security functions will include:

Ability to Identify Threats

- What can attack the organization?
- How would they attack?

Actively Protect Information Assets

- What would they attack?
- What are my information assets?
- What is the value to my organization?

Ability to Detect Cyber Incident

- Are there alerts to detect cyber events?
- How long does it take to detect events?

Understand How To Respond and Contain Cyber Event

- In receiving the alerts is there a methodology to responding?
- Does the organization have roles and responsibility defined for cyber events?
- Can we measure during attack extent of event?

Have resilience and ability to recover from cyber event

- What is the organisations ability to operate during an attack?
- Is there a documented recovery methodology?
- Are their resources (data backup and alternative systems) to help recover?
- How often are these tested to measure effectiveness?

In reading through this, one may ask what tools are available to measure each of the above areas.

There are several resources available to help assess these areas. Beginning with perhaps the simplest and least expensive is a self-assessment using template or questionnaire downloaded from resources such as NIST or the SANS Institute. An organization without internal resources with expertise in technology or cyber security might struggle working through the terminologies found in such templates.

However, they innately understand their operating environment and have the best knowledge in identifying impact a threat may have on the business. The next level would be engaging an external third party to conduct an assessment. Most organizations contract external parties to conduct a Vulnerability assessment and Penetration test (VAPT). These assessments, while are good and indicative of vulnerable areas may not fully explore all the areas required to ensure Cyber Security basic needs are met.

Additionally the output tends to be technical in nature showing systems and vulnerabilities in terms of lack of patching or misconfiguration of systems. It is imperative that the output is contextualized in terms of business critical process to help create and implement and effective remediation plan.

Having measured your organization against each of the above needs where should one begin? Particularly if all indicate that the organization scores poorly in each area, is there one area that should be prioritized?

Security practitioners and academicians would probably offer convincing arguments and positions on what is most important. I offer the following as a practitioner from my experience on which I have been successful in improving global organizations in raising their cyber security posture.

- Ability to detect cyber security incident and classify its impact.
- Ability to respond and contain event.
- Build the ability to exercise resilience during the event and quickly recover from the event.

In concentrating limited resources in building the above capabilities, I have realised exceptional value in protecting and organizations information assets.

Additionally I have found a clearer path in associating the above activities to key business goals around risk management. This becomes essential in making the business cases to business leaders and having them avail budgets in order to raise an organization cyber security posture.

Sector Ranking

Banking/ FInancial Sector

Hacking has become a real menace for Nigerian banks as they have become targets both internally and externally experiencing losses amounting to billions of Nairas. Recently, Nigerian banks were among the countries targeted by North Korean hackers Lazarus. The Central Bank of Nigeria rates e-fraud as the biggest risk in the financial sector which has widely incorporated electronic payment solutions such use of ATMs, NIP and Mobile banking.

Customers are experiencing losses and inconveniences after their deposit banks become victims of cyber fraud. New innovations such as Remita Application serve to heighten the risk in this integral sector- this application provides a single interface for use across multiple banks and currently has 8 of the major banks in use.

Intelligence gathering and Information sharing by key industry players has been called for by Cyber Security Experts as a way to prepare and mitigate the risks that come with digital banking and payment solutions.

Telecommunications

Attackers are now targeting Telcos with the intent to disrupt service delivery and infiltrate the data that they hold. This year, SIM Swap and USSD e-payment fraud are currently a serious cyber threat in the telecommunications industry. Fraudsters conduct Sim swaps of targeted individuals then conduct USSD based unauthorized transactions costing victims great losses.

The Central Bank of Nigeria in association with the National Communications Commission is working on laying down frameworks that will enable financial organizations to detect and potentially prevent this kind of fraud.

CYBER SECURITY IS NO LONGER A CONCERN FOR THE FINANCIAL & BANKING SECTOR ONLY. AS THE ADOPTION OF INTERNET USE AND AUTOMATED SERVICES INCREASES ACROSS ALL INDUSTRIES, CYBER SECURITY COMES ALONG AS PART OF THE PACKAGE. IN NIGERIA, AS IN THE REST OF THE WORLD, THERE HAVE BEEN INSTANCES OF CYBER COMPROMISE, ATTACKS AND ATTEMPTS THAT HAVE RAISED CYBER SECURITY TO A CRITICAL LEVEL. CYBER SECURITY KEEPS METAMORPHOSING ACROSS A WIDE RANGE OF FIELDS. HERE IS A MOST CURRENT RANKING OF DIFFERENT SECTORS FACING DIFFERENT CYBER RISKS.

Education

Compromise and defacement of websites that are used for various key processes by academic institutions is the most common threat facing the academic sector.

The JAMB website was recently compromised by a number of hackers from various states who had tampered with registration of the Unified Matriculation Examinations.

This is becoming a serious concern for academic institutions that use their websites for grading, examination administration and registration as these are lures for fraudsters and hackers. It is important to ensure website security and put in place measures to detect and respond to such incidences.

Mobile Services

Mobile money is one of the most embraced technology platform in Nigeria and Africa as a whole. Being a core aspect of transacting, mobile money is also integrated into the other sectors including hospitality, banking, transportation, telecommunication, E-commerce, Government and other financial sectors. As a towering platform, mobile money can be a single point of success just as easily as it could be of failure. With platforms such as UMo, GTMobileMoney, PocketMoni, Ecobank Mobile Money and Fortis Mobile Money, payment convenience has been achieved in most of the sectors mentioned above. Mobile money in Nigeria has experienced numerous attacks through social engineering, use of malware and account personifications. As one of the alternative channels for most banks, hackers are now exploiting the weak security controls around the mobile money platform to steal millions of dollars.

Olufemi Ake

Country Manager, Nigeria | Ghana

ESET

In the year 2017, what were the key Cybersecurity products that clients purchased?

Based on our internal data, the product with the highest sale is the Endpoint Security which offers all-round proactive protection and security for business devices, including mobile phones, tablets and computers. At some point in the year, we also experienced a temporary surge in demand for the Internet Security version of our product due to consumer customers seeking to prevent ransomware attacks on their personal devices.

Based on your opinion, which products have a higher market appetite?

Firewalls.

What are the clients' top priorities or needs to be addressed when purchasing Cybersecurity products?

Our clients' priorities vary depending on the existing infrastructure, number of staff and user policy. We have clients that have top priorities on prevention of the loss or exposure of their Organisation data. These clients, you will find out that they process sensitive transit data and may have staff who are constantly on the move with the information from one point to the other. These clients will certainly seek for Data Loss Prevention (DLP) solution to help them monitor the transfer of the data as they move and strictly control unauthorized access in case of device loss or theft.

There are other categories of clients who are keen on preventing various forms of malware from infiltrating their network due to the fact that they constantly interact with the Internet and also relate to external users who are prone to exposing the company to risks of cyberattacks. These type of customers would be keen on Endpoint Security solutions.

