



S E R I A N U

**NIGERIA**

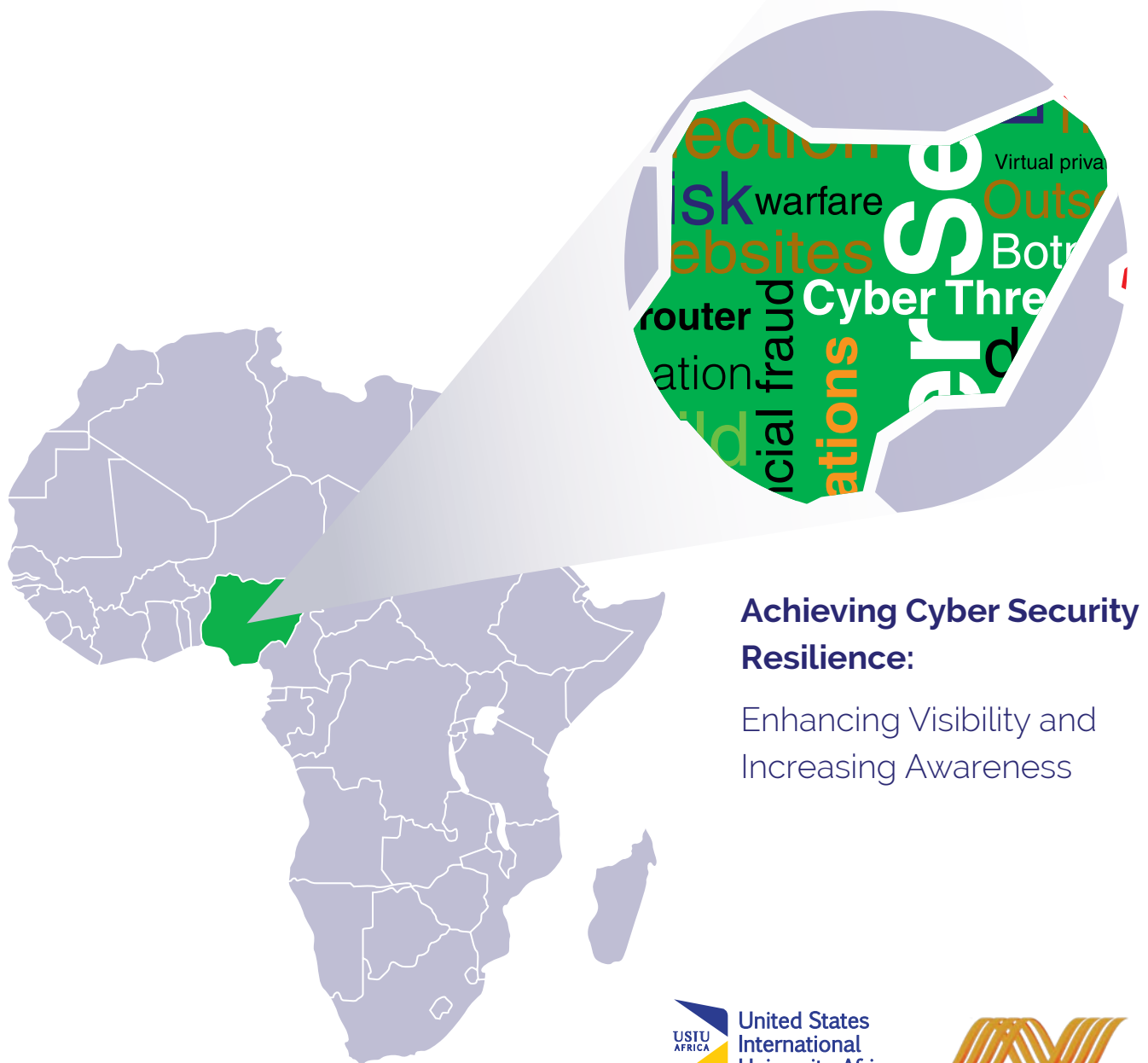
CYBER SECURITY  
REPORT

**2016**





S E R I A N U



## Achieving Cyber Security Resilience:

## Enhancing Visibility and Increasing Awareness

# STAY SAFE, SECURE AND COMPLIANT WITH OUR COMPREHENSIVE, INTEGRATED & INTELLIGENT CYBER SECURITY MANAGEMENT SERVICE

- Over a Decade of Experience in Cyber Security
- Actively servicing more than 700 satisfied clients
- Global presence and delivery capabilities in US, Europe, India, Middle East, Africa and South East Asia with network of Global Security Operations Centers
- Proven delivery models based on Artificial Intelligence and Analytics Platform coupled with highly skilled and certified resource pool of 1000+ Cyber Security Experts.
- Recognized and awarded by Gartner, Asian Banker, and Red Herring amongst others



# Contents

Achieving Cyber Security Resilience

06	About the Report
07	Acknowledgement
08	Foreword
09	Executive Summary
14	Nigeria Cyber Intelligence Report
21	2016 Nigeria Cyber Security Survey
36	Top Security Issues in 2016
40	Risk Ranking by Sector
44	Top ICT Trends Affecting Cyber Security
51	The Serianu Cybersecurity Framework
56	References

## About the Report

The Nigeria Cyber Security Report 2016 was researched, analysed, compiled and published by the Serianu Cyber Threat Intelligence Team in partnership with Demadiur Systems Limited and the USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology.

## Data Collection and Analysis

The data used to develop this report was obtained from various sources including; surveys and interviews with different stakeholders; several sensors deployed in Nigeria and review of previous research reports.

The sensors are non-intrusive network monitoring devices that perform the function of monitoring an organisation's network for malware and cyber threat activities such as brute-force attacks against the organisation's servers. In an effort to enrich the data we are collecting, we have partnered with The Honeynet Project™ and other global cyber intelligence partners to receive regular feeds

on malicious activity within the country. Through such collaborative efforts we are able to anticipate, detect and identify new and emerging threats using our intelligent analysis-engine. The analysis-engine assists in identifying new patterns and trends in cyber threat sphere that are unique to Nigeria.

Partnerships through the Serianu CyberThreat Command Centre (SC3) Initiative are warmly welcomed in an effort to improve the state of cyber security in Nigeria and across Africa. This initiative is geared towards collaborative cyber security projects in academia, industrial, commercial and governmental organisations. .

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](mailto:info@serianu.com)**

## Acknowledgement

### Authors

#### Demadiur Systems Limited & Serianu Ltd

**Chike Nzeh**

**Alphonso Kehinde**

**Brencil Kaimba**

**Kevin Kimani**

**Martin Mwangi**

**Barbara Munyendo**

**Faith Mueni**

**Daniel Ndegwa**

**Stephen Wanjuki**

**Nabihah Rishad**

**Samuel Keige**

**Jeff Karanja**

**Hilary Soita**

#### USIU Africa

**Paula Musuva-Kigen**

**Secauose Onyibe**

**Polly Mugure**

**Kenneth Mbae**

**Newton Karumba**

**Andrew Ngari**

**Edward Owino**

#### Others

**Martin Ekpeke** - Editor, IT Pulse Magazine

**Akin Naphtal** - Director, Instinctwave

**Mike Anigbogu** - Cyber Security Expert

**Francis Okoh** - Director, Telecom Allianz

### Contributors

#### Dr. Nwonyi Polycarp Emeka

Manager Intelligence, Police Special Fraud Unit (PSFU)  
Force Criminal Investigation & Intelligence Department  
Lagos

#### Olusola Teniola

President Association of Telecommunications Companies  
of Nigeria (ATCON)

#### Onajite Regha

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

#### Abdul-Hakeem Ajijola

Chair, Consultancy Support Services Ltd., Abuja, Nigeria. A  
Cybersecurity & Cybercrime Advisor and Consultant

#### Dr. Joshua Atta

Project Manager, Nigerian Research and Education  
Network (NgREN)

#### Muhammed Rudman

CEO of Nigerian Internet Exchange

#### Remi Afon

President Cyber Security Experts Association of Nigeria  
(CSEAN)

#### Dr. Krishnan Ranganath

Vice President - Century Group

#### Collins Onuegbu

Executive Vice Chairman of Signal Alliance and Founder of  
Sasware Nigeria

#### Bolanle Omotosho

CEO of Digital Assure Ltd. He is also Cybersecurity and  
Cybercrime specialist and consultant to many banks in  
Nigeria

Report Research and Analysis was conducted by the Serianu team in partnership with the USIU's Centre of Informatics Research and Innovation.

Design, layout and production: Tonn Kriation

Copyright © Serianu Limited, 2016

All rights reserved

#### For more information contact:

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

**Tel:** +234 803 347 1283

**Email:** [contact@demadiur.com](mailto:contact@demadiur.com) | **Website:** [www.serianu.com](http://www.serianu.com)



## Foreword

Technology adoption is driving business innovation and growth in Nigeria, at the same time it is exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers and fraudster are increasingly motivated to target our ICT infrastructure due to the increasing value of information held within it and the perceived lower risk of detection and capture in conducting cybercrime as compared to more traditional crime.

Recently, I received a phishing email from one of the leading banks in Nigeria. The email was addressed to me but it was sent from an American university's domain (kwm4ef@virginia.edu). This incident highlights one of the many schemes and typical modus operandi of cybercrime perpetrators. They thrive on the ignorance, fear, and sometimes greed of their victims.

The increase in cybercrime in Nigeria can be attributed to the rising poverty levels, greed (on both the perpetrators and sometimes even the victims), easy access to gullible targets by the criminals and lack of adequate legal and regulatory policies to prevent and prosecute the perpetrators when identified.

While the corporate world has a lot of tools available to it to combat this issue, individuals are still the most vulnerable. Basic education on some of the approaches an individual can take to identify potential harmful materials is the starting point to combat this. We are taught that when crossing the street, we should check for oncoming cars by looking left, then right, then left again. Some have wondered why the additional requirement to look left a second time.



**Ikechukwu Nnamani**

President Demadiur Systems Limited; Board member Nigerian Internet Registration Agency (NIRA); Board member Association of Telecommunications Companies of Nigeria (ATCON)

But this highlights the level of seriousness that is placed on safety. The philosophy behind this basic rule of the road that has saved tons of lives, appears to be left behind when we enter the world of information technology as people with access to information technology gadgets have failed to simply pay close attention to what is received electronically before taking actions on them. In the process many have fallen victim to cybercrimes that would otherwise have been prevented.

Our research findings show that most Nigerian organisations are still ill-equipped and unprepared to respond to information security threats.

This level of vulnerability presents great business opportunities for Nigerian entrepreneurs, researchers and vendors. For us to stay ahead of the threat curve, we need to continually invest in research, build local cyber threat management infrastructure and enhance their ability to anticipate, detect, respond and contain information security threats.

We need to step up; work together to build and provide information security services that enables Nigeria to address these challenges. We need to leverage our local presence and understanding of the environment to provide a clear indication of the security problems on the ground. This local presence combined with partnerships with regional and global players will provide globally tested solutions and approaches to address identified security problems.



William Makatiani

CEO, Serianu Ltd

## Executive Summary

Technology has changed the business landscape dramatically. Technology use is now a key part of doing business and affects all aspects of the corporate process, ranging from strategic options to creation of new opportunities for innovation in products and services.

In Africa, internet usage has been rapidly rising as more people connect to the inter-web mostly through their mobile phones. This increased use has created a new challenge for the continent in potential attack vectors at both individual and organizational level.












The Nigeria Cyber Security Report is part of the Africa Cyber Security Report 2016.

In this report we sought to understand the top threats, risks and levels of awareness currently in Africa. We took a regional approach and analysed countries from both East and West Africa (Kenya, Tanzania, Nigeria, Ghana and Uganda) that would provide an accurate image of the continent.

Our choice of a sample-based survey was based on the realization that a wider census-based research would be costly. A snapshot of the economic and internet demographics of these five countries (as indicated on the graphics) strengthened our resolve to focus on them for this particular survey.



Breakdown of key statistics for In-Scope countries:

	 <b>Population (2016 Est.)</b>	 <b>GDP (2016)</b>	 <b>Internet users &amp; subscribers (2016)</b>	 <b>Estimated Cost of cyber- crime (2016)</b>	 <b>Estimated No. of Certified Professionals</b>
 Africa	1,185,529,578	\$2.89T	340,783,342	\$2B	6892
 Nigeria	186,879,760	\$481.066B	97,210,000	\$550M	1500
 Kenya	46,790,758	\$63.398B	37,716,579	\$175M	1400
 Tanzania	52,482,726	\$44.895B	17,263,523	\$85M	250
 Ghana	26,908,262	\$37.86 B	19,125,469	\$50M	460
 Uganda	38,319,241	\$26.369B	14,564,660	\$35M	300

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

In this report, we look at the current state of Nigeria's cyber security landscape. We have broken down, analysed and summarized the top threats, risks and levels of awareness in Nigeria.



## Highlights of the Report

- ◆ **The estimated cost of cyber-crime in Nigeria has soared to \$550 million.** This cost continues to grow as many organisations automate their processes. This is particularly so for the Ecommerce and financial services sector where the introduction of e-services has introduced new weaknesses that have allowed loss of money through these channels.
- ◆ **E-Commerce Platforms hit with more Online Scams, ATM Skimming and Identity Theft** as increased Electronic Payment Integrations with these platforms and Financial Institutions. At the same time **electronic banking and cashless initiative have been introduced into the country.** This has resulted in some unintended consequences from online scams, ATM Skimming and identity theft.
- ◆ **Technical Training of employees is insufficient. The increase in the number of home grown cyber criminals in Nigeria** is not because they are more talented, it's because they are more creative, patient, single minded and they explore limitless pathways. Nigerian organizations are not leveraging their own creative, curious analysts. **Our technical teams are not empowered with tools and education to enable them explore the why?**
- ◆ **Low Security budget in Most organisations led to Low Security Awareness.** This has been proven by the numerous breaches we have seen in the period under review alone attributed to compromised employees.
- ◆ **Nigerian cyber-attackers are targeting other countries** by defrauding unsuspecting users, hacking accounts and email addresses and in other cases sending phishing emails to bank customers requesting for passwords, PINs or other bank account security details.
- ◆ **Customised malware targeting critical mobile and Internet banking infrastructure.** The results from our Internal Traffic Analysis revealed that there are numerous forms of Malware on systems, these include; Trojans such Dridex and Zeus malware. Attackers are using these malwares to compromise and access an account. Unfortunately, statistics still remain vague as organisations are reluctant to reveal the extent to which they have been targeted by it.

### ...at a glance



- ◆ E-Commerce Platforms hit with more Online Scams, ATM Skimming and Identity Theft
- ◆ Technical training of employees is insufficient.
- ◆ Low security awareness.
- ◆ Malware targeting critical mobile and internet banking infrastructure are on the rise.
- ◆ Insider threat is still the largest contributor of direct losses in cybercrime
- ◆ Lack of practical regulatory guidance from industry regulators and government
- ◆ **Insider threat is still the largest contributor of direct losses in cybercrime in Nigeria.** Insider threats refer to fraud involving information or employee abuse of IT systems and information.
- ◆ Most organisations in **Nigeria are ill prepared to deal with information security threats** (Anticipate, Detect, Respond and Contain). This can be attributed to: Lack of sufficient budgets, Lack of skilled professionals, and Lack of visibility within the organisation.

- ◆ **Increase in IoT threats** - Due to their insecure implementation and configuration, these Internet-connected embedded devices, including CCTVs and nanny cams, Smart TVs, DVRs, Smart routers and printers, are routinely being hacked and used as weapons in cyber-attacks.
- ◆ Security professionals are **struggling to demonstrate business value to senior management** because they are providing very technical operational metrics whereas business managers are looking for more business-oriented metrics.
- ◆ **Lack of practical regulatory guidance from industry regulators and government** leads to poorly implemented and unenforceable security controls since they are not locally focused and are instead copied and pasted regulations..