Email Security is also very essential as the majority of company's threats come in through this channel, mainly from email attachments or web links which sometimes may be embedded in the body of the email as a clickable image. These mails are mostly catchy and highly likely to lure users into clicking. Unfortunately, this is the least sought products in our portfolio and serve as the most a key component to securing company data and assets.

What makes the local market unique when choosing what Cybersecurity products to invest in?

There is no doubt that every cybersecurity product has its specific sets of benefits to respective users and with immense potential to impact Organisation's ROI as the need to secure our devices and activities both online and offline has never been this vital. The growth recorded in the ICT sector makes our market very unique as the sector marked its first double-digit growth in 2015 which accounted for more than 11% of Nigeria's Gross Domestic Product. Over 93 million mobile devices are currently connected and the e-commerce sub-sector equally process hundreds of thousands of online transactions, handling sensitive third-party data on a daily basis with tons of data being exchanged every minute. This goes to show a higher risk of exposure as cyberattacks in our market is far-becoming 'when' as against 'if' you will be hit.

Based on your previous experience, what are the most critical Cybersecurity challenges being faced by the local market?

The most critical cybersecurity challenges is the human factor. A company's network security is as good as its weakest link. An Organisation could have millions of dollars ICT security investment, but if the 'user' or staff is 'weak' when it comes to taking measures not to expose the organisation, it nullifies the efforts of other parties involved. Users need to be constantly educated on best practices and safe computing while handling personal or company's data within and outside the company network.

Asides the human factor, data is most critical. Ensuring that data is secure has become more important to home and business operations considering the volume of information being shared across the Internet on a minute-by-minute basis. Exhaustive data security should start with a comprehensive strategy and risk assessment to help the company or user identify the worth of the information they hold and how susceptible they are to cyberattacks.

Necessary measures such as access control (2FA), intrusion prevention systems, anti-malware and anti-phishing solutions, device control and web filtering policies, network traffic analysis tools, patch management solutions, data loss prevention and encryption, backup & recovery etc should be put in place as measures to keep data secured while constant education of human serves to complement the measures.

Promoting An Information-Rich Environment

In today's world, robust socio-economic environments thrive on effective and efficient communications infrastructure and services.

This is why we shall not relent in exploring modern and innovative ways to achieve regulatory solutions that promote information-rich environment.

As a responsive and innovative telecommunications regulator, we are guided by the principles of fairness, firmness and transparency in the promotion of access to information by all.

Be a part of our connected environment of endless apportunities. Your partneship counts.

NCC...Connecting Nigeria

NIGERIAN COMMUNICATIONS COMMISSION

Nigerian Communications Commission
Plot 423, Aguiyi Ironsi, Street Maitama, Abuja, Federal Capital Territory,
Tel: 234-9-4617000 Fax: 234-9-4617514
www.ncc.gov.ng

Home Security

OUR CULTURE, PAN AFRICANISM, EMPHASISES ON THE NEED TO BE MINDFUL OF FELLOW AFRICANS. WE'RE ALL CONNECTED VIA THE SHARED NETWORK WE CALL THE INTERNET. IT IS IN OUR OWN BEST INTERESTS TO MAKE SURE EVERYONE – FROM THE YOUNG TO THE OLD, ON SNAPCHAT, FACEBOOK AND TWITTER - KNOW AND PRACTICE BASIC SECURITY HABITS.

This section highlights top trends and security issues and corrective measures for security in our homes.

IP Cameras/Nannny Cams

For young parents, a baby monitor is an essential device to check on the baby's welfare. Majority of these devices are misconfigured and have default passwords. This means a hacker or a pervert could potentially gain access and monitor your child or play eerie music. This calls for home owners to be vigilant in securing their electronic devices.

Smart Homes

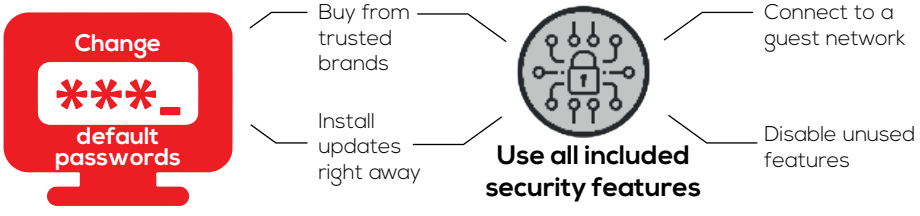
IoT is changing our traditional approach to how we live and interract with our homes. A number of houses, apartments and estates in Lagos have CCTV surveillance, Smart TVs, DVRs and connected thermostats that you can monitor and handle from any part of the world. These gadgets add convenience like locking your door or shutting off the lights all from a smartphone app, but they come with certain risks. In October, hackers took over 100,000 IoT devices and used them to block traffic to well-known websites, including Twitter and Netflix.

Home Routers

When buying a home router, no consideration is put on the security of these devices. Recent research has shown that your home routers can be used by malicious outsiders to launch attacks against websites belonging to other organisationss without your direct involvement.

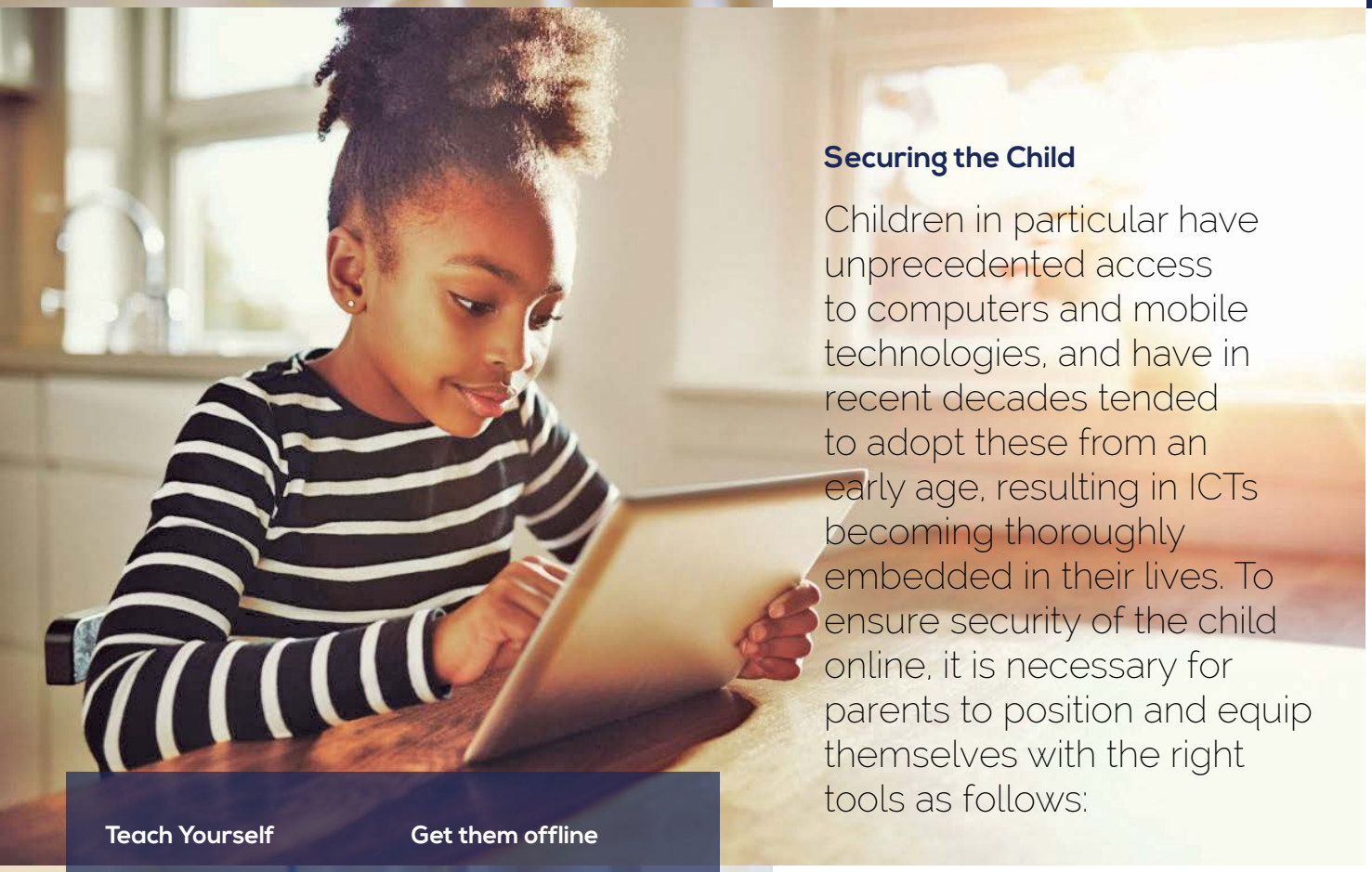
As a home owner, you run the risk of being blocked by certain sites, your internet speed may be slow due to the excessive bandwith utilization and you will incur higher costs.

Security Tips



Security Begins at Home

Home-owners and essentially anyone with property in Africa, locks their doors without thinking twice. African parents are well known for monitoring who their children are associating with, the language they use around other people and so on. But millions of users around Africa still don't have the same mentality about their digital presence.



Securing the Child

Children in particular have unprecedented access to computers and mobile technologies, and have in recent decades tended to adopt these from an early age, resulting in ICTs becoming thoroughly embedded in their lives. To ensure security of the child online, it is necessary for parents to position and equip themselves with the right tools as follows:

Teach Yourself

Educate yourself about the apps they're using in order to make informed decisions about what they're able to do on those apps.

Check Privacy Settings

Take advantage of built-in parental controls. Major apps and services – like Facebook or your DSTV box – have ways of restricting access for young people, so check through the settings thoroughly before letting your child onto a device.

Parents can also leverage technologies meant to secure kids online such Google's Kiddle, this presents a colorful space-themed page with a filtered search bar to ensure only kid friendly content is displayed.

Get them offline

It is key to remind children that there's a whole world offline too. This is important in a number of way, most important being to help dampen the impact of potential Cyberbullying. It is important to remind children to have fun in other ways off mobile phones.

Cyber Bullying

With the statistics and games such as blue whale piling up, it has become increasingly clear that the cruelties inflicted by Cyberbullying have become a devastating reality for many teens.This can cause damaging self-esteem issues, depression, self-harm, feelings of isolation that hinder performance in school, social skills, and general well-being.

Parents should educate themselved on detecting when their child is being bullied and ways of helping them through this.Here are some other examples of behavior that could cross the line into Cyberbullying:

- Sending or posting mean things to or about someone
- Creating a hostile environment in an online world or game

Parents can

- Talk about bullying with their kids and have other family members share their experiences.
- Remove the bait. If it is lunch money or gadgets that the school bully is after.
- Don't try to fight the battle yourself.

Abdul-Hakeem Ajijola

Chairman,

Consultancy Support Services Limited

In the year 2017, what were the key Cybersecurity consultancy services that clients were looking for?

- Vulnerability Assessments
- Forensics

Based on your experience, approximately how many times do organizations within the country carry out comprehensive Cybersecurity audits annually?

Zero.

Where would you rate the Cybersecurity maturity levels of the organizations you have conducted audits at?

Low.

In your opinion, were there more Cyber-attacks in the year 2017 as compared to previous years?

Yes, however, one needs to add that there is more awareness and thus more discussions about such matters.

Which categories of Cybersecurity were organizations most keen on?

- Vulnerability Assessment and Penetration Testing Services
- Cybersecurity Risk Audit Services
- Forensics and Investigations Services

Which sector releases the highest number of Cyber Security tenders within the country?

Financial Sector.