## Way Forward

Based on our research findings, most Nigerian organisations are ill-equipped to respond to information security threats. Although there are different initiatives (regulators, government and private organisations) in place set out to address information security issues in Nigeria, these initiatives cannot adequately address the current information security issues. Public and private organisations need to rethink their whole approach to information security and establish security practices needed to protect critical IT infrastructure. They also need to train and grow security experts needed to secure this infrastructure. Most organisations now recognize that it is imperative that local organisations take action before the situation worsens and the cost of inaction becomes even greater.



# Top 5 priorities for 2017

The challenges faced by Nigeria and in essence African countries, present great business opportunities for entrepreneurs, researchers and vendors. In order for us to stay ahead of the threat curve, we need to continually invest in research, build local cyber threat management infrastructure and enhance our ability to anticipate, detect, respond and contain information security threats. In our current state, we are unable to build these capabilities.

Nigerian entrepreneurs need to step up, work together to build and provide information security services that address these challenges. Nigerian entrepreneurs and researchers should leverage their local presence and understanding of the environment to provide a clear indication of the security problems on the ground. This local presence combined with partnerships with global players will provide globally tested solutions and approaches to address identified security problems.

## Awareness and Training

It is evident that attackers are now performing more targeted attacks against specific members in organizations. It is crucial that organizations develop and implement security awareness training programs. This can be done in-house or outsourced to qualified service providers. Regardless of the mode of training, an organization should ensure a needs assessment is conducted before adopting any form of employee training program. Generally, top issues that should be addressed by the program include: Social Engineering averting, detection of phishing scams, Email hygiene, internet usage best practices and password hygiene.

## Continuous Monitoring and Log Analysis

There is need for continuous monitoring. Best practice mandates that organizations should conduct continuous monitoring on all critical systems. Standards such as NIST identify a three-tiered impact system—low, moderate and high impact—to use when developing monitoring policies. Continuous monitoring does not imply true, real-time 24 x 7, nonstop monitoring and reporting. Instead, it means implementing monitoring and oversight processes that provide a clear picture of security state at a given time while also providing a mirror of control effectiveness over time.



## Vulnerability and Patch Management

With the numerous attacks occurring as a result of missing patches and susceptibility to malware, it's critical for local organizations to focus on developing vulnerability and patch management programs within their institutions. This will involve running periodic and automated vulnerability scanners on the network which can identify vulnerabilities such as buffer overflow, open ports, SQL injections, obsolete systems and missing patches. Use of antivirus software is also crucial for detecting and removing malware. All in all, the most important part is correcting the identified vulnerabilities which will involve the installation of a patch, a change in network security policy, reconfiguration of software (such as a firewall) and/or educating users about social engineering.

## Continuous Risk Assessment and Treatment

In this era where the threat landscape is evolving and threat vectors (BYOD, IoTs) increasing day by day, there is need for maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. A network is only as strong as its weakest security link. Continuous risk assessment and treatment calls for constant monitoring of the endpoints and remediation of the identified issues. Efficient remediation will involve starting to remediate the most critical issues to the less critical.

## Managed Services and Independent Reviews

With the increase in work overload of in-house security teams, higher pressure to show ROI quickly and higher potential for collusion between security analyst and an insider attacker, there is need for organizations to look at the option of engaging the services of managed service providers. These providers come with wide range of expertise to manage security related incidents and provide independent reviews for the organization.



## Nigeria Cyber Intelligence Report

In this section of the report we share cyber threat intelligence from the Serianu Cyberthreat Command Centre-SC3. This section aims to provide an analysis of local (Nigerian) cyber security threats, trends and insights concerning malware, spam and other potentially harmful business risks observed by the Serianu Cyberthreat Command Centre.

For the purposes of this report, we inspected network traffic inside a representative of Nigerian Organizations, reviewed contents of online network monitoring sites such as Project honeypot and reviewed information from several sensors deployed in Nigeria. The sensors perform the function of monitoring an organization's network for malware, and cyber threat attacks such as brute-force attacks against the organization'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.

## External Cyber Threat Landscape

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



### Project Honeypot Intelligence Analysis

This section covers data from the honeypot project, a global database of malicious IP addresses. We analysed data specific Nigeria.

## IP Statistics

### Analysis

a.

The IP Address

**41.222.208.33**

was found to be the

**top IP address** in

total malicious events, total spam servers, top dictionary attackers and top comment spammers.

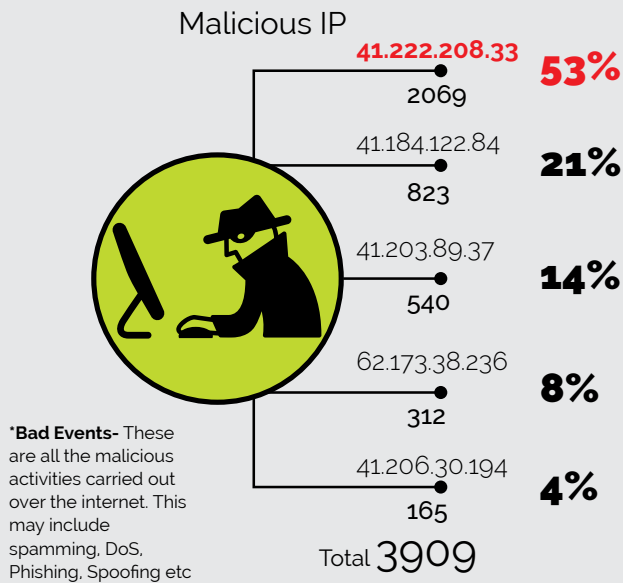
b.

The category that had the **Highest** number of malicious activity is

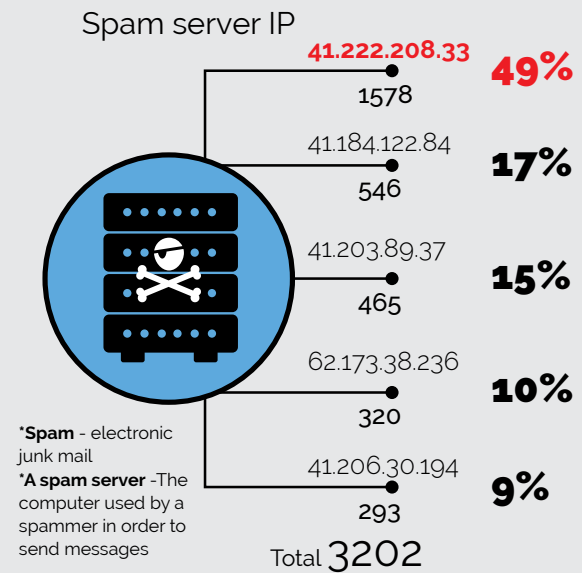
**comment spammers**



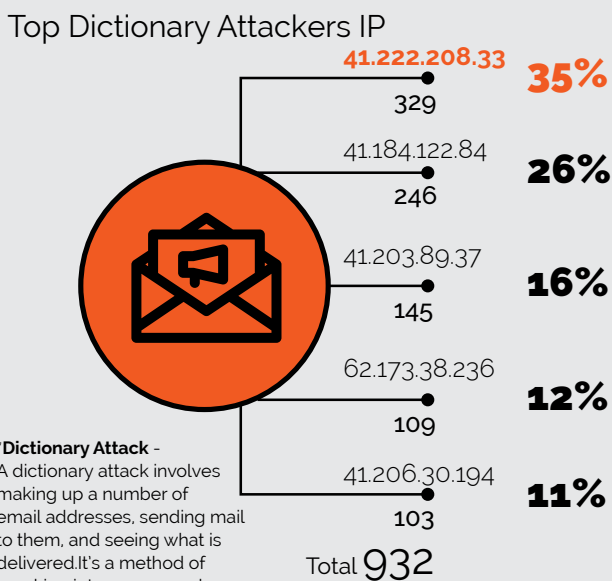
## Total Bad Events



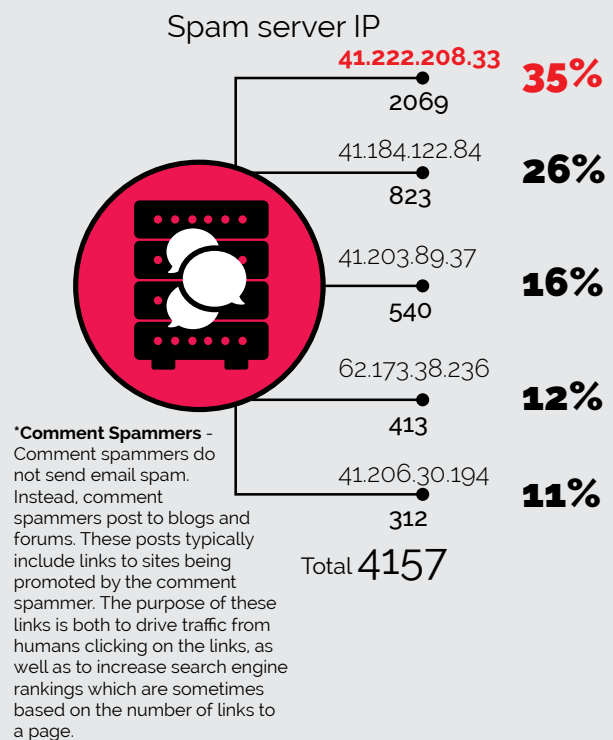
## Top Spam Servers-Email



## Dictionary Attackers



## Top Comment Spammers



External Cyber Threat Landscape

In this section, we provide a summary of data collected from a controlled review of publicly available IP addresses in the countries in scope.

Scan Analysis

a). Vulnerable Ports

Port 80 formed the highest percentage of the online running services at 18%. Running applications on this port comprise of routers, web servers, applications and web portal management systems which are vulnerable to attack

b). Routers

MikroTik and Cisco routers are the most vulnerable enterprise routers at 39% and 19% respectively

c). Web Servers

Apache HTTPD was the most vulnerable web server at 28% followed by IIS Server at 14%

d). Applications

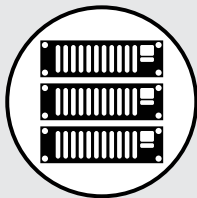
Mail Servers formed the highest percentage of the analyzed vulnerable applications with Microsoft Outlook Web App being the most common mail server identified.



Port 80  
**18%**  
Ports 443, 8080, 3306, 3389, 22, 23, 21, 445, 139  
**9%**  
**Most Vulnerable Port**



MikroTik  
**39%**  
Cisco  
**19%**  
**Most Vulnerable Enterprise Routers**



Apache HTTPD  
**28%**  
Mic IIS Server  
**14%**  
**Most Vulnerable Web Server**



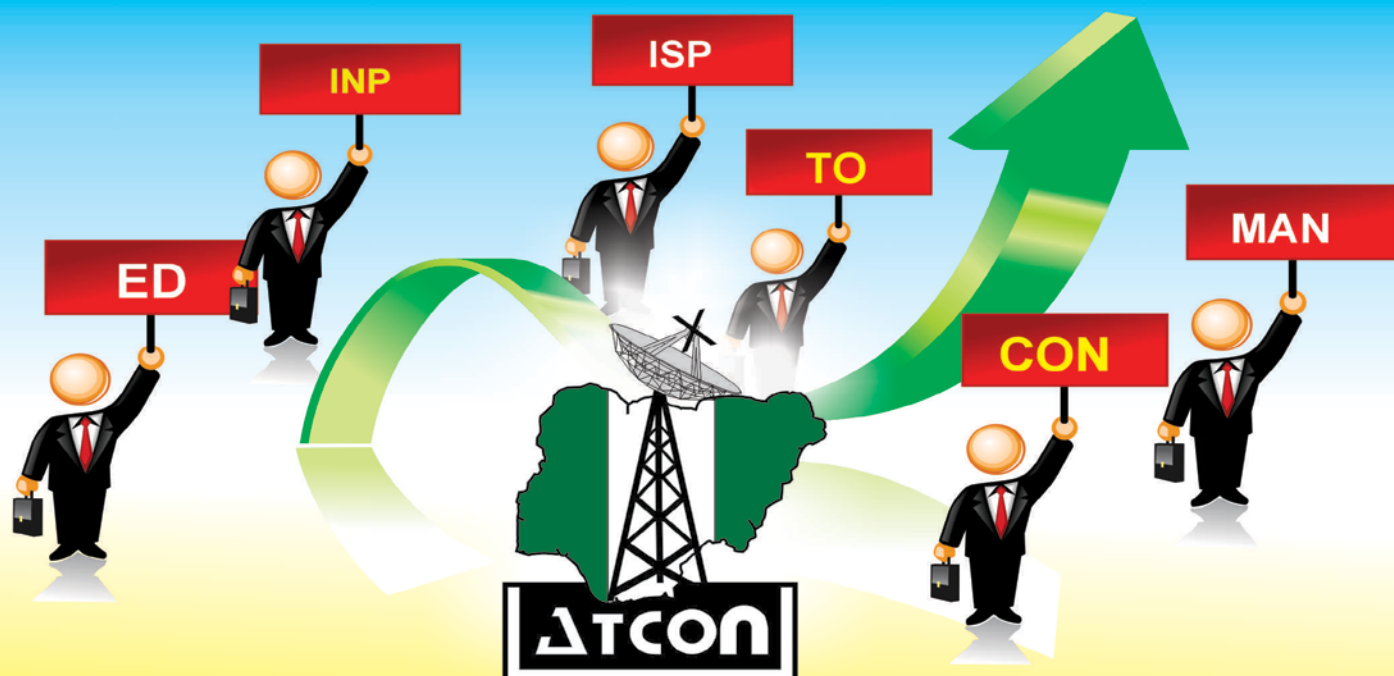
Microsoft Outlook Web App  
**Most Vulnerable Application**

Traffic Analysis - Trojan Traffic



TROJAN W32/Dridex POST CnC Beacon **49%**  
TROJAN MS Remote Desktop micros User Login Request **22%**  
TROJAN MS Remote Desktop edc User Login Request **5%**  
EXPLOIT Possible CVE-2014-6271 Attempt Against SIP Proxy **19%**  
CNC Ransomware Tracker Reported CnC Server group 5 **13%**  
EXPLOIT Supermicro BMC Password Disclosure **2%**

# 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](http://www.atcon.org.ng)

...Partnering for Telecom Development!

**Dr. Nwonyi Polycarp Emeka**

Manager Intelligence, Police Special Fraud Unit (PSFU)  
Force Criminal Investigation & Intelligence Department,  
Lagos



Over my 20 plus years of being involved in cyber security and electronic fraud investigation and prosecution, there has never been a time with major cybercrime upswing like the past few years. The reason for this can be attributed to poverty, adventurism, disgruntled revenge, bad socio-economical/political policies, negative/failed religio-cultural norms, and unemployment. The recent launch of cashless policies as well as growing e-business solutions in the country has further exasperated this situation.

The lack of adequate cyber threat preventions infrastructure and logistics as well as the absence of a strong legal framework that guarantees timely prosecution of identified cases has further encouraged people to get involved in cybercrime. Rather than looking at this as a collective problem to be addressed by all, many still see the solution to identify and fight cybercrime as an exclusive preserve of the government. However, it has been found that the biggest source and victim of cybercrime are individuals and corporate entities in the private sector. The private sector has simply not done enough investment in fighting cybercrime.

The government needs to do more in the area of legislative revamp in empowering stakeholders like law enforcement agencies on capacity building, and encouraging synergy amongst the various agencies. Research grants need to be established for training and empowerment of the public on cyber security services. Human resources/capacity building is key, backed up by legal and legislative reviews of the current laws.