Anatomy of a Cyber Heist

INDICATORS OF COMPROMISE

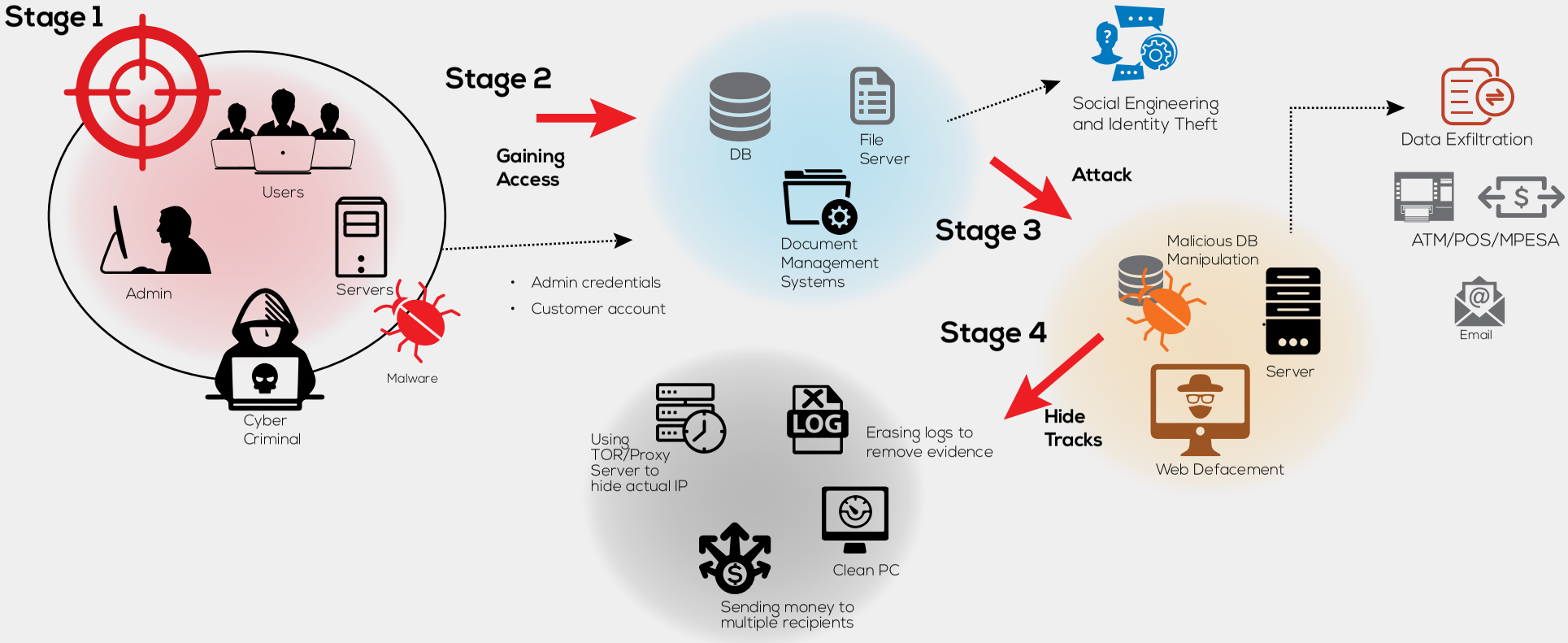
MULTIPLICITY	• Scanning from external IP	• Traffic to core VLAN from extenal IP	• Dormant account activity	• Logs deleted
VELOCITY	• Bruteforce attempts	• Multiple posting on DB	• Bulk transaction processing	• System unavailable
VOLUME	• Excessive DNS queries	• Remote Access tool detected	• Transaction over limit	• AV disabled
LIMITS	• IP conflicts	• Auditry disabled		

KEY SYSTEMS

Firewall · Antivirus · DNS · DHCP · Active Directory

ATTACK STAGES

RECONNAISSANCE → GAINING ACCESS → ATTACK → HIDE TRACKS



Leke Akinpelu

Manager, Cybersecurity Engineering,

FirstBank Nigeria

Kindly highlight some of the top cyber security issues of 2017 and how these issues impacted you personally, your organisation or country?

Lack of national regulations on Cybersecurity to curb the menace of cybercrime threats. Though, the federal government has enacted the cybercrime bill, this should go beyond just cybercrime bill. There is need for national cybersecurity framework which covers whole lots.

Poor Cybersecurity practice in various organizations especially the financial institutions has resulted in huge financial loss and reputational damage. Even though the regulator has made it compulsory for the financial institutions to adopt best practice such as ISO 27001, PCI, NIST, COBIT 5 in order for organization to maintain good cyber hygiene, yet the menace still persist. I believe security should be seen beyond compliance to regulatory requirements, it needs to be part of integral culture of the organization. Low security budget as a result of lack of top management support to security initiatives also prone organization to electronics fraud. Executive management support is a key success factor to maintaining good security posture.

Shortage of skilled resources in the country makes it difficult to get experienced cybersecurity professionals, this issues can be addressed if cybersecurity courses can be introduced into the tertiary institutions curriculum. Institutions can collaborate organization such as ISACA or technology company to ensure that students are exposed to the theories and practice of security.

Do you think fake news is a major problem in your country or Africa?

Yes.

If yes, who should be responsible for controlling the creation and distribution of fake news (government, end users, Telcos or ISPs or content owners)?

Government should champion this and in collaborations with Telcos and of course content owners.

Should regulators force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

Yes, the regulators need to force the social medias from disseminating fake news.

What can be done to improve the general user awareness on the detection of fake news in the country?

Aggressive campaign over the medias have a long way to go on the detection of fake news in the country.

Many governments in Africa are investing in e-services (e-government, e-voting, e-tax systems and many other portals.) Do you think the African citizenry is ready to consume and utilize these systems without the worry of privacy, security and fraud?

In my opinion, Africa citizenry is not ready to consume and utilize these systems without worry of privacy, security and fraud because currently there is no national regulations such as privacy law that guides the adoption of these technologies. Each African governments need to drive their privacy law or cyber security framework or better still the continents can come up with privacy standard like the European General Data Privacy Regulation (GDPR).

What are some of the risks we face with the introduction of government driven e-services and do you have any examples of these cases in your country?

There are lots of risks associated with the adoption of electronic payment in Nigeria, such as increase in electronic fraud, identity theft, social engineering with lots of reported cases of compromise personal sensitive data such as card holder information, unauthorize access to customers online and mobile banking application as a result of compromised login details.

In 2017, we had several cases of cyber security attacks including ransomware attacks across the world–were you impacted by these attacks?

If yes, how did you (company or country) respond to these cases? We were not really impacted even thoughYes, we are affected by my company but we are able to curb the menace of the threats based on the Advanced Malware Protection (AMP) and tools that help us to have the visibilities of what is happening on our network. We were able to identify, respond and contain the various threats.

Considering the shortage of skilled resources in Africa, how can we limit the impact of ransomware cases?

I believe awareness or education is very key for us to limit the impact of ransomware or other forms of malware in Africa. Cybersecurity degrees need to be included and funded in our tertiary institutions in order to bridge the resources gap in the continent.

Do you think organisations are spending enough money on combating cybercrime?

No.

What can be done to encourage more spending on cyber security issues?

Top level executive support is required to address the lack of funding issues as it relates to security.

Based on our research the Africa cyber security market will be worth USD2 billion dollars by 2020. Despite this opportunity, Africa has not produced a single commercially viable cyber security product or solution.

In your opinion, what should African countries or universities focus on to encourage innovation in the development of cyber security solutions?

African technology Companies need to partner with the universities to support and finance security related researches and also provide seed funding for individuals that are interested in the development of cyber security solutions. Strong collaborations between technology company and the universities have a long way to go in the African made cyber security solutions.