There is need to understand the cybercrime dynamism, developing information technology essential for fighting cybercrime, and closing the loophole between government agencies. A public-private sector initiative is required to build the intelligence and strategy required to be ahead of the cyber criminals. A policy document outlining with detection/investigating/prosecuting of cybercrime, protecting trusted communication and safety, security software and hardware requirement and guidelines.



### Onajite Regha

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

#### Do you think Cyber security is a major problem in Nigeria?

Yes, Cyber security is a major challenge in the country and we all know that it is a global issue. The main cause of this is the inadequate technical support infrastructure and policy to guard and guide the use of the cyber space. In addition, domestic and international law enforcement, unemployment, poverty rate, corruption, lack of standards and national central control, lack of national functional databases, proliferation of cybercafés, porous nature of the internet are also challenges. We thank the National Assembly especially the 7th National Assembly that passed the Bill on the Cybercrime which the former President Goodluck Jonathan has signed into law.

#### Do you think the private sector is investing enough in cyber security?

Is the private sector investing? Of course they are because for the many that offer any type of services via the internet the integrity of their system will be at stake if they don't secure their space. However we cannot say that they have reached the pinnacle of investment in cyber security as long as these cyber criminals are perfecting their acts and look for more sophisticated techniques to commit cybercrime.

Cyber security is a national problem and should be seen and treated as such. Achieving a secured cyberspace should involve the coordinated collaboration between the private and public sector. It needs viable legislation and political will power of the government to enforce existing laws and policy that will address the issues in the cyberspace. Our law has to recognize the cyberspace and its activities knowing that just as in the real world criminal abound in the cyberspace and proactive measures should be taken to protect the nation in that sphere. The government therefore has to invest in cybersecurity with the

### Achieving Cyber Security Resilience



collaboration or the private sector to defend itself against cyberattack from friendly and hostile countries. Not having solid cyber defense as a country means that our cyber space could be easily breached by intruders which can bring about a monumental damage to our economy and security as a whole.

#### In your opinion what drives criminals to commit cybercrime?

It is a well-known fact that criminals will go where the money is and where they find that the security is lax. They will always take advantage of loopholes in a system and use it for their criminal gains. The internet is a relatively new phenomenon which offers good and bad opportunities. Unemployment, poverty, lack of adequate infrastructure amongst many others contributes to this. Most cybercrimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These "expert" criminals find new ways to commit old crimes, treating cybercrime like a business and forming global criminal societies. Criminal societies share strategies and tools thereby combining forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities. It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things incognito and from any location on the globe. Many computers used in cyber attacks have actually been hacked and are being organized by somebody far away. Crime laws are different in every country too, which can make things really complex when a criminal launches an attack in another country.

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

Cybercrime is a national issue. Just like offline crime where people build walls and gates to protect them from thieves. It is not a cross for the private sector alone. Everyone has a part to play. For us it's more of a PPP project for national good. The government may or may have not put in place processes and infrastructure to support the private sector in combating cybercrime, but we all can come together in a concerted effort to combat cybercrime. One of such is collaborative platform is the Nigerian Electronic Fraud forum where the regulators and the stakeholders such as the E-Payment Providers Association of Nigeria and the Banks and other stakeholders meet to come up with effective ways and action plans to curb electronic fraud . This is yielding great results in the electronic payment space. If we scale up this type of collaboration to a national level because cybercrime cuts across all industry, we will be able to achieve more and everyone will benefit. In other words, while companies and individuals will do the best to protect themselves from hackers and cyber criminals, government has to reform our police system, the judicial system and all other stakeholders to combat cybercrimes.

**Do you personally know of a company or individual who's been affected by cyber crime?**

Yes I do

**Were these cases reported to government authorities and prosecuted?**

Yes. Our Annual Payment Systems and Fraud Conference 2015 shown cased someone whose account was breached by cyber criminals. The case was taken up by the security officers present at the conference. Investigation commenced. Remember cyber criminals operate as a cartel. Once you entrap one, it's possible to get others in the ring.

I believe the authorities are aware of some of the crime in the financial industry. The banks and other players in the financial industry announce how much they have lost to fraud every year. It's to check the percentage of that loss that is electronic and cyber fraud. I am worried though that the capacity of government to fight this crime is hampered by our poor legal and police system. That is the industry and key stakeholders came up with a structure such as

the Nigeria Electronic Fraud Forum. This allows exchange of information and knowledge sharing on fraud issues amongst key stakeholders, ensuring collaboration and proactive approach to tackling and mitigating fraud while limiting its occurrences and loses.

**What do you think would be the best approach to address the cyber crime issue in Nigeria**

We need to have the right legislative environment to allow police and the courts bring criminals to justice whether in cyber or physical world. At the moment we are struggling with basic policing when criminals are moving online. We need to have cyber commands in our police and military to first understand the threat and then prepare to fight it. Others are education, mobilization & sensitization, establishment of programs & IT forums for Nigerian youths, Cyber Ethics and Cyber Legislation Law.

**From an African context, what would be the top priority to address cybercrime across the continent?**

A 2013 report warned of Africa becoming a "safe harbor for cybercrime" is frequently quoted in articles about online security. It cited increased internet availability at lower costs, a rapidly growing internet user base and the dearth of cybercrime laws on the continent as contributing to this threat. However, Africa can have a conversation around continental response to Cybercrimes.

As I am aware, Governments in Africa are working with Interpol and regulatory bodies to develop global strategies to tackle cybercrime and bring together evidence, academic research and innovative practice from around the world. They are also recognizing the value of education and training, not just for those who work to fight crime but as a means to prevent it by empowering people to stay safe online. I believe nations need to protect themselves and entities that exist in those countries.

If criminals can exploit the power of networking, then networking on a global scale is vital in the fight against them. But like most things that concern developing countries, capacity to police their cyber space will be related to how good they are in providing networking infrastructure for their citizens



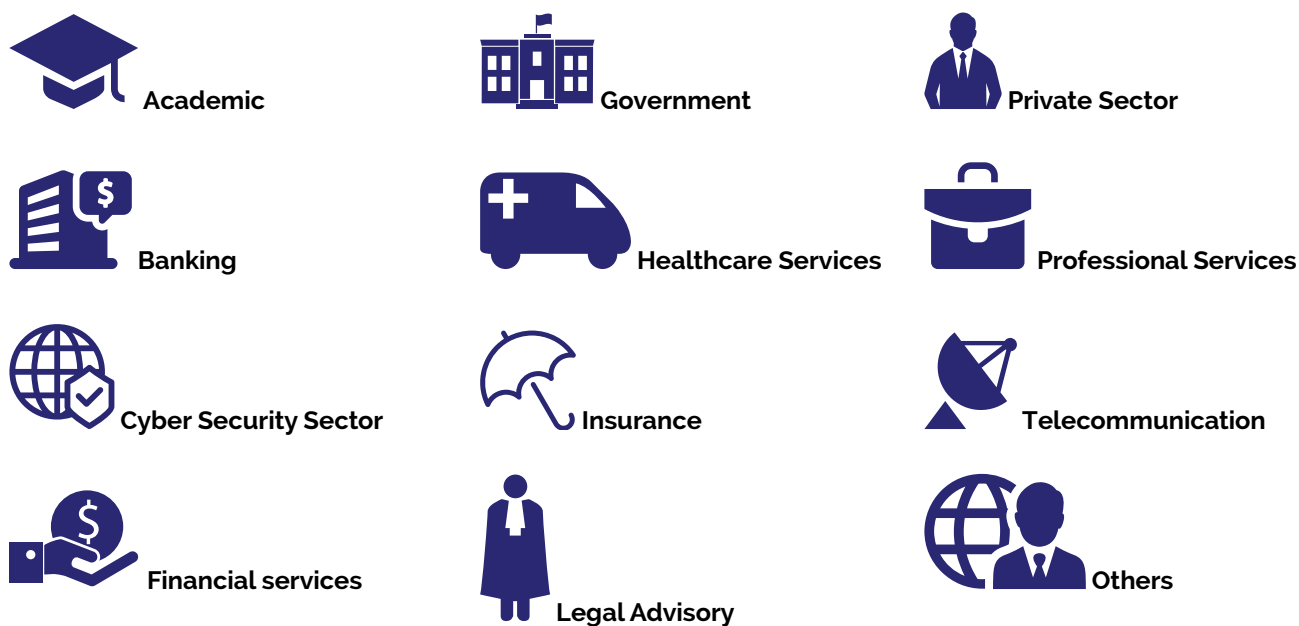
## 2016 Nigeria Cyber Security Survey



The goal of the Nigeria Cyber Security Survey was to explore the evolving threat landscape and the thousands of cyber-attacks that have been forged against individuals, SMEs and large organizations within Nigeria. Cybercriminals continue to take advantage of the vulnerabilities that exist within systems in Nigeria and the low awareness levels. **This survey results identify current and future cyber security needs within local organizations and the most prominent threats that they face.**

### About the Survey

report was prepared based on data collected from a survey of over 300 respondents across organizations in Nigeria. This included companies from the following sectors:



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, HR professionals and office managers). The survey measures the challenges facing local Nigerian organizations and the security awareness and expectations of their employees.

## Summary of Findings

According to the survey findings, **98.3% 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's expected that majority of individuals have a general idea of what cybercrime is.



### 01 97% of organisations are concerned by Cybercrime.

**97%** Concerned about cybercrime

while **3%** Not Concerned



### 02 CyberCrime is a problem rooted in technology says 40% of the organizations.



**40%** believe its rooted in technology

while

**15%** believe its rooted in the society



### 03 75% research on cybercrime regularly but more than 82% lack adequate management systems.

**75%** research information on cybercrime regularly

while

more than **82%** lack adequate management system



### 04 More than 55% organisations DO NOT regularly train their staff on cyber security.



**55%**

not given training or get training only when an incident occurs

**14%** never given training

### 05 Does your organisation allow the use of Bring Your Own Devices (BYOD)?



over

**56%**



allow

**44.1%**

not adopted



### 06 Does your organisation have a best practices policy for BYOD?

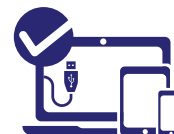
**47.4%**

Have

while

**34.7%**

Don't have



**07** More than 63% have experienced a cybercrime in the last 5 years.

**63.4%**

through work or at personal capacity



**08** If you have been a victim of cybercrime in the last 5 years, what was the effect of the action?



**65.3%**

experienced negative impact



**09** Less than 18% reported cyber crime incidents.



**82%**

did not report cases of cybercrime

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



**95%**

spend less than \$5000 on cyber security annually

**11** 83% of organisations manage cyber security internally or lack management systems in place.

**17.4%**

outsourced to either an ISP or Managed Services providers while



**82.6%**

manage cyber security internally or don't have any management system in place.

**12** Is your organisation's security policy based on globally accepted standards?

**70.4%**

don't base their policies on International standards like ISO 27001, PCI DSS, NIST etc

while

**29.6%**

have defined security frameworks based on these standards.



**13** Which repository contains the most sensitive data in your organisation?

**25%**

general purpose file servers contain most critical information



**14** To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?



**19%**

Improve our understanding of society and the cyber community

**16%**

Better education of users of the Internet & Better encryption and improved privacy

**14%**

Better laws and regulations.

**13%**

Improved technology for our networks and operating systems



## Analysis

According to the survey findings, majority 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's expected that majority of individuals have a general idea of what cybercrime is. Concerns around cybercrime are also very high.

Monetary investments in cyber security products however, does not match up to the levels of concern registered earlier. Majority of the organizations represented in the survey spend no money or less than \$5,000 annually on cyber security product. From our research and analysis, we established that the average number of days taken to detect an attack in a typical organisation in Nigeria is 260 days and an additional 80 days to resolve the attack. However, It takes double this time to detect and resolve malicious insider attacks especially for organisations that don't invest in cyber security products; these products include solutions that facilitate anticipation, detection, recovery and containment of cybercrime.

With the increase in use of BYOD, businesses are now saving money by not having to equip and maintain an increasingly mobile workforce.

With the expensive devices they need to do their jobs, it was found that more than half of the organizations represented in the survey have adopted BYOD. However, even with these developments, more than 40% did not have any internal device usage policy or BYOD policy to govern the usage of these devices.

When it comes to cyber security management, a majority of the respondents (38%) manage their security In-house, 13.6% have an in-house CERT whereas 12.7% have independent specialists or organizations dedicated to handle their security needs while 16.9% have no knowledge on how their cyber security is managed.

It should be noted that, even though majority of the companies are managing their cyber security in-house, more often than not these individuals are overloaded with other tasks within the organization and/or lack the necessary skill set to handle cyber incidents efficiently. This is based on the survey results which reflected that only 29.6% of the respondents had Information Security Management certifications while 40.8% did not have the relevant. Moreover 29.6% of the respondents had no knowledge of Information Security Certified personnel within their organisation.

## Highlights of Nigerian

### Organisations:



Majority of respondents have a general understanding of what cybercrime is.



Majority of the organizations spend

less than **\$5,000** annually on cyber security product



More than half of the organizations have allowed

BYOD but **40%** don't have any BYOD policy



**38%** manage their security In-house,

**13.6%** have an in-house

CERT, **12.7%** have independent specialists

while **6.9%** have no knowledge on how their cyber security is managed

...cont



**29.6%** had Information Security Management certifications,

**40.8%** dont have

while **29.6%** had no knowledge



**24.9%** carried out penetration and vulnerability testing,

**18.8%** carry out audits while **56.3%** have no knowledge of any testing techniques



**63.4%** have been affected by cybercrime in one way or another



**92.5%** security incidences go unreported or unsolved

Of equal importance was that 24.9% of the respondents carried out system testing in terms penetration and vulnerability testing. 18.8% carry out audits while 56.3% have no knowledge of any testing techniques have been implemented in their organizations. All these testing techniques are not independent and in fact work best when they are applied concurrently.

More than half of Nigerian businesses are vulnerable to cyber-crime with most of them being unaware of it. This is because these organisations do not perform any form of assessments within their environments. Only 6.6% do Penetration testing, 18.3% Vulnerability testing and 18.8% Audits. It should be noted that all these testing techniques are not independent and in fact work best when they are applied concurrently

With the increased rate of Cybercrime in Nigeria, most of the respondents (63.4%) have been affected

by cybercrime in one way or another. Out of these, 65.9% was within the work environment while 34.1% was in their individual day-to-day interactions. This highlights the importance of incorporating cyber security awareness and vigilance in the work environment as it is the most susceptible to cybercrime incidences.

There are low levels of awareness within Nigeria, hence it is no surprise that when it comes to reporting of cybercrime to the police the number of security incidences that go unreported or unsolved stand at 92.5% whereas only 6.6% of the reported cases were followed through to a successful prosecution.

External Infrastructure Vulnerabilities identified during the survey include unnecessary services enabled such as content management and remote administration, misconfigured SSL certificates and encryption settings. With these vulnerabilities an unauthorized attackers can easily get access to critical systems.

The results of our Internal Traffic Analysis revealed that there are numerous forms of Malware on systems. This includes trojans such as Dridex and Zeus malware. Most of these go undetected malware on systems.



Rajat Mohanty

Chairman and CEO, Paladion Networks

Achieving Cyber Security Resilience



Cybersecurity Needs a New Paradigm - Speed!

Companies today are spending more than ever to protect their digital assets. Worldwide spending on cyber security has reached over 80 billion and likely to double in next 4 years. Yet, security breaches are rising year on year, with a compounded growth rate of 60% for last 5 years. This year itself, we have already seen one of the largest data breach in history affecting 500 million user accounts, one of the largest attack on banks with USD 100mn stolen, more than hundred other mega breaches and thousands of ransomware attacks. Obviously, more security spending is not translating to better security.

Asymmetry in Cyber Security

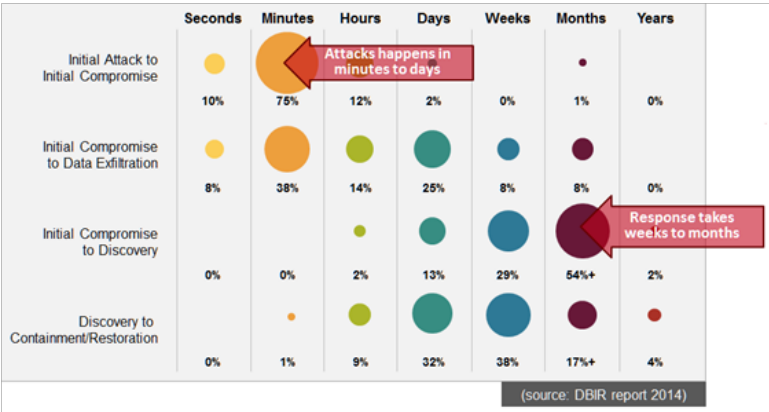
It's a common adage that while defender has to protect thousands of weaknesses, an attacker needs to find just one and exploit it. Cyber security fundamentally is an asymmetric problem where defense needs manifold resources compared to an attacker. The dominant paradigm of last decade in cyber security was layered security where more and more security products were installed for creating a defense in depth. While that paradigm still holds good for prevention, it has diminishing returns beyond a point.

Due to this over last few years, industry has reached an acceptance that it is not possible to prevent incidents within finite resources, rather it should focus on detection and response capabilities. Hence the new paradigm has come into being- invest in detection and response while accepting breaches will happen.

State of Detection and Response

Modern attacks are sophisticated and long drawn. Advanced attackers enter into a network with initial attack and then navigate through the network over months to

carry out their objective. The industry average shows that these breaches are not detected till around 200 days by the organizations. As per Data Breach Investigation Report 2015, over 60% of the times such breaches are actually reported by external entities and not detected by organizations themselves.



Even when the attacks get detected, the response takes weeks to months in containing, eradicating and recovery from the attacks.

This delay in detection and response is the primary cause of large losses due to cyber breaches. As per the survey by IBM 2016, the average loss per data breach is over 4 million USD. That cost can be significantly reduced if the attacks could be detected and responded early.

Speed as the new Determinant of Success

Given that breaches are inevitable and organizations will have security incidents despite best effort, the focus should shift to how soon the breaches can be detected and how



fast they can be responded. No organizations get impacted because they get breached, they get affected and become news items only due to the long period of time that elapses from an attacker's first entry to the final detection and response. What security needs as a new paradigm is speed of operations: increasing the speed in discovery and response. With enough speed, every breach will be insignificant. As part of this paradigm, the questions that management should ask are- How fast can we detect attacks- Is it as fast as the attacks themselves? And how fast can we investigate, contain and eradicate attacks- Is it as fast as the attacker's movement within the network?

Cyber security of future will focus on investing in capabilities that increases speed of security operations. Primarily that involves three aspects-

- 1. 360° Situational Awareness:** For fast discovery of attacks, the security operations should have full visibility into every asset, user activity, network traffic, system vulnerabilities and network topography at all times. Today, such visibility is limited to critical assets and users, which severely impedes discovery of attacks. With rapid progress of big data technologies and reduced cost of storage, organizations need to move towards a strategy of collecting and storing all security data for full situational awareness.
- 2. Applying machine learning:** Modern attacks bypass traditional rule based security systems. Such attacks thus remain undiscovered for long period till further activities of the attacker trigger a rule based alert or gets noticed by external entities. For faster discovery, the detection methods should use machine learning system which do not rely on rules. Machine learning discovers abnormalities based on patterns, profiles, past incidents and mathematical models, going beyond just rules. Today machine learning is getting used in every filed of IT and business and it is time to introduce them into security operations to provide fast early detection of advanced attacks.

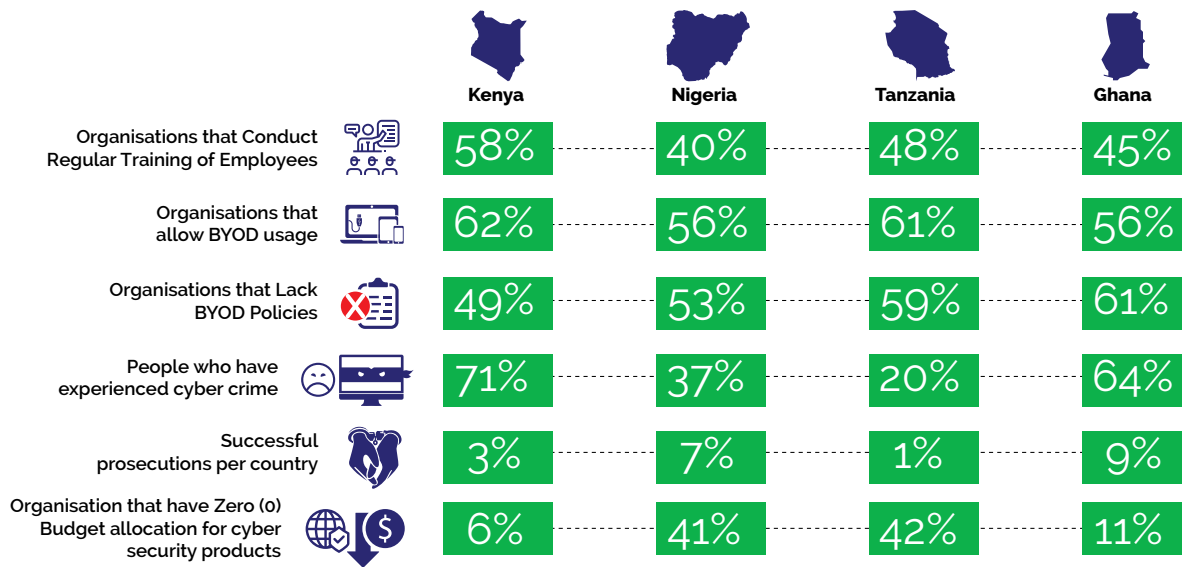
### **3. Automation for response:**

Today the process of triaging, investigating and containing an incident is entirely manual. If an alert is triggered, the security operation center today manually collects data from systems and manually analyzes the incident. The containment action in terms of system configuration, access, changes or reimaging are all manual. This significantly increases the response time. Modern SOC need to invest in automation and orchestration platform to make response as fast as the attacks.

The way forward for cyber security is to have the security operations run so fast that the impact of breaches become immaterial. Speed will be the new determinant of success for cyber security and investing in such capabilities will differentiate between good organizations and breached organizations.

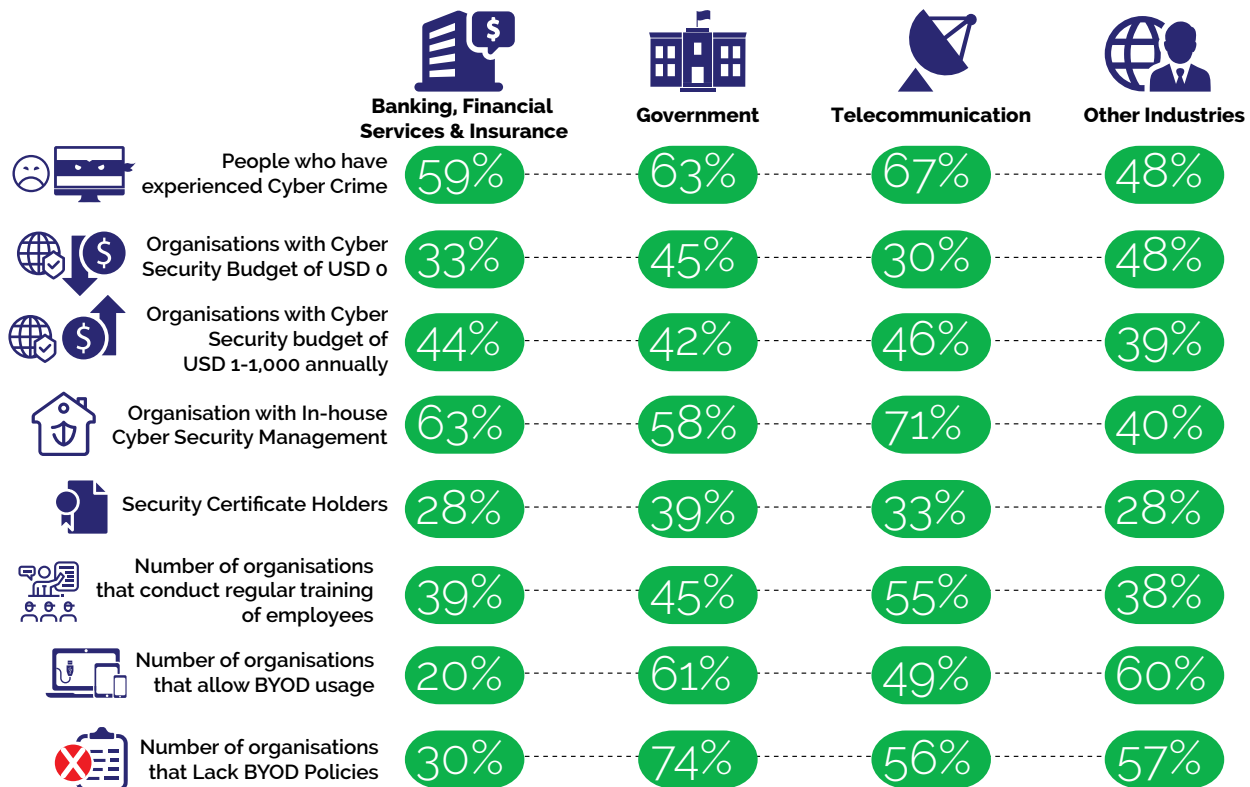
## Inter Country Analysis

For this section, we evaluate how the different countries in scope compare to each other.



## Industry Analysis







For this section, we look at how the different Industries and compare their performance using different metrics.







## Cause(s) and Effect(s) of Cyber Security in Nigeria

### 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)
<b>Understanding of Cyber Crime</b> 	Perceptions are different on what is an act of cybercrime.	<ul style="list-style-type: none"> <li>◆ No standard definition</li> <li>◆ No collaboration between countries to fight cyber crime</li> </ul>	Clear-cut definitions of cybercrime and cross-border co-operation to improve legal sanctions	How Nigerian companies can collaborate and share information on cybercrime issues.
<b>Monetary investments in cyber security solutions</b> 	Limited or no investments in Cybersecurity solutions	Organizations are losing money through cyber-crime.	<ul style="list-style-type: none"> <li>◆ Cater for cyber security during annual budgets</li> <li>◆ Proactive Investments in analysis, analysts and incidence response.</li> </ul>	Metrics to determine minimum budgetary allocations for Cyber security for different industries.
<b>BYOD</b> 	High BYOD usage with low rates of best practice policies	<ul style="list-style-type: none"> <li>◆ Acceptable usage of company resources not defined</li> <li>◆ High risks associated with such devices</li> </ul>	<ul style="list-style-type: none"> <li>◆ Define BYOD policies</li> <li>◆ Compliance within the workplace. Effective measures in place</li> </ul>	Policies and best practices for the workplace
<b>Cyber Security Management</b> 	<ul style="list-style-type: none"> <li>◆ In-house management of cyber security</li> <li>◆ Cyber security roles combined with other IT roles</li> </ul>	Individuals assigned cyber security roles in organizations are more often overloaded with other tasks within the organization and/or lack the necessary skill set to handle cyber incidents.	Develop in-house CSIRTs, defined IS Departments or Managed security services.	Developing, operating and maintaining cyber security functions at the work place.
<b>Information Security Certification &amp; Technical Training</b> 	Few individuals with sufficient security technical training	Company employees lack basic information about information security foundation principles, best practices, important tools and latest technologies.	<ul style="list-style-type: none"> <li>◆ More training on different Information Security standards</li> <li>◆ Acquire information security certifications.</li> </ul>	Training more information security professionals
<b>Employee Training</b> 	Employee training done mainly after a cyber security incident	<ul style="list-style-type: none"> <li>◆ Sharing information with unknown entities</li> <li>◆ Poor internet practices</li> <li>◆ Lack of preparedness after an incident</li> </ul>	<ul style="list-style-type: none"> <li>◆ Conduct regular people based risk assessment</li> <li>◆ Develop an employee security awareness program</li> </ul>	<ul style="list-style-type: none"> <li>◆ Developing and running and effective security awareness programs.</li> </ul>

## Achieving Cyber Security Resilience

Theme	Scenario	Consequence (s)	Mitigation	Identified Gap(s)
<b>Reporting of Cyber Crimes</b> 	High number of cybercrime is not reported to police, and for those that are reported, very few are followed through to prosecution.	<ul style="list-style-type: none"> <li>Immature cyber security bills, laws and processes.</li> <li>Lack of user awareness</li> </ul>	<ul style="list-style-type: none"> <li>Adopt more mature processes for cybercrime prosecution.</li> <li>Involve more sectors during development of cyber laws; Universities, local groups, organizations and cyber security specialists.</li> <li>Raise awareness to citizens on reporting of Cyber crimes</li> </ul>	<ul style="list-style-type: none"> <li>Escalation matrix for country wide cybercrime reporting.</li> </ul>
<b>External Threat Analysis</b> 	<ul style="list-style-type: none"> <li>Publicly accessible IP infrastructure has unnecessary services enabled, including content management and remote administration</li> <li>Misconfigured SSL certificates and encryption settings.</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized access to critical systems</li> <li>High rise of wide spread attacks leveraging vulnerable infrastructure</li> </ul>	<ul style="list-style-type: none"> <li>Monitoring the latest security vulnerabilities published</li> <li>Updating the security configuration guideline</li> </ul>	<ul style="list-style-type: none"> <li>Standard Configuration for systems</li> <li>Continuous testing and monitoring</li> </ul>
<b>Internal Cyber Threat Analysis</b> 	<ul style="list-style-type: none"> <li>Use of obsolete systems and Apps</li> <li>Use of clear text and insecure protocols</li> <li>Server misconfiguration</li> <li>Use of default credentials</li> </ul>	<ul style="list-style-type: none"> <li>Unauthorized access to critical systems</li> <li>Vulnerable systems</li> </ul>	<ul style="list-style-type: none"> <li>Configuring all security mechanisms</li> <li>Turning off all unused services</li> <li>Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords</li> <li>Applying the latest security patches</li> <li>Regular vulnerability scanning from both internal and external perspectives</li> </ul>	<ul style="list-style-type: none"> <li>Password management and best practice</li> <li>Patch management best practice</li> <li>Emergency patch management practices</li> </ul>
<b>Internal Traffic Analysis</b> 	<ul style="list-style-type: none"> <li>Malware on systems</li> <li>Botnets in private infrastructures</li> </ul>	<ul style="list-style-type: none"> <li>Undetected malware on systems</li> <li>Delayed incidence response</li> </ul>	<ul style="list-style-type: none"> <li>Continuous monitoring Incidence response plan</li> </ul>	<ul style="list-style-type: none"> <li>Managing 24X7 monitoring</li> <li>Traffic monitoring and analysis</li> </ul>



### Olusola Teniola

President Association of Telecommunications Companies of Nigeria (ATCON)



#### Do you think Cyber security is a major problem in Nigeria?

Yes

#### If yes, what do you think is the main cause of the Cyber security problem?

[OT] Data protection and privacy are weak areas where data sovereignty means that a majority of applications and services being adopted by Nigerians are based in foreign climes, including Government data and services. This needs to be immediately addressed.