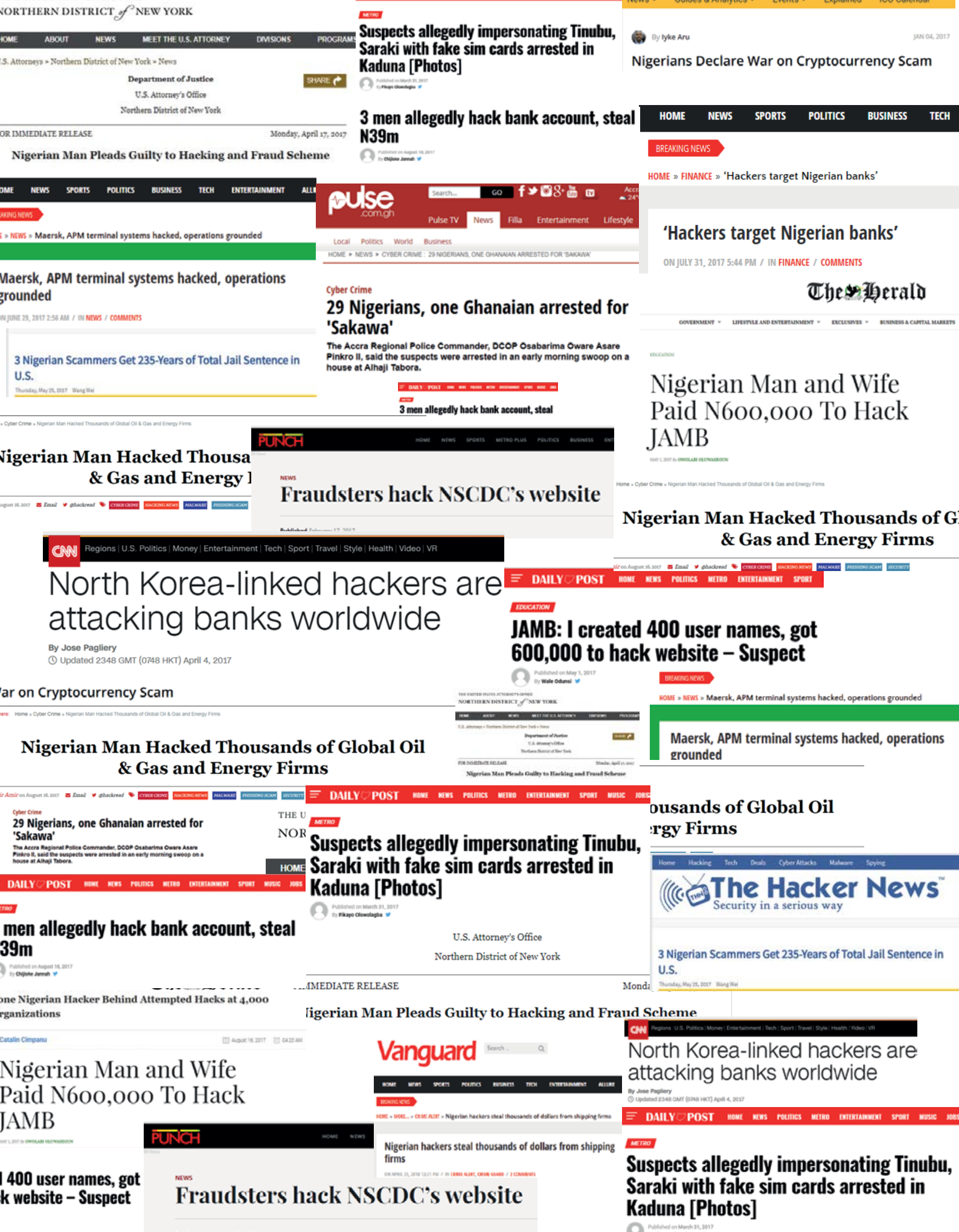
What role can the private sector and consumers of imported cyber security products play to ensure we can encourage local players to start developing African grown cyber security products or solutions or even services?

Just like I mentioned earlier, the private sector and consumers of imported security products should support local players that are interested in local cyber security products or services by making sure that they patronize them and also advise them if there is need for improvement in the products or service offerings. I believe strong collaboration between the consumers/importer of cyber security solutions and the local players have a long way to position Africa to be among the developers of security solutions.

In your opinion and from an African context, what are the top 2018 cyber security priorities for African countries and organizations?

The following should be the top priorities for 2018 cyber security for African countries;

- Encouragement of locally produced security solutions.
- Special Research Focus on Cyber security in our tertiary institutions in order to bridge the talent gaps.
- Continent wide information security awareness/education.


NORTHERN DISTRICT of NEW YORK
HOME ABOUT NEWS MEET THE U.S. ATTORNEY DIVISIONS PROGRAMS
U.S. Attorneys » Northern District of New York » News
Department of Justice
U.S. Attorney's Office
Northern District of New York
SHARE
FOR IMMEDIATE RELEASE
Monday, April 17, 2017
Nigerian Man Pleads Guilty to Hacking and Fraud Scheme
METRO
Suspects allegedly impersonating Tinubu, Saraki with fake sim cards arrested in Kaduna [Photos]
3 men allegedly hack bank account, steal N39m
By Iyke Aru
JAN 04, 2017
Nigerians Declare War on Cryptocurrency Scam
HOME NEWS SPORTS POLITICS BUSINESS TECH
BREAKING NEWS
HOME » FINANCE » 'Hackers target Nigerian banks'
HOME NEWS SPORTS POLITICS BUSINESS TECH ENTERTAINMENT
NEWS » Maersk, APM terminal systems hacked, operations grounded
Maersk, APM terminal systems hacked, operations grounded
3 Nigerian Scammers Get 235-Years of Total Jail Sentence in U.S.
pulse.com.gh
Search... GO
Pulse TV News Filla Entertainment Lifestyle
Local Politics World Business
HOME » NEWS » CYBER CRIME : 29 NIGERIANS, ONE GHANAIAN ARRESTED FOR 'SAKAWA'
Cyber Crime
29 Nigerians, one Ghanaian arrested for 'Sakawa'
The Accra Regional Police Commander, DCOP Osabarima Oware Asare Pinkro II, said the suspects were arrested in an early morning swoop on a house at Alhaji Tabora.
'Hackers target Nigerian banks'
ON JULY 31, 2017 5:44 PM / IN FINANCE / COMMENTS
The Herald
GOVERNMENT LIFESTYLE AND ENTERTAINMENT EXCLUSIVES BUSINESS & CAPITAL MARKETS
EDUCATION
Nigerian Man and Wife Paid N600,000 To Hack JAMB
Cyber Crime » Nigerian Man Hacked Thousands of Global Oil & Gas and Energy Firms
Nigerian Man Hacked Thousands of Global Oil & Gas and Energy Firms
PUNCH
NEWS
Fraudsters hack NSCDC's website
CNN
Regions | U.S. Politics | Money | Entertainment | Tech | Sport | Travel | Style | Health | Video | VR
North Korea-linked hackers are attacking banks worldwide
By Jose Pagliery
Updated 2348 GMT (0748 HKT) April 4, 2017
DAILY POST
HOME NEWS POLITICS METRO ENTERTAINMENT SPORT
EDUCATION
JAMB: I created 400 user names, got 600,000 to hack website – Suspect
Published on May 1, 2017
By Wale Odunsi
BREAKING NEWS
HOME » NEWS » Maersk, APM terminal systems hacked, operations grounded
Maersk, APM terminal systems hacked, operations grounded
Nigerian Man Pleads Guilty to Hacking and Fraud Scheme
Nigerian Man Hacked Thousands of Global Oil & Gas and Energy Firms
Cyber Crime
29 Nigerians, one Ghanaian arrested for 'Sakawa'
The Accra Regional Police Commander, DCOP Osabarima Oware Asare Pinkro II, said the suspects were arrested in an early morning swoop on a house at Alhaji Tabora.
DAILY POST
HOME NEWS POLITICS METRO ENTERTAINMENT SPORT MUSIC JOBS
METRO
Suspects allegedly impersonating Tinubu, Saraki with fake sim cards arrested in Kaduna [Photos]
Published on March 31, 2017
By Fikayo Olowolagba
U.S. Attorney's Office
Northern District of New York
The Hacker News
Security in a serious way
3 Nigerian Scammers Get 235-Years of Total Jail Sentence in U.S.
Nigerian Man Pleads Guilty to Hacking and Fraud Scheme
Vanguard
Nigerian hackers steal thousands of dollars from shipping firms
Nigerian Man and Wife Paid N600,000 To Hack JAMB
PUNCH
NEWS
Fraudsters hack NSCDC's website
CNN
North Korea-linked hackers are attacking banks worldwide
By Jose Pagliery
Updated 2348 GMT (0748 HKT) April 4, 2017
DAILY POST
HOME NEWS POLITICS METRO ENTERTAINMENT SPORT MUSIC
METRO
Suspects allegedly impersonating Tinubu, Saraki with fake sim cards arrested in Kaduna [Photos]

Oluseyi Akindeinde

Chief Technology Officer,

Digital Encode

What is fake news?

It is fabricated news and deliberate misinformation spread via traditional news and broadcast media as well as on social media platforms.

How did fake news become such a big problem?

It was brought to the fore in 2016 during the US presidential election especially by the anti-Clinton and anti-Trump online media organizations.

What will ultimately get brands to fight fake news?

Taking legal action against anyone or media house spreading fake news.

Should regulators force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms?

Absolutely.

What happens when fake news spreads? What actions can people take to verify news stories, photographs and other sources of online information?

Vigilance is key as well as referencing more than one source.

We do everything online – book doctors' appointments, manage our bank accounts and find dates – Do you think we are ready to vote from our PCs or smartphones? Explain.

Not yet. There are still a lot of people that are technology averse and illeterate.

What is the highest risk that we face by moving to electronic voting?

Apathy. People may not really embrace it.

What are some of the pros?

It has a wider reach.

Why is Ransomware so effective?

It encrypts the entire computing device and you lose access to your data.

What is the possible impact of Ransomware?

Loss of critical data.

Have you or know someone you know been affected by Ransomware?

Yes. A number of people.

How often do you transact using your mobile phone?

Have you ever been a victim of online or mobile scam?

No.

Why does the cyber skills shortage need immediate attention?

Because cyber hacking is on the increase.

How many unfilled security jobs are estimated to exist today?

A fairly high number.

How does collaboration help enrich the students' learning?

Cross fertilization of ideas.

In the year 2017, what were the key Cybersecurity consultancy services that clients were looking for?

- Vulnerability Assessments
- Forensics
- Audit Services
- Risk Management Programs
- Managed Security Services

Based on your experience, approximately how many times do organizations within the country carry out comprehensive Cybersecurity audits annually?

Once every quarter or 4 times a year.

Where would you rate the Cybersecurity maturity levels of the organizations you have conducted audits at?

High.

In your opinion were there more Cyberattacks in the year 2017 as compared to previous years?

Yes there were more and increasing.

Which categories of Cybersecurity were organizations most keen on?

- Vulnerability Assessment and Penetration Testing Services
- Cybersecurity Risk Audit Services
- Forensics and Investigations Services
- Managed Security Services

Which sector releases the highest number of Cyber Security tenders within the country?

Financial Sector.

In the year 2017, what were the key Cybersecurity products that clients purchased?

Vulnerability Management Systems or Authentication Solutions or Network access and monitoring solutions.

Based on your opinion, which products have higher market appetite?

SIEM.

Africa Cyber Security Framework

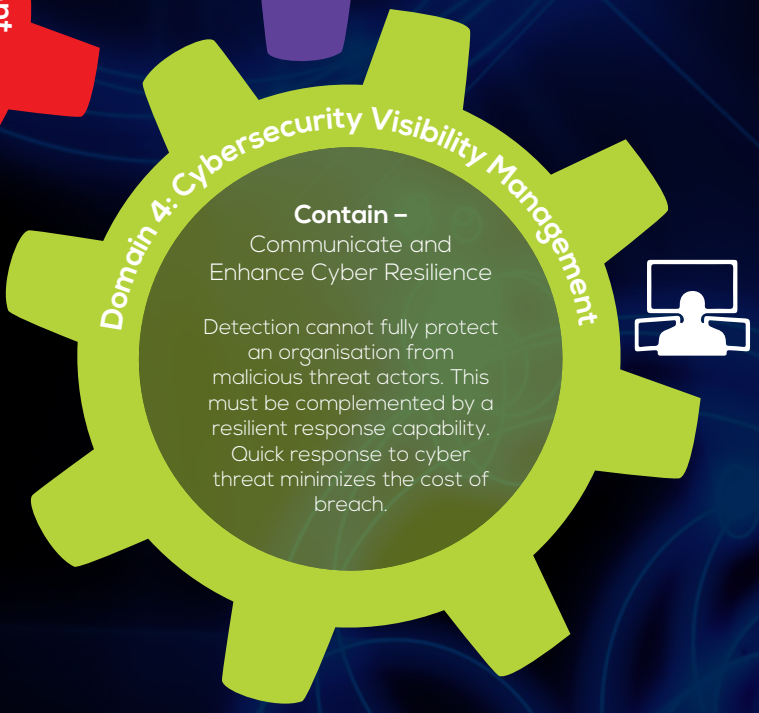
Cybercrime in the African continent particularly within the Small Medium Enterprises (SMEs) setting is a growing concern. SMEs are especially expanding the use of cloud, mobile devices, smart technologies and work force mobility techniques. This reliance has however unlocked the doors to vulnerabilities and Cybercrime. Attackers are now launching increasingly sophisticated attacks on everything from business critical infrastructure to everyday devices such as mobile phones. Malware threats, Insider threats, data breaches resulting from poor access controls and system misconfigurations are some of the ways that attackers are now using to deploy coordinated attacks against these organisations.

With the increasing business requirements of the 21st century businesses and the inadequate budget allocated to IT, it has become expensive especially for small and medium sized companies to adopt complex and international Cyber security frameworks. As such, Cybercrime prevention is often neglected within SMEs. This has resulted in a situation whereby SMEs are now one of the popular targets of Cyber criminals. While at the same time, the SMEs lack a comprehensive framework that will help them determine their risk exposure and provide visibility to their security landscape without necessarily adding to the strained costs.