#### Do you think the private sector is investing enough in cyber security?

The digital age race suggests that we have a lot more work to create a local content environment and to fully implement the cybercrime bill to its fullest. A significant further funding is required by not only the private sector but also by the public sector.

#### In your opinion what drives criminals to commit cyber crime?

The temptation of circumventing weak systems around the world is a known fact! Weak systems and processes attracts criminals, cyber terrorists and the radicals to break in and create havoc in complex systems.

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

Government is still recognizing what exactly is cyber crime, basic IT development and this means that Government hasn't yet begun to address the infrastructure let alone the processes required to combat cyber terrorism and cyber crime. I believe our Government is at least 7 years behind South Korea or China.

#### Do you personally know of a company or individual who's been affected by cybercrime?

Not in Nigeria, as media hasn't been able to reveal anything significant.

#### What do you think would be the best approach to address the cyber crime issue in Nigeria

We need to create an arm of the Government that will specifically address cyber related issues and a framework should be out in place to ensure that Nigeria implements a blueprint that solves our idiosyncratic challenges

#### From an African context, what would be the top priority to address cybercrime across the continent?

All legal framework that unify various cyber counter measures needs urgent implementation across Africa both at regional levels and nationally. Then we need a communicate that resolves interoperability challenges across borders to ensure seamless security protection and exchange of data in different jurisdictions.



### Abdul-Hakeem Ajijola

Chair, Consultancy Support Services Ltd., Abuja, Nigeria.  
A Cybersecurity & Cybercrime Advisor and Consultant



#### Do you think Cyber security is a major problem in Nigeria? If yes, what do you think is the main cause of the Cyber security problem?

Yes, I believe that Cyber security is a major challenge. Nigeria, like most of the world, is building an electronic future upon capabilities, processes and infrastructure that it doesn't understand how to protect. There is a common saying in Nigeria that "Awoof dey run belle." This also applies to cyberspace; we must not get carried away. "If something is "free" then know that you are not the customer, but you are the product being sold. Do you think the private sector is investing enough in cyber security?

I believe all sectors can and should do more. Sometimes, however, it is not simply a case of spending more, but spending more, smartly.

#### In your opinion, what drives criminals to commit cyber-crime?

I believe that there are 3 broad reasons why people commit cyber-crimes: Financial gain, Political ambitions and Personal reasons (Script kiddies).

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

I believe that the government has started putting in place processes but much more needs to be done. It's critical that the government, private sectors, academia, civil society and our youth work together to ensure enhanced Cybersecurity Solutions are in place. I believe that we can only succeed by working together.

#### Do you personally know of a company or individual who's been affected by cybercrime?

Yes, many Nigerian websites have been and continue being defaced. Between 13 April 2015 & 01 Feb 2016, Zone-H received notifications of 3,599 breaches of Nigerian (.ng) domains out of which 2,518 websites were defaced. There have also been a number of serious database breaches and intrusions reported in the press over the last few years that involve Nigerian organisations in the private, government and academia.

#### Were these cases reported to government authorities and prosecuted?

I do not know. It should be noted that cybercriminals operate at the speed of light while law enforcement moves at the speed of law. Even with this, several prominent cases were reported by the press implying that no form of formal reporting to the authorities has taken place. We however appreciate all is not lost as in 2015, the president signed the Cybercrime (Prohibition Prevention, etc..) Act 2015 into law.

#### What do you think would be the best approach to address the cyber-crime issue in Nigeria?

Build capacity by generating synergies among Government, Private Sector and Academic Institutions so as to enhance another triple helix of People-Process-Technology.

#### From an African context, what would be the top priority to address cybercrime across the continent?

Similar to Nigeria, which is to build capacity by constructively bringing together Government, Private Sector/ Industry and Academic Institutions.



**What do you think is the estimated cost of cybercrime to the Nigeria economy?**

I'd base my estimate on McAfee's value of 0.80% of Nigeria's GDP which is \$450 million.

**Parting shot**

The Africa Cybersecurity market was worth \$0.92 billion in 2015 and is projected to grow to \$2.32 billion by 2020. It's up to our youth, policy makers and entrepreneurs to determine what piece of this market share they want to corner. The scope of the market ranges from awareness, prevention, recovery and other professional services. Some specific technical segments for Nigeria to look into and work towards dominating, at least in Africa for now include Antimalware, Data Loss Prevention (DLP), DDoS Mitigation, Disaster Recovery and Business Continuity, Encryption, Firewall, Identity Access Management (IAM), Intrusion Prevention Systems (IPS), Risk and Compliance Management, Security/ Vulnerability Management, Unified Threat Management (UTM)/ Unified Security Management (USM) as well as Web Filtering.

# Scammers using my name, Onu cries out

International Business Times

NAIJ.com

Latest Recession! Boko Haram Football LiveScore Advertise with us

## Anonymous Nigeria Hacks Government Websites, Declares Cyberwar Against Corruption, Poverty, Theft

BY MORGAN WINSOR

ON 01/08/16 AT 3:31 PM

## Nigerian hacks Ghana bank, steals \$25,000

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

Published: 29.07.2016 , Refreshed: 01.08.2016 · Vwovwe Egbo

Print · e

NAIJ.com

Latest Recession! Boko Haram Football LiveScore Advertise with us

## My Twitter Account Was Hacked - Fashola

Akpan Jeremiah 1 year ago

pulse News

## Nigerian hacks Ghana bank, steals \$25,000

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

Published: 29.07.2016 , Refreshed: 01.08.2016 · Vwovwe Egbo

## Scammers using my name

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

## Scammers using my name

## Nigerian hacks Ghana bank, steals \$25,000

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

Published: 29.07.2016 , Refreshed: 01.08.2016 · Vwovwe Egbo

## Nigerian hacks Ghana bank, steals \$25,000

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

## My Twitter Account Was Hacked - Fashola

Akpan Jeremiah 1 year ago

NAIJ.com

Latest Recession! Boko Haram Football LiveScore Advertise with us

OFFICIAL	OFFICIAL	MARKET
1.91	315.25	470
NGN/USD	USD/NGN	USD/NGN

## \$25,000

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

## My Twitter Account Was Hacked - Fashola

Akpan Jeremiah 1 year ago

pulse

## Anonymous Nigeria Hacks Government Websites, Declares Cyberwar Against Corruption, Poverty, Theft

## Nigerian hacks Ghana bank, steals \$25,000

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

Published: 29.07.2016 , Refreshed: 01.08.2016 · Vwovwe Egbo

Gist Celebs Music

## Anonymous Nigeria Hacks Government Websites, Declares Cyberwar Against Corruption, Poverty, Theft

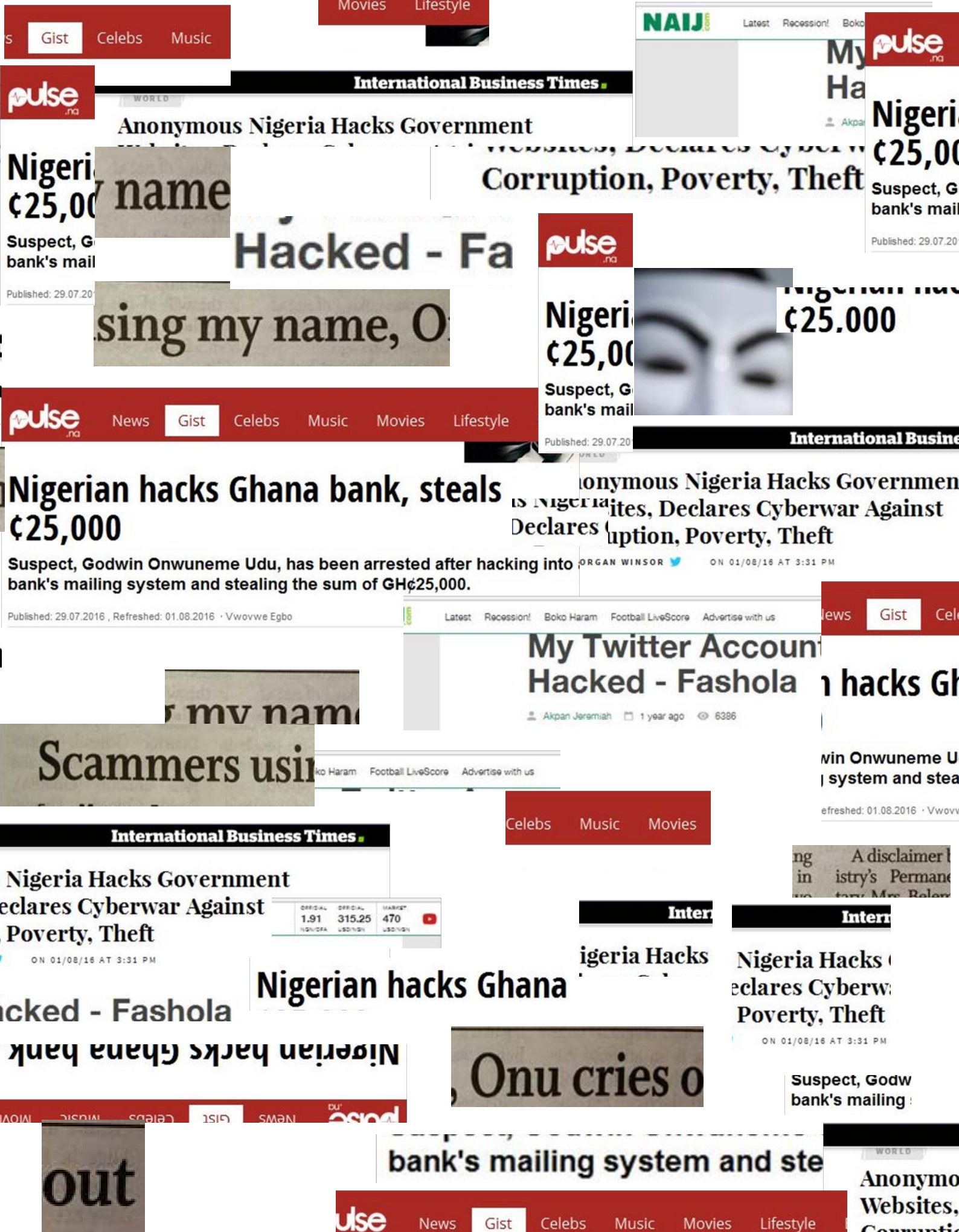
Published: 29.07.2016 , Refreshed: 01.08.2016 · Vwovwe Egbo

## Corruption, Poverty, Theft

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into bank's mailing system and stealing the sum of GH¢25,000.

my name





Gist Celebs Music

International Business Times

NAIJ

Latest Recession! Boko

pulse

WORLD

Anonymous Nigeria Hacks Government

My Ha

Nigeri

\$25,00

Suspect, G

bank's mail

Published: 29.07.20

Nigeri  
\$25,00

Suspect, G  
bank's mail

Published: 29.07.20

name

Hacked - Fa

pulse

Nigeri  
\$25,00

Suspect, G  
bank's mail

Published: 29.07.20

Nigerian Hack  
\$25,000

using my name, O

pulse

News Gist Celebs Music Movies Lifestyle

International Business

Nigerian hacks Ghana bank, steals  
\$25,000

Anonymous Nigeria Hacks Government  
ites, Declares Cyberwar Against  
Declares (upution, Poverty, Theft

Suspect, Godwin Onwuneme Udu, has been arrested after hacking into  
bank's mailing system and stealing the sum of GH\$25,000.

ORGAN WINSOR ON 01/08/16 AT 3:31 PM

Published: 29.07.2016 , Refreshed: 01.08.2016 · Vwovwe Egbo

Latest Recession! Boko Haram Football LiveScore Advertise with us

News Gist Celebs

My Twitter Account  
Hacked - Fashola

Akpan Jeremiah 1 year ago 6386

hacks Gh

Scammers using

win Onwuneme U  
system and stea

refreshed: 01.08.2016 · Vwovwe

International Business Times

Celebs Music Movies

Nigeria Hacks Government  
Declares Cyberwar Against  
Poverty, Theft

OFFICIAL	OFFICIAL	MARGET
1.91	315.25	470
USD/NGN	USD/NGN	USD/NGN

Inter

Intern

Hacked - Fashola

Nigerian hacks Ghana

Nigeria Hacks

Nigeria Hacks  
Declares Cyberwar  
Poverty, Theft

ON 01/08/16 AT 3:31 PM

Onu cries o

Suspect, Godw  
bank's mailing

bank's mailing system and ste

out

WORLD

Anonymous  
Websites,  
Corrupti

pulse

News Gist Celebs Music Movies Lifestyle



## Top Cyber Security Issues in 2016



### Cyberstalking/Social Media Abuse

Cyberstalking is a crime as stated in the Nigeria's Cyber Crime Bill (released on June 24th 2015). Cyber-stalking is the act in which an attacker harasses a victim using electronic communication means, such as e-mail or messages posted to a Web site or a discussion group. On **August 2016**, a **blogger was arrested for allegedly cyber-stalking Government agency personnel**; this revealed the lack of distinction between Freedom of Speech and Cyberstalking.

to an international bank hacking syndicate. The **syndicate managed to withdraw roughly \$20 million from one bank within one month**.

- ◆ In **June 2016**, a cyber security and crime check division team of Dhaka Metropolitan Police (DMP) arrested 2 people including a Nigerian citizen who **hacked into a bank's email account** and took money from the bank account. A hacking team in Nigeria colluded with the assailants to hack the business email while a Bangladesh citizen acquired the hacked amount illegally.
- ◆ In **August 2016** a Nigerian man was accused of being part of a **\$60 million heist** involving a number of individuals from Nigeria, Malaysia and South Africa that compromised email accounts of small and medium-sized businesses around the world. A supplier's email would be compromised and fake messages sent to a buyer with instructions to make payment to a bank account under the network's control.
- ◆ In **August 2016**, a pair of security researchers uncovered a Nigerian scammer ring that operates a new kind of attack called **"wire-wire"** after a few of its members accidentally infected themselves with their own keylogging malware. This technique was used to steal hundreds of thousands of dollars from small and medium-size businesses worldwide.



### Web Defacements

Website defacement is one of the biggest challenges targeting a majority of the Nigeria (.ng) domain sites. It is an attack on a website that changes the visual appearance of the site by hacking into a web server and replacing the hosted website with the attacker's signature.

In 2015-2016 timeframe, Zone-H received notifications of 4,368 breaches of websites with Nigeria (.ng) domains of which **3,383** were **mass defacements**. Majority of the received notifications were from defaced government sites that had been defaced.

**Example of the defacements include:**

**January 2016** - Anonymous Hacks Nigerian Government sites for ongoing corruption, theft and poverty throughout the country.

### Cyber Fraud Landscape

Nigerian Cyber attackers are also targeting other countries to defraud unsuspecting users. Incidences identified include:

- ◆ In **July 2015**, 3 Nigerians are arrested for the **hacking of US bank accounts** by hacking email addresses and accounts and stealing private information.
- ◆ In **October 2015**, a Nigerian graduate **defrauds 2.4 million Naira** from foreign men and women on dating sites and also sends phishing emails to bank customers requesting for passwords, PINs or other bank account security details.
- ◆ In **December 2015**, 7 Nigerians posing as students and tourists were arrested in the Philippines for allegedly belonging





## E-payment Fraud

Financial institutions are fighting a growing threat of electronic payments fraud across a range of payment channels. **NIBSS Instant Payment (NIP), Nigeria recorded electronic transaction volume and value of over 195 million and 40 Trillion respectively, from January to September 2016.**

Nigerians have adopted the use of electronic channels like POS, Internet Banking, Mobile Banking, e-Commerce among others as their preferred means of payment. This is evident in the volume and value of transactions recorded in the year across multiple electronic payment channels.

As Nigerian Banks strive to enhance customer experience by embracing new technologies, majority of bank Cyber-security hacks have succeeded due to weak Information System Security. A number of **2015 Fraud scams** ranged from **email spoofing to hacking of email accounts** and **using the accounts to request for fraudulent money transfers**.

Attackers are targeting possible victims at ATM terminals and point of sales machines across the country. Methods include duping victims having difficulty using the ATM and obtaining their personal identification numbers and using unsuspecting e-payment users to cover their tracks by using their accounts to transfer the amount withdrawn from the victims account.

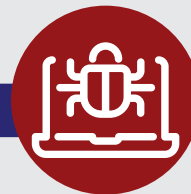


## Cyber Terrorism vs Hacktivism

Cyberterrorism is **the act of Internet terrorism in terrorist activities**, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

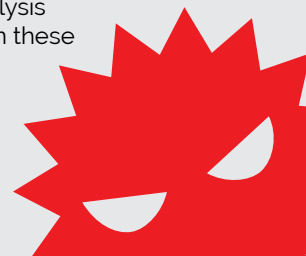
In **2015, Boko Haram pledged allegiance to ISIS in Iraq and Syria**. Boko Haram are now using **email scams to raise funds** and video developing tools as its **online propaganda strategy**.

In **December 2015**, the official websites of the Lagos State Government and the Court of Appeal were hacked by an unknown group sympathetic to the Shiite Muslim sect. The hackers in a message posted on the two websites after the attack, described the Nigerian government as terrorists.



## Malware Attacks

Malware refers to **malicious software programs designed to access or damage a computing device without the knowledge of the owner**. Malware targeting mobile banking, Internet banking and consumer bank accounts are on the rise. Attackers can now access an account through any normal channel after stealing credentials through the infected devices. The results of our Internal Traffic Analysis revealed that there are numerous forms of Malware on these including; Trojans such **Dridex** and **Zeus malware**.





### Dr. Joshua Atta

Project Manager, Nigerian Research and Education Network (NgREN)



#### Do you think Cyber security is a major problem in Nigeria?

Yes

#### If yes, what do you think is the main cause of the Cyber security problem?

Poorly designed networks and lack of investments in network security. A second major problem is the improperly coordinated/ structured system of education which has failed to equip people with good morals and appropriate skills to create jobs or be self-sustaining. Thus, the youth (with poor moral upbringing) tend to have affinity for using their skills for crime and on the other hand, cannot create genuine businesses or trade to sustain them but want to make money easily through crime.

#### Do you think the private sector is investing enough in cyber security?

No

#### In your opinion what drives criminals to commit cybercrime?

Bad morals and advancement in knowledge making it possible for them to bypass security

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

No

#### Do you personally know of a company or individual who's been affected by cybercrime?

Yes

#### Were these cases reported to government authorities and prosecuted?

Yes

#### What do you think would be the best approach to address the cybercrime issue in Nigeria?

More awareness, improvement in the education system, demotivation of crime and more investment in security

#### From an African context, what would be the top priority to address cybercrime across the continent?

More investment in moral education and enhancement of skills and job creation.





### Muhammed Rudman

CEO, Nigerian Internet Exchange



#### Do you think Cyber security is a major problem in Nigeria?

##### If yes, what do you think is the main cause of the Cyber security problem?

Yes Cybersecurity is a major problem in Nigeria. The main causes of Cybersecurity problems are:

- Lack of awareness of end users on how to protect themselves, and the implications of not protecting themselves.
- There is no major agency either of Government or Non-government that is responsible in protecting the citizens against Cybercrime or even where to report incidence of Cybercrime. Though financial crimes are usually reported to the EFCC or the Police.
- Lack of legal framework and the required skill by the law enforcement agents to handle Cybercrime.

#### Do you think the private sector is investing enough in cyber security?

No. Only very few private organizations are investing in Cybersecurity and they are mostly focused on financial institutions (Banks).

#### In your opinion what drives criminals to commit cybercrime?

Mostly for financial gains, but sometimes for political, religious or other reasons.

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

NO - I'm not aware of any such processes or support.

#### Do you personally know of a company or individual who's been affected by cyber-crime?

Yes, I know few companies and it even happen to an organization that I work for.

#### Were these cases reported to government authorities and prosecuted?

No, they were never reported.

#### What do you think would be the best approach to address the cyber-crime issue in Nigeria?

Nigeria has a Nation Cybersecurity Strategy with the Office of the National Security Adviser, we need to ensure the execution of that strategy.

#### From an African context, what would be the top priority to address cybercrime across the continent?

Coordination and collaboration between Government agencies and the Private sector across the continent.



## Risk Ranking by Sector

In this section, we breakdown the current risks facing different industries in Nigeria and in the process provide a risk ranking of these sectors based on likelihood and impact of attack.

1



### Banking

Nigerian banks continue to face electronic fraud mainly in the form of internet banking and automatic teller machine cards. A large percentage of the losses reported are attributed to insiders. Some insiders collude with hackers to illegally defraud the banks. Phishing scams are also on the rise with many bank employees falling for these scams and releasing critical information to malicious attackers. The lack of awareness amongst employees and poorly implemented security controls in Nigerian banks continues to expose the sector to fraud risks. However, the nationwide introduction of the Bank Verification Number (BVN) by the Central Bank of Nigeria has helped reduce these cases and theft in banks have decreased significantly.

from ISPs. These compromised IoTs are being used by attackers as bots to launch further attacks on other sectors.

Recently, Nigeria Communications Commission (NCC) has expressed their concerns over a secure cyberspace and have announced plans to set up Computer Security Incident Response Teams (CSIRT) exclusively for the telecommunications sector.

2



### Telecommunication Companies

The telecom industry has become a major target for hackers. This is especially so because of the vast amount of information that they hold and the many network infrastructures that they support including financial industries and government agencies. Attackers are now targeting these organisations with the intent to disrupt service delivery and infiltrate the data that they hold. Another critical threat unique to telecommunications industry is attacks on leased infrastructure equipment such as home routers



### E-commerce

The E-commerce sector in Nigeria has seen tremendous growth with business activities now being carried out electronically on the Internet rather than at a physical location. While these platforms create a lot of convenience, they collect a lot of information about visitors to their websites. Because of their many misconfigurations and vulnerabilities, we are seeing an increase in the number of online scams, fraudulent transactions and breach of consumers' personal information. Merchants need to be aware of the risks electronic transactions carry, and work towards securing the systems to the highest standards.

3



### Government

The Nigerian government has recently automated most of its critical processes including tax applications, filing returns and through the central bank it has adopted the BVN and cashless policies. While this has increased its service delivery and efficiency, this same digitization and transition

4

has exposed the government and especially ordinary citizens to more attacks. The lack of awareness on the part of the end user, privacy concerns, unreliable distribution and delivery process and lack of properly secured infrastructures has led to the increase in cyber-crime activities through these established channels. Attacks such as online scams, Identity theft and credit card fraud are on the rise as a result.



## Mobile Money

Mobile money is one of the most embraced technology platform in Nigeria and Africa as a whole. Mobile money is 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 malwares 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.



## Other Financial Services

Sacco's, Cooperatives and microfinance institutions are rapidly gaining popularity not only in Nigeria but throughout Africa. This is mainly due to their customer friendly rates and reduced ease to which one is granted access to their facilities. While the main focus of these institutions is centered on increment of the customer base and satisfaction of their financial

needs, their information security concerns are not always prioritized. Most of these institutions do not focus on employee awareness and technical training and as such we are seeing a lot of employees falling victims to social engineering scams, email phishing attacks and online scams. Most of these organisations systems are often vulnerable with many reported cases of system misconfigurations, open ports and default passwords. Critical to the financial services is also the issue of insider threats. Like the banking sector, the rise of insider threats within financial services is high and has resulted in more than 50% of the attacks that have been reported.

It is therefore paramount that as these firms try to reduce their operating costs and increase efficiency, they should also invest in the relevant security requirements including employee training and awareness.



## Hospitality & Retail Sector

The hospitality industry is primarily client facing and as such deals with a great deal of sensitive customer information. Processes ranging from reservation details, payment, travel, personal information are now automated and we are seeing introduction of services such as digital conference facilities, smart room keys and mobile applications which enable the client to perform a wide range of otherwise manual processes. However, information security aspects tends to be neglected as most of the focus is on automation. This leads to a myriad of risks ranging from information theft, data breaches and credit card theft. Malware targeting these businesses are now being seen in POS (point-of-sale) terminals to steal credit card data and targeted attacks against hotel systems to steal confidential data. This has both financial and reputational impact on these organisations as customers quickly lose trust in them.



### Remi Afon

President of Cyber Security Experts Association of Nigeria (CSEAN)



#### Do you think Cyber security is a major problem in Nigeria?

Yes.

#### If yes, what do you think is the main cause of the Cyber security problem?

The low level of cyber security awareness and lack of adequate regulation to compel organizations to take cyber security seriously.

#### Do you think the private sector is investing enough in cyber security?

Apart from the banking sector, private organizations in Nigeria are not really investing in cyber security.

#### In your opinion what drives criminals to commit cybercrime?

Financial gains remain the primary motive of majority of cybercriminals followed by espionage.

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

Adequate infrastructure is not in place. We are still lagging behind in this area.

#### Do you personally know of a company or individual who's been affected by cybercrime?

I know of a lot of big organizations that have been attacked by cyber criminals but have kept quiet about it to avoid reputational damage.

#### Were these cases reported to government authorities and prosecuted?

They were not reported due to reason mentioned above. There is need to compel organizations to report cybercrime, it will surely help in tackling the crime.

#### What do you think would be the best approach to address the cybercrime issue in Nigeria?

Strengthen the cybercrime law and equip the law enforcement agencies with the relevant skills and cyber security tools to apprehend and prosecute cyber criminals.

#### From an African context, what would be the top priority to address cybercrime across the continent?

Top priority should be cross-border collaboration.

#### What do you think is the estimated cost of cybercrime to the Nigeria economy?

It has been estimated that Nigeria loses N127billion to cybercrime every year.



### Dr. Krishnan Ranganath

Vice President - Century Group

## Achieving Cyber Security Resilience



### Do you think Cyber security is a major problem in Nigeria. If yes, what do you think is the main cause of the Cyber security problem?

Yes this is one of the major issues, we face here. The Nigerian Cyber Criminals operate in many ways and it is active across many countries. The gap between haves and have nots is a fundamental issue.

### Do you think the private sector is investing enough in cyber security?

I doubt, but on a minimal level they are investing. Examples are in the very preliminary levels of putting controls in local gate way level by using Cyberroam, or Cisco PIX.

### In your opinion what drives criminals to commit cybercrime?

Nobody is a born criminal. Situations are the root cause for a crime, this situation can be anything from need of money for regular need, need of money for a lavish life. The bottom line is the need for money.

### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?

Yes, the government has put regulations in place first from Telco regulator side also to monitor and control traffic at international gate way levels, filter contents and others. There is also a need to educate people on this, because many of this happens just because of lack of education.

### Do you personally know of a company or individual who's been affected by cybercrime? Were these cases reported to government authorities and prosecuted?

Yes, I myself got affected in India 2 years back. My debit cards were cloned and used in Cambodia which I have never visited. The bank / local cybercrime department took it up however I lost more than \$1500 on that. This was through three attempts from two cards.

### What do you think would be the best approach to address the cybercrime issue in Nigeria?

Education & Awareness is the best approach. Once a common man is aware of this, he will be careful. In addition, at the enterprise level, organizing workshops / explaining case studies will be of help.. This has to be done in parallel with the 3-Dimensional way that is Government – Enterprise – Public education / awareness

### From an African context, what would be the top priority to address cybercrime across the continent?

Cybercrime is a global issue. Africa can have a conversation around continental response to Cybercrimes. Nigeria need to protect themselves and entities that are specific to it. In most of the developing nations it depends on the capacity of their cybercrime space and how good they are in providing other infrastructure for their citizens. Considering our infrastructure, it's better to assume that Africa will be behind in this regard. On the contrary, Africa will not be a priority target for international cyber criminals as there is less to steal. As the continent grows, this scenario will change. Local cybercrime is rising in countries like Nigeria. Nigerian cyber criminals will possibly operate globally and their victim countries may put pressure on Nigeria to get its acts together.



## Top ICT Trends Affecting Cybersecurity in Nigeria



### E-services

The use of E-services is growing in Nigeria. From online shopping, filling tax returns, cashless policy introduction and the use of Bank Verification Number (BVN). Most of the business processes are now automated and run over the internet. With transfer of most processes from the physical world to the cyber world, this opens up the country to a lot of attack vectors. Cases of online scams and identity theft are now on the rise. The low awareness levels in Nigeria also contributes to these e service platforms being one of the most targeted platforms in the country.



### BYOD

Research has shown that there is widespread BYOD acceptance in Nigeria. This is reflected by the 55.9% of respondents who were allowed BYOD within their organisations. However, it is worrying to note that security concerns around BYOD have not been considered a top priority for most organizations that have adopted it. Most organisations lack acceptable use policies and procedures, an internal device usage policy, a security policy and/or a BYOD policy to provide guidance on the use of these devices.



### Cloud – Based Solutions

SMEs, SACCOs and public services in Nigeria are now adopting Infrastructure or software as a Service (IaaS)/(SaaS) where users replace physical ICT environments and systems and use cloud hosted alternatives to remove complexities and reduce overall costs involved in the installation, maintenance and upgrading of complex ICT systems. Majority of these organizations have adopted cloud services such as Google apps, Microsoft office 365, Microsoft Azure, Amazon and Oracle cloud.

From a security perspective, this trend has given rise to two security issues; traditional security controls can no longer help protect local business critical systems. Also Nigerian companies are losing visibility of their security posture. It's therefore paramount that even with cloud adoption, businesses should review the Service Level Agreements and contracts with the cloud providers to ensure security of their data and systems.



### Outsourcing- Vendor Risk

From air conditioning vendors to IT suppliers, there is no telling where the next attack vector lies. Outsourced vendors are now described as the greatest risk to the security of most organizations in Nigeria. With the increased reports of data breaches involving third party vendors, it's unfortunate that the conveyance of trust does not always end well. Third-party management best practices and service-level agreements (SLA) are not prioritized in most local organisations. It is also evident that most organisations don't perform regular risk assessments on their potential vendors before contracting them.





## Industry Regulation

In 2015, the Cybercrimes Act was passed into law. This was to address the different cyber related crimes within the country. However, even with these measures, it's apparent that these laws alone cannot address the growing challenges of cyber security such as Cyber terrorism. There is need to improve the capacity of relevant ICT and cyberspace stakeholders for the training and support of cyber security officials and the sharing of cyber security best practice from across the globe.



## Automation and Technology Adoption Rates

There is an increase in investment in technological infrastructure and the growth of internet connectivity across the continent. As the number of mobile users increase, the number of services offered on this platform have increased too. Consequently, this drift has created new security vulnerabilities that directly impact the users.



## IoT

The Internet of Things (IoT) or Internet-connected devices are growing at an exponential rate and so are related threats. Due to the insecure implementation and configuration, these Internet-connected embedded devices, including CCTVs and nanny cams, Smart TVs, DVRs, Smart routers and printers, are routinely being hacked and used as weapons in cyber-attacks.



## Terrorism & Radicalization, Cyber-activism

There is an increase in the number of terrorists and activists using the internet to spread their agenda, recruit new members and attack their targets. We have seen Boko Haram and other terrorist organisations move to the internet.