Solution

In order to assist businesses in Africa particularly SMEs, we developed the Serianu Cyber Security Framework. The Framework serves to help businesses in Africa particularly SMEs to identify and prioritize specific risks and steps that can be taken to address them in a cost effective manner. The baseline controls developed within the framework, when implemented, will help to significantly reduce Cyber related security incidences, enable IT security to proactively monitor activities on their key ICT infrastructure and provide assurance that business operations will resume in the appropriate time in case of an attack or disruption.

Domains of the Africa Cyber Security Framework



Appendix

List of Remote Access Tools for Database

Product	License	Windows	Mac OS X	Linux	Oracle	MySQL	PostgreSQL	MS SQL Server	ODBC	JDBC	SQLite
Adminer	Apache License or GPL	Yes	Yes	Yes	Yes	Yes	Yes	Yes			Yes
Advanced Query Tool (AQT)	Proprietary	Yes	No	No	Yes	Yes	Yes	Yes	Yes		
DaDaBIK	Proprietary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Database Deployment Manager	LGPL	Yes	No	Yes		Yes					
DatabaseSpy	Proprietary	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	
Database Tour Pro[4]	Proprietary	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes
Database Workbench	Proprietary	Yes			Yes	Yes		Yes	Yes		
DataGrip	Proprietary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
DBeaver	Apache License	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DBEdit	GPL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Epictetus	Proprietary	Yes	Yes	Yes	Yes		Yes	Yes			
HeidiSQL	GPL	Yes				Yes	Yes	Yes			
Jailer Relational Data Browser[5]	Apache License	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maatkit	GPL	Yes	Yes	Yes		Yes					
Microsoft SQL Server Management Studio	Proprietary	Yes	No	No				Yes			
ModelRight	Proprietary	Yes	No	No	Yes	Yes		Yes	Yes		
MySQL Workbench	Community Ed: GPL Standard Ed: Commercial Proprietary	Yes	Yes	Yes		Yes					
Navicat	Proprietary	Yes	Yes		Yes	Yes	Yes	Yes	Yes		Yes
Navicat Data Modeler	Proprietary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes
Oracle Enterprise Manager	Proprietary	Yes	No	Yes	Yes	Yes		Yes			
Oracle SQL Developer	Proprietary	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	
Orbada	GPL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
pgAdmin III	PostgreSQL License	Yes	Yes	Yes							
pgAdmin4	PostgreSQL License						Yes				
phpLiteAdmin	GPL	Yes	Yes	Yes	No	No	No	No	No	No	Yes
phpMyAdmin	GPL	Yes	Yes	Yes		Yes					
SQL Database Studio	Proprietary	Yes	No	No	No	No	No	Yes			
SQLyog	GPLv2	Yes				Yes					
SQuirreL SQL	GPLv2 & LGPLv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TablePlus	Proprietary	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes
Toad	Proprietary	Yes	No	No	Yes	Yes		Yes	Yes		
Toad Data Modeler	Proprietary	Yes	No	No	Yes	Yes	Yes	Yes			
TOra	GPL	Yes	Yes	Yes	Yes	Yes	Yes				

Remote Access tools for Endpoints

Software	Protocols	License	Free for personal use	Free for commercial use
AetherPal	Proprietary	Proprietary	No	No
Ammyy Admin	Proprietary	Proprietary	Yes	No
AnyDesk	Proprietary	Proprietary	Yes	No
Anyplace Control	Proprietary	Proprietary	No	No
AnywhereTS	RDP, ICA	Proprietary	Yes	Yes
Apple Remote Desktop	RFB (VNC)	Proprietary	No	No
Apple Screen Sharing (iChat)	Proprietary, RFB (VNC)	Proprietary	Yes	Yes
AppliDis	RDP	Proprietary	No	No
BeAnywhere Support Express	Proprietary	Proprietary	No	No
Bomgar	Proprietary	Proprietary	No	No
Cendio ThinLinc	RFB (VNC)	Proprietary	Yes[a]	Yes[a]
Chicken of the VNC	RFB (VNC)	GPL	Yes	Yes
Chrome Remote Desktop	Chromoting	BSD Client, Proprietary Server	Yes	Yes
CloudBerry Lab (CloudBerry Remote Assistant)	Proprietary	Proprietary	Yes	Yes
Citrix XenApp/Presentation Server/MetaFrame/ WinFrame	RDP, ICA	Proprietary	No	No
Fog Creek Copilot	RFB (VNC)	Proprietary	No	No
GO-Global	Proprietary	Proprietary	No	No
GoToMyPC	Proprietary	Proprietary	No	No
HP Remote Graphics Software (RGS)	HP RGS	Proprietary	Yes[b]	Yes[b]
HOB HOBLink JWT	RDP	Proprietary	No	No
HOB HOB MacGate	RDP	Proprietary	No	No
IBM Director Remote Control	Proprietary	Proprietary	No	No
I'm InTouch	Proprietary	Proprietary	No	No
iTALC	RFB (VNC)	GPL	Yes	Yes
KDE	RFB (VNC), RDP	GPL	Yes	Yes
LiteManager	Proprietary	Proprietary	Yes[d]	Yes[d]
LogMeIn	Proprietary	Proprietary	No	No
Mikogo	Proprietary	Proprietary	Yes	No
Netop Remote Control	Proprietary	Proprietary	No	No
NetSupport Manager	Proprietary	Proprietary	No	No
Netviewer	Proprietary	Proprietary	No	No
NoMachine	NX	Proprietary	Yes	Yes[e]
OpenText Exceed onDemand	Proprietary	Proprietary	No	No
Open Virtual Desktop	RDP	GPL Client, Proprietary Server	No	No