## Cyber Insurance

Several insurance companies in Nigeria are now offering cyber insurance covers for liabilities as a result of cyber-attacks. These companies also cover processes related to investigations, remediation and regulatory fines during the period. We expect this trend to continue, especially with the rise in cybercrime.



## Poverty Rates-Unemployment Rates

The high rate of unemployment in Nigeria has contributed greatly to the cybercrimes witnessed in 2016 within the region. The rate of poverty in the region has encouraged cases of rogue employees within organisations to find means to generate extra income, hence insider attacks.



### Collins Onuegbu

Executive Vice Chairman of Signal Alliance  
and Founder of Sasware Nigeria



#### Do you think Cyber security is a major problem in Nigeria?

Cyber Security is a global problem and will increasingly become a major problem as the world gets more connected.

#### If yes, what do you think is the main cause of the Cyber security problem?

The internet is a relatively new phenomenon. It offers both good and bad opportunities. Unfortunately, there are vengeful people and governments that have converted the internet into a place for war and crime. Looking into the future, new wars will be fought in the cyber world. Crime is moving online because it's more remote and more effective than the good old physical crime we have had for generations.

#### Do you think the private sector is investing enough in cyber security?

Is the private sector investing? Of course. Are they investing enough? No one can really say. Cyber security is a national problem and should be seen as such. Fighting it involves action by both the private and public sector and need legislation. Our law has to recognize this as a crime and define enforcement for it. The nation has to invest to defend itself against an attack from friendly and hostile countries. Unfortunately, Nigeria is not known for building modern infrastructure. So like our roads and airports and every other thing, I can guess that our national cyber defense is poor.

#### In your opinion what drives criminals to commit cybercrime?

What drives a criminals generally? I guess its human nature for some to be good and some to be bad. Criminals work to dispossess people what they have worked hard to acquire. For most of human history, this has been done offline. It's only recently they discovered that online theft can be done more effectively than offline theft. Therefore, it's natural for a new class of criminals to evolve and use the internet and cyberspace as their operating medium.

#### Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security?

Cybercrime is a national issue just like offline crime. While people build walls and gates to protect from thieves, government sets up the police, judicial system to try those who are caught stealing? In the same way, while companies and individuals will do the best to protect themselves from hackers and cyber criminals, government has to reform our police system, the judicial system to combat cybercrimes.

#### Do you personally know of a company or individual who's been affected by cybercrime?

Of course all of us. As simple as the computer virus is, that's the beginning of cyber-attacks. All of us have had one virus or spam attack at some point. These viruses have gotten more complex and have morphed into software than can steal passwords and steal money from your accounts and steal valuable company data. The explosion of social media means that stealing passwords in certain sites could create

such embarrassment that people have committed suicide on exposure. So cyber criminality comes in various forms. Locally, there have been attacks on government websites. Banks have lost money to cyber criminals however most of these go unreported.

**Were these cases reported to government authorities and prosecuted?**

I believe the authorities are aware of some of the crime in the financial industry and banks announce how much they have lost to fraud every year. It is a matter of checking the percentage of that loss that is electronic and cyber fraud. Of concern, however is that the capacity of government to fight this crime is hampered by our poor legal and police system.

**What do you think would be the best approach to address the cybercrime issue in Nigeria?**

We need to have the right legislative environment to allow police and the courts bring criminals to justice whether in cyber or physical world. At the moment we are struggling with basic policing when criminals are moving online. We need to have cyber commands in our police and military to first understand the threat and then prepare to fight it.

**From an African context, what would be the top priority to address cybercrime across the continent?**

Cybercrime is a sovereignty problem. While Africa can have a conversation around continental response to cybercrimes, I believe nations need to protect themselves and entities that exist in those countries. Like most things that concern development, countries' capacity to police their cyber space will be related to how good they are in providing other infrastructure for their citizens. It's safe to assume

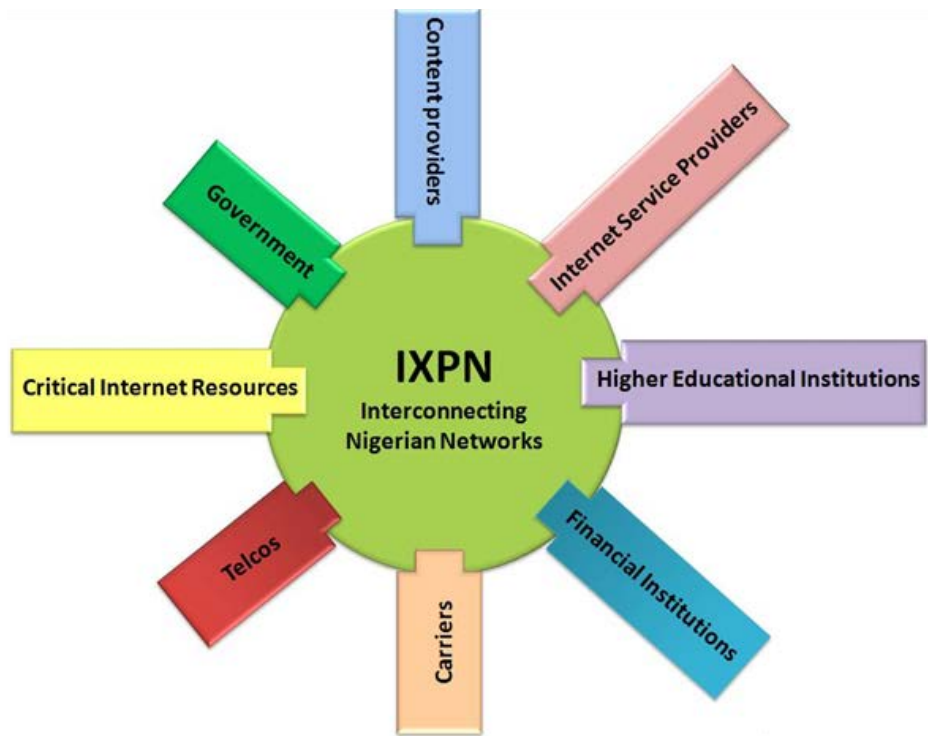
that Africa will lag in this regard. The flipside is that Africa will not be a priority target for international cyber criminals as there is less to steal however this will change as the continent grows. Local cyber criminality is rising in countries like Nigeria. In Nigeria's case, Nigerian cyber criminals will possibly operate globally and their victim countries may put pressure on Nigeria to get its acts together.

**What do you think is the estimated cost of cybercrime to the Nigeria economy?**

I am not sure anyone has reliable data. It could just be an irritation or we could be losing billions. I know for sure that the banking system has lost money to cyber fraud. They have reacted by beefing up their spending on security. The most vulnerable is government as most of our government employees still use insecure email platforms. How much sensitive information in Nigeria was exposed by that hacking incident is not known and the fact that our government does not have a safe mail system for government communication shows how unprepared we are as we move online. In the event that the government loses data through cyber fraud, it may not even be aware of the associated costs.



## Internet eXchange Point of Nigeria (IXPN) “Where Networks Meet”



*Is your organisation part of the above categories?*

*Then get connected to IXPN and enjoy the following benefits:*

- Cheaper Internet Bandwidth.
- Peer with leading Service Providers and Content Providers in Africa.
- Faster access to locally hosted content.
- Access to DNS Root servers for Many ccTLDs and gTLDs.



### **Bolanle Omotosho**

CEO, Digital Assure Ltd. He is also Cybersecurity and Cybercrime Specialist and Consultant to many banks in Nigeria

## Achieving Cyber Security Resilience



### **Do you think Cyber security is a major problem in Nigeria?**

Yes, it is a major challenge in Nigeria and for the users of Computers and electronic channels in Nigeria.

### **If yes, what do you think is the main cause of the Cyber security problem?**

As the various sectors of the economy move towards cashless transactions, so have the criminals too. This is simply because cyber thefts are silent, fast, highly yielding, and with little or no cost because the cybercriminals do share information about successful attacks for others to try out on unsuspecting organizations.

A major problem in Nigeria and the world exists simply because the Cybercriminals are always researching and developing new attack vectors in order to get high yields and cheap success, whereas the computer users and organizations are not developing their personnel to bridge the knowledge gaps. It is a moving goal post, it is not a static situation.

About 95% of attack techniques now rely on the human being to unleash the attacks which means that without human intervention or action, the attacks would not be successful, according to SANS Institute, 93% of all the successful attacks are due to human errors, errors could be intentional or unintentional due to ignorance.

Almost all Organizations pay more attention to training and developing their technical personnel and IT Security Professionals, leaving out the workforce who are more prone to errors and have become easy targets to the cybercriminals.

It may interest you to note that they no longer attack the security technical control tools such as the firewall, IDS, IPS, ACL, UTM, USM, etc, the cybercriminals attack and target the ignorant users now to succeed. It is a problem because the typical non-technical computer users, who are more in number, are not up to date on the latest techniques of the cybercriminals.

### **Do you think the private sector is investing enough in cyber security?**

Yes, they are trying. However, most of the time they are not investing well. They invest in all kinds of choke points and endpoint security solutions but they are neglecting the weakest link in the information security chain, which is the insiders, the human beings. The users have both physical and logical access and are trained to use the information resources of the company. The users have privileged accounts to execute complex and highly privileged transactions within the firm and a matter of concern arises when a typical criminal hijacks or spoofs the legitimate profiles of the privileged users. This happens regularly and that is why the users have to be turned into human firewalls so that if the technical control misses anything, the human beings will stop some.

### **According to Reuters, consistent information security awareness reduces cyber-attacks by up to 40% -65%. I believe this is huge!**

Information security awareness is a continuous process, not a one stop action. The organization should also invest in proactive detective solution that can predict an attack in the making and stop same even before it is executed.

### **In your opinion what drives criminals to commit cybercrime?**

Cybercriminals are everywhere and are getting sophisticated by the day. In the past, the main motivation was just truancy or youthful exuberance. However these days criminals are motivated by the pecuniary gains, fame, success, industrial espionage, and self-esteem. Cybercrimes continue to grow everyday and has become an industry on its own.

### **Do you think the government has put in place processes and infrastructure to support the private sector in combating cyber security issues?**

To a large extent, the Nigerian government is putting concerted efforts in place to secure the cyberspace however more investment is needed in this regard. There is a need to engage the professionals to constantly review the laws and methodologies to protect the information assets and the environment. The government needs to invest more in preventative and detective solutions, especially to empower the Law Enforcement Agencies to do their work better. Prevention and Investigation are very key to check a crime trend. Many cases will never be properly prosecuted simply because our LEA don't have what it takes to thoroughly investigate or set technical traps for the criminals. Effective and timely prosecution of cybercrimes have a way of sending positive signals to the criminals to vacate the Country.

### **Do you personally know of a company or individual whos been affected by cyber crime?**

Very many.I won't be able to mention the names for business confidentiality reasons.I will mention the CBN incident since it is a public knowledge already in the public domain. On March 16, 2016, our CBN lost about \$441,000 to the cybercriminals, although about \$190,000 was recovered from Dubai.

Based on our corporate services and my professional calling, we receive calls and invitation to assist organizations daily. In summary, no single organization is safe.

### **Were these cases reported to government authorities and prosecuted?**

Most organizations don't like to report these crimes to prevent reputational losses. They manage the situation internally by way of privately investigating to uncover all attributes of the system compromise, and they can deal with the culprits internally without causing further damage.

### **What do you think would be the best approach to address the cybercrime issue in Nigeria?**

- Regular Compromise Assessment
- Deployment of Proactive And Intelligent Technical solution
- Consistent Awareness for the users
- Empowerment of the Law Enforcement Agencies and the judiciary to aid effective prosecution and justice dispensation system.

### **From an African context, what would be the top priority to address cybercrime across the continent?**

The governments should come together to make life difficult for the criminals to save the proceeds from cybercrimes. If nobody can open an account just anywhere and anyhow to save money, without properly stating what led to it and from where, then it will become difficult for the criminals to operate.The various arms of the governments responsible for fighting cybercrimes should be sharing information on criminals and attack vectors. Effective legislation should be in place to back all these up to achieve success.

### **What do you think is the estimated cost of cybercrime to the Nigeria economy?**

I don't have a specific figure for Nigeria due to lack of effective reporting of cybercrimes and statistics, but recently, precisely on 19 Jul 2016, the incumbent Minister of Communications, Barrister Adebayo Shittu said about N127 billion is lost annually to cybercrimes. Globally speaking, just in the first three months of 2016, \$209M was lost to the cybercriminals who specialized in unleashing ransomware.





## The Serianu Cybersecurity Framework

### Introduction

Cybercrime in the African continent particularly within the Small Medium Enterprises (SMEs) setting is a growing concern. SME's 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 organizations.

With the increasing business requirements of the 21st century businesses and the inadequate budget allocated to IT, it's become expensive for especially small and medium sized companies to adopt complex and or International cyber security frameworks. As such, cybercrime prevention is often neglected within the SME environment. This has resulted in a situation whereby SMEs are now one of the popular targets of cybercriminals. 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 SME's 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, provide assurance that business operations will resume in the appropriate time in case of an attack or disruption.

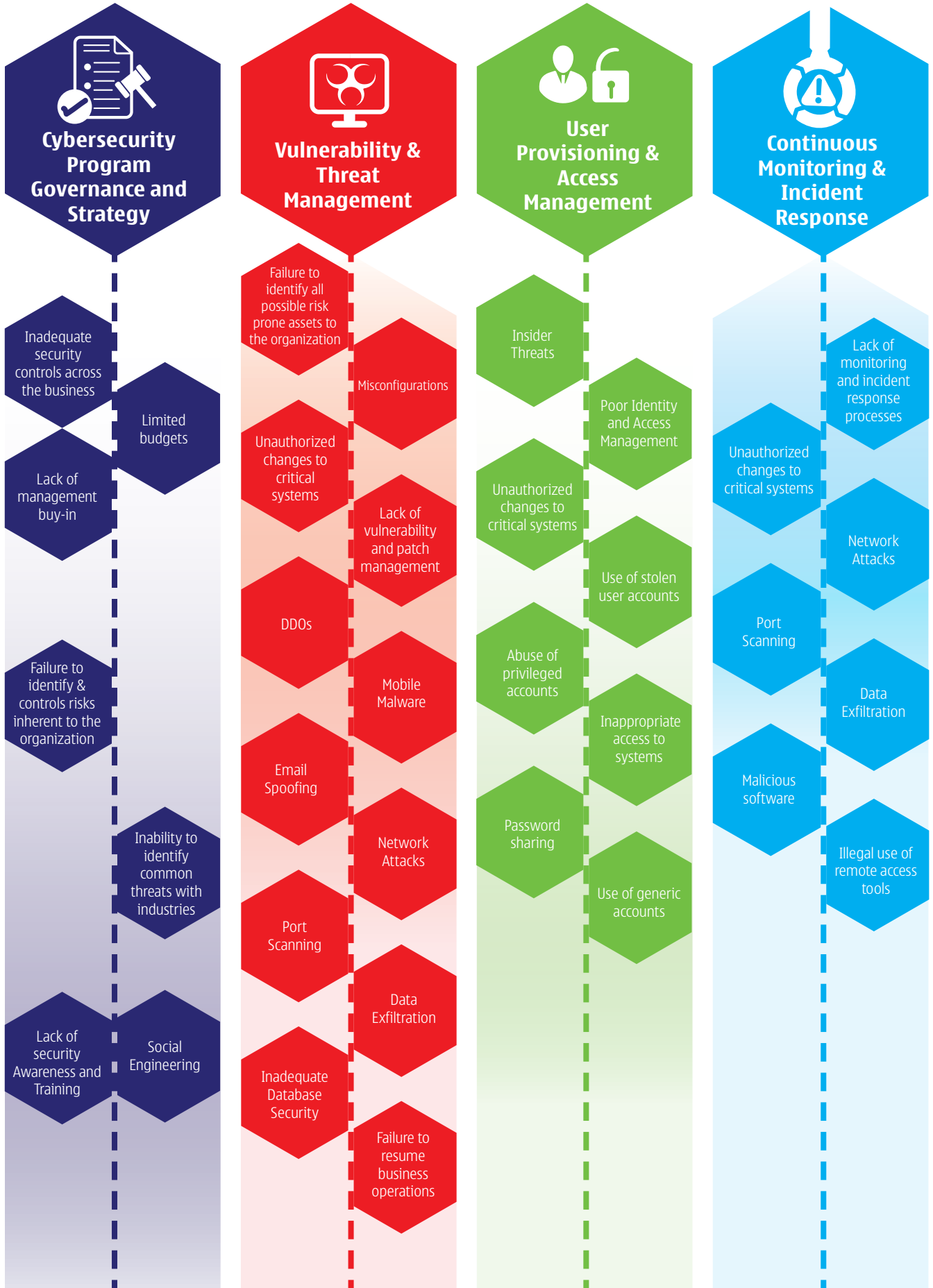
The framework is notably helpful also to small and medium-sized businesses seeking to implement global frameworks breaking down more complex categories and analysis into our four domains namely: **Cyber Security Program Governance and Strategy, Vulnerability and Threat Management, User Provisioning and Access management and Continuous Monitoring and Incident Response**. These domains simplify analysis and implementation of these global standards.