Software	Protocols	License	Free for personal use	Free for commercial use
Oracle Secure Global Desktop Software/Sun VDI	AIP	Proprietary	No	No
Proxy Networks	Proprietary	Proprietary	No	No
Pilixo Remote Access	Proprietary	Proprietary	No	No
QVD	NX and HTTP	GPL	Yes	Yes
rdesktop	RDP	GPL	Yes	Yes
RealVNC Open	RFB (VNC)	GPL	Yes	Yes
RealVNC	RFB (VNC)	Proprietary	Yes[e]	No
Remmina	RDP, RFB (VNC), SPICE, XDMCP, SSH	GPL	Yes	Yes
Remote Desktop Services/Terminal Services	RDP	Proprietary	Yes	Yes[g]
ScreenConnect	Proprietary	Proprietary	No	No
Splashtop Remote	Proprietary	Proprietary	Yes	No
SSH with X forwarding	X11	BSD	Yes	Yes
Sun Ray/SRSS	ALP	Proprietary	?	?
Symantec pcAnywhere	Proprietary	Proprietary	No	No
TeamViewer	Proprietary	Proprietary	Yes	No
Techinline	RDP	Proprietary	No	No
Teradici	PCoIP	Proprietary	No	No
Thinc	Thinc	GPL	Yes	Yes
TigerVNC	RFB (VNC)	GPL	Yes	Yes
TightVNC	RFB (VNC)	GPL	Yes	Yes
Timbuktu	Proprietary	Proprietary	?	?
TurboVNC	RFB (VNC)	GPL	Yes	Yes
Ulterius	RFB (VNC)	GPL	Yes	Yes
UltraVNC	RFB (VNC)	GPL	Yes	Yes
Vinagre	RFB (VNC), SPICE, RDP, SSH	GPL	Yes	Yes
XDMCP	X11	MIT	Yes	Yes
xpra	Bencode-based, rencode-based, YAML-based, RFB (VNC) for desktop mode	GPL	Yes	Yes
X11vnc	RFB (VNC)	GPL	Yes	Yes
X2Go	NX	GPL	Yes	Yes
x2vnc	RFB (VNC)	BSD	Yes	Yes
x2vnc	Ulterius (VNC)	BSD	Yes	Yes
x2x	X11	BSD	Yes	Yes
Software	Protocol	License	Free for personal use	Free for commercial use

List of Open Source Tools

Vulnerability Scanners

1. OpenVAS

OpenVAS isn't the easiest and quickest scanner to install and use, but it is one of the most feature-rich, broad IT security scanners that you can find for free. It scans for thousands of vulnerabilities, supports concurrent scan tasks, and scheduled scans. It also offers note and false positive management of the scan results. However, it does require Linux at least for the main component.

2. Retina CS Community

Retina CS Community provides vulnerability scanning and patching for Microsoft and common third-party applications, such as Adobe and Firefox, for up to 256 IPs free.

3. Microsoft Baseline Security Analyzer (MBSA)

Microsoft Baseline Security Analyzer (MBSA) can perform local or remote scans on Windows desktops and servers, identifying any missing service packs, security patches, and common security misconfigurations.

4. Nexpose Community Edition

Nexpose Community Edition can scan networks, operating systems, web applications, databases, and virtual environments. The Community Edition, however, limits you to scanning up to 32 IPs at a time.

5. SecureCheq

SecureCheq can perform local scans on Windows desktops and servers, identifying various insecure advanced Windows settings like defined by CIS, ISO or COBIT standards.

6. Qualys FreeScan

Qualys FreeScan provides up to 10 free scans of URLs or IPs of Internet facing or local servers or machines.

References

https://www.businessdayonline.com/remitas-disruptive-mobile-app-throws-banks-off-balance/

https://www.thisdaylive.com/index.php/2017/04/07/north-korea-hacking-nigerian-banks-financial-institutions-of-17-other-countries/

http://allafrica.com/stories/201707210062.html

http://thenationonlineng.net/fraud-challenge-e-payment-cbn/

http://thenationonlineng.net/cyber-security-experts-urge-intelligence-sharing-among-banks/

http://leadership.ng/2017/07/23/nigerias-atm-galleries-failure/

http://allafrica.com/stories/201708070092.html

https://www2.deloitte.com/ng/en/pages/risk/articles/2016-nigeria-cybersecurity-outlook.html

Top Issues

http://punchng.com/fraudsters-hack-nscdcs-website/

http://www.herald.ng/nigerian-man-wife-pay-n600000-hack-jamb/

https://www.vanguardngr.com/2017/06/maersk-apm-terminal-systems-hacked-operations-grounded/

https://www.hackread.com/nigeria-man-hacked-global-oil-gas-and-energy-firms/

https://www.bleepingcomputer.com/news/security/lone-nigerian-hacker-behind-attempted-hacks-at-4-000-organizations/

https://www.vanguardngr.com/2018/04/nigerian-hackers-steal-thousands-dollars-shipping-firms/

https://thehackernews.com/2017/05/nigerian-scams.html

Identity Theft

http://dailypost.ng/2017/03/31/suspects-allegedly-impersonating-tinubu-saraki-fake-sim-cards-arrested-kaduna-photos/

Ponzi Schemes

https://www.oasdom.com/7-current-ponzi-schemes-nigeria-2017/

https://cointelegraph.com/news/nigerians-declare-war-on-cryptocurrency-scam

Ransomware

https://www.schneier.com/blog/archives/2017/05/the_future_of_r.html

Privileged User Management

http://lp.cyberark.com/rs/316-CZP-275/images/BR-CyberArk-PAS-1910-2016-final-en.pdf

SERIANU

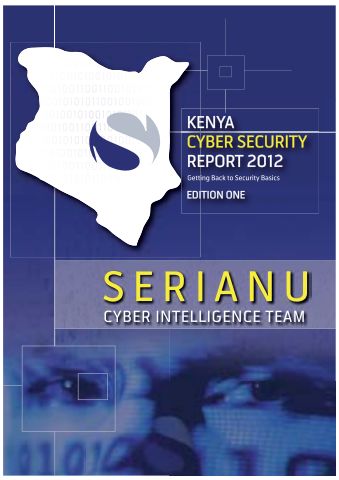
Cyber Immersion

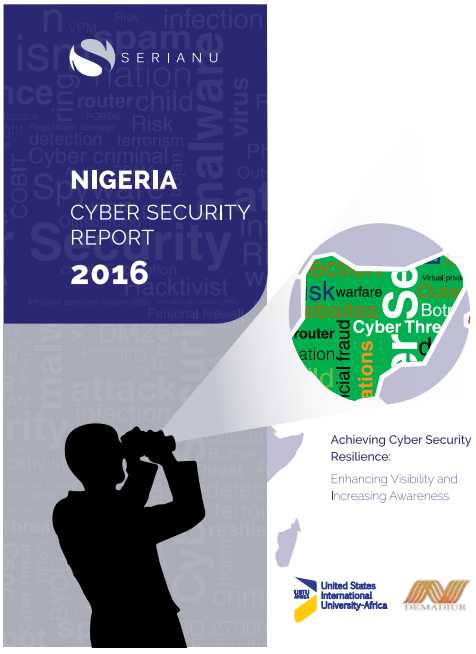
Hands on Cyber Security Training for Professionals

Africa Cyber Immersion Centre
acic
Engage | Educate | Empower

Cyber Immersion is Serianu's premier training program that aims to arm private and public organisations with the necessary know-how to counter cyber threats in a holistic manner, helping them mitigate the risks and costs associated with cyber disruptions.

info@serianu.com | www.serianu.com





SERIANU
United States International University-Africa
ISACA
Trust in, and value from, information systems
Lagos Chapter
DEMADIUR