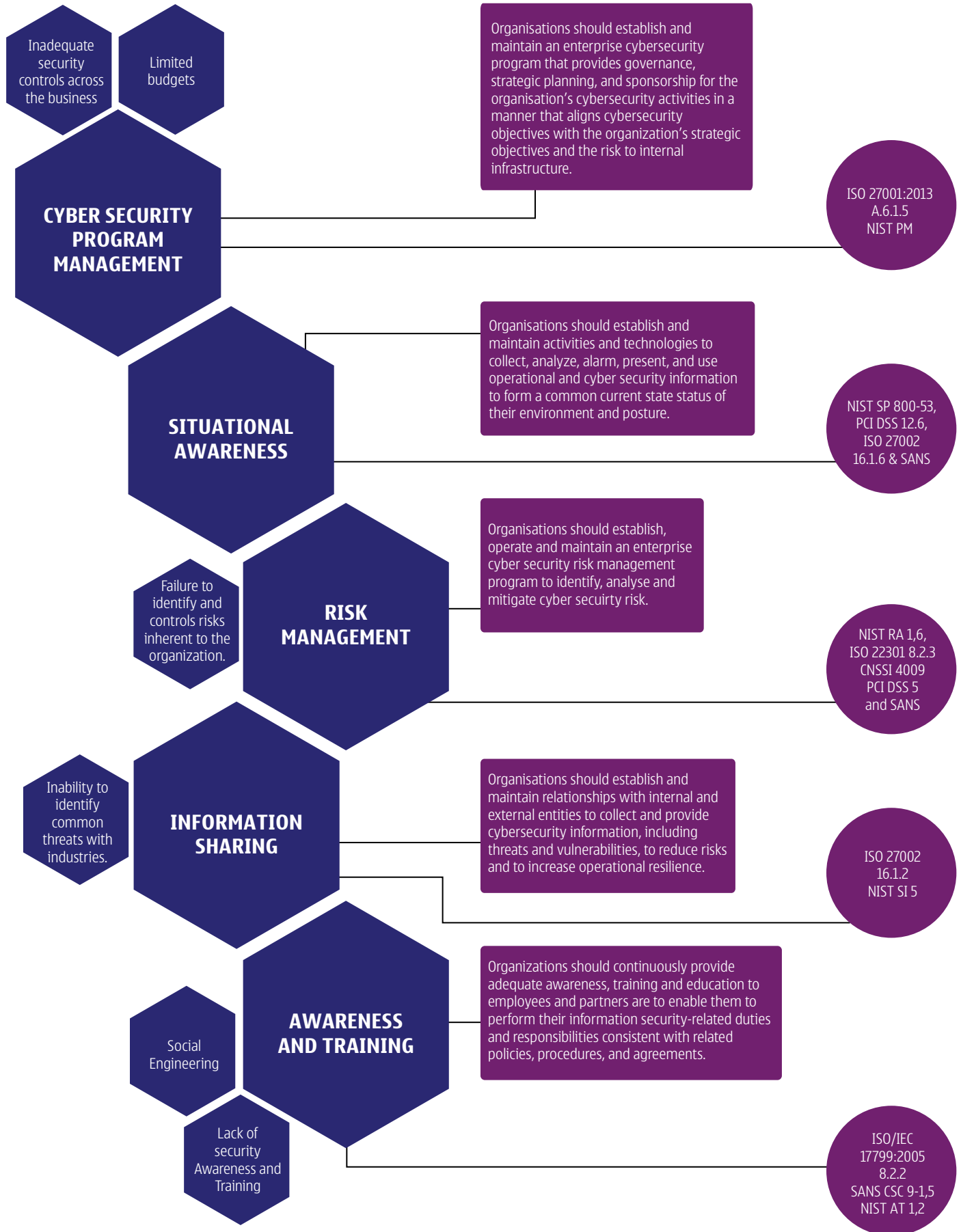
Serianu cyber security framework is not intended to replace other cyber security related activities, programs, processes or approaches that organizations operating in sub-Saharan Africa have implemented. As such it's important for organizations to understand that choosing to implement the framework solely means that the organization wishes to take advantage of the benefits that the Serianu cyber security framework offers.

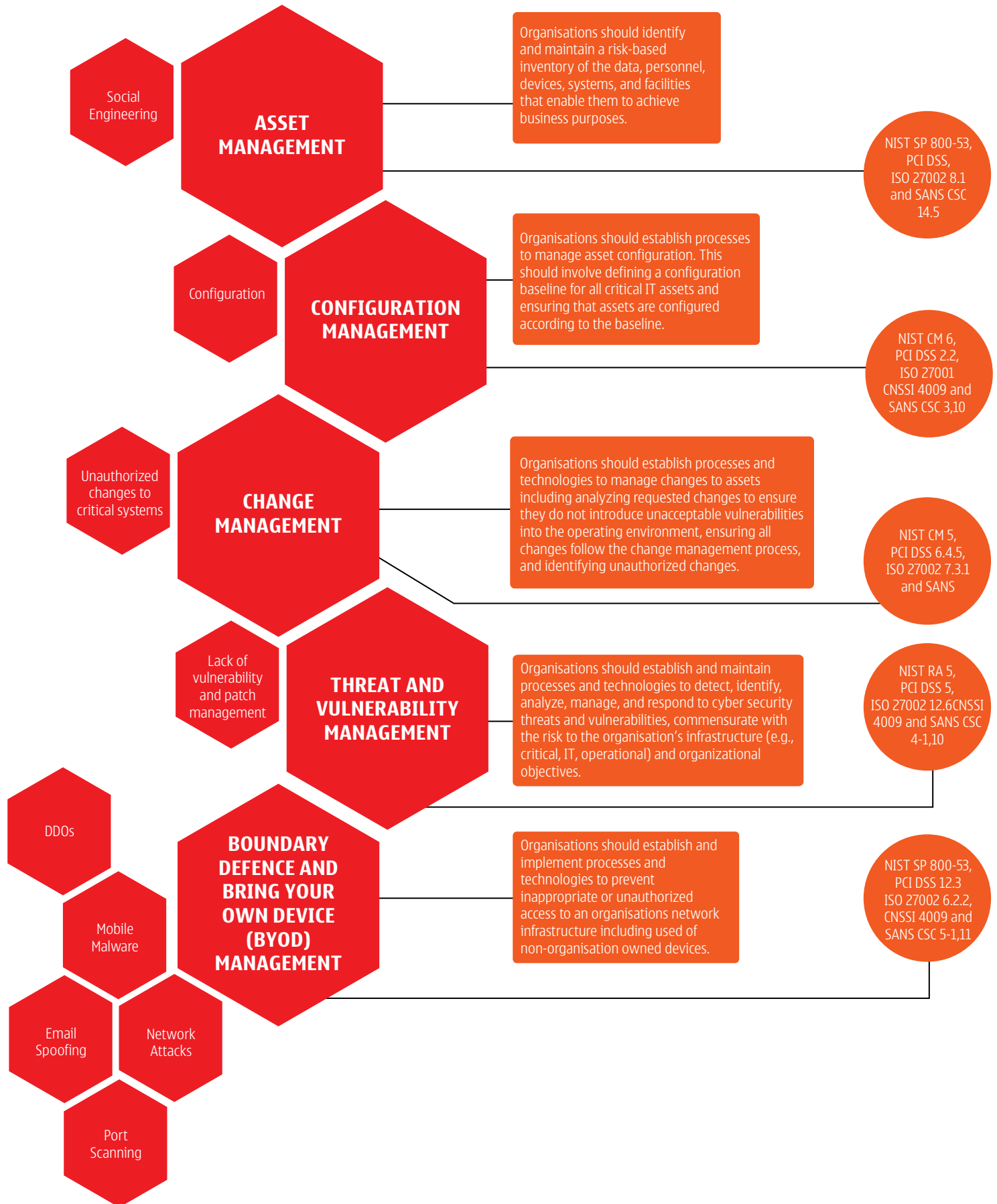
### Our Framework

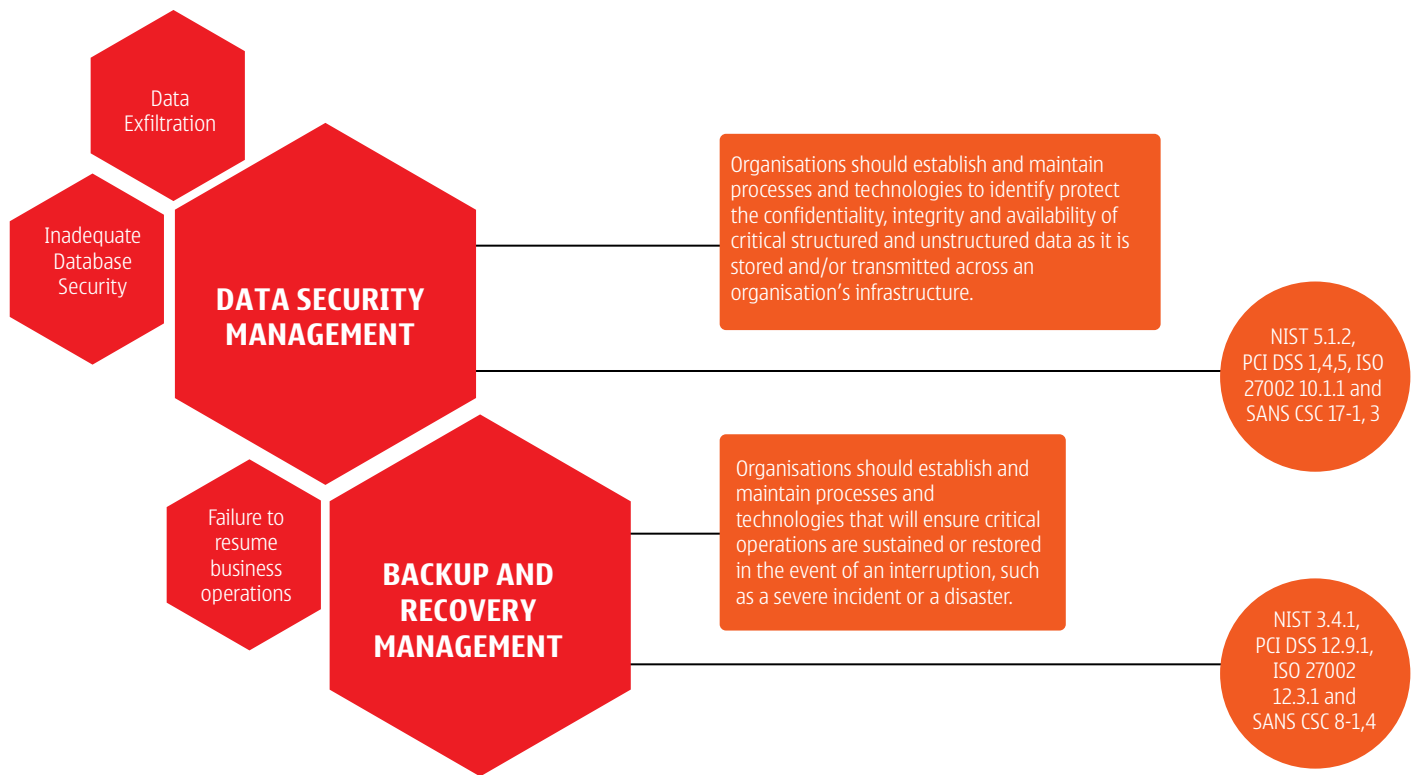
The Serianu Cyber security framework is detailed in the booklet provided separately.

## CATEGORIES







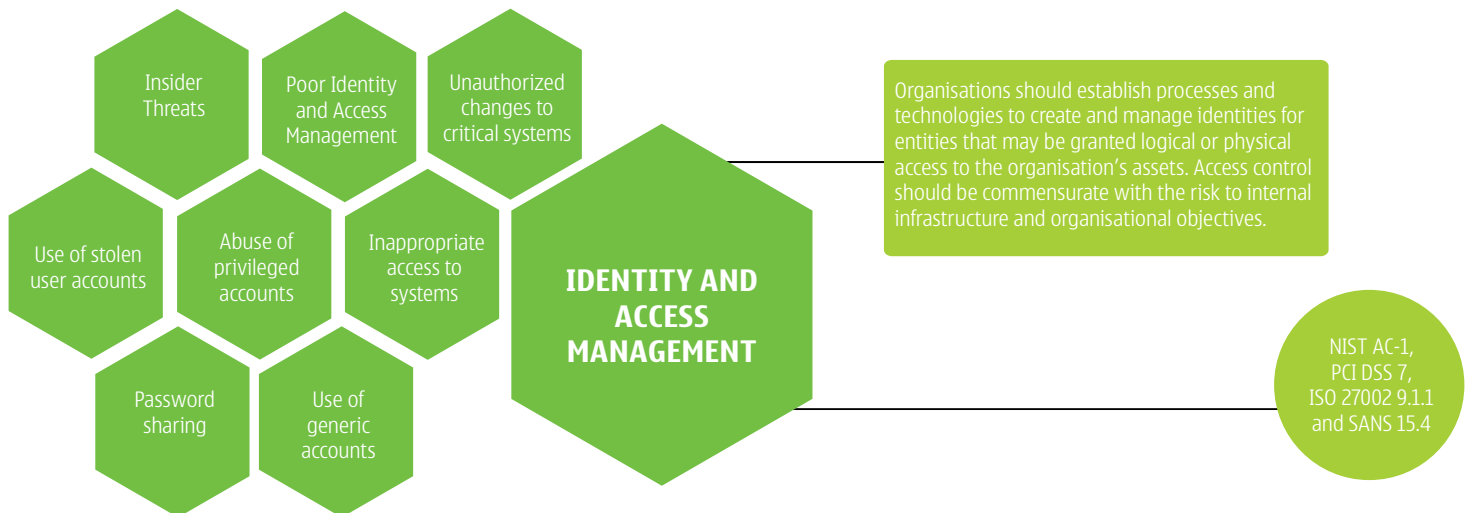


## User Provisioning & Access Management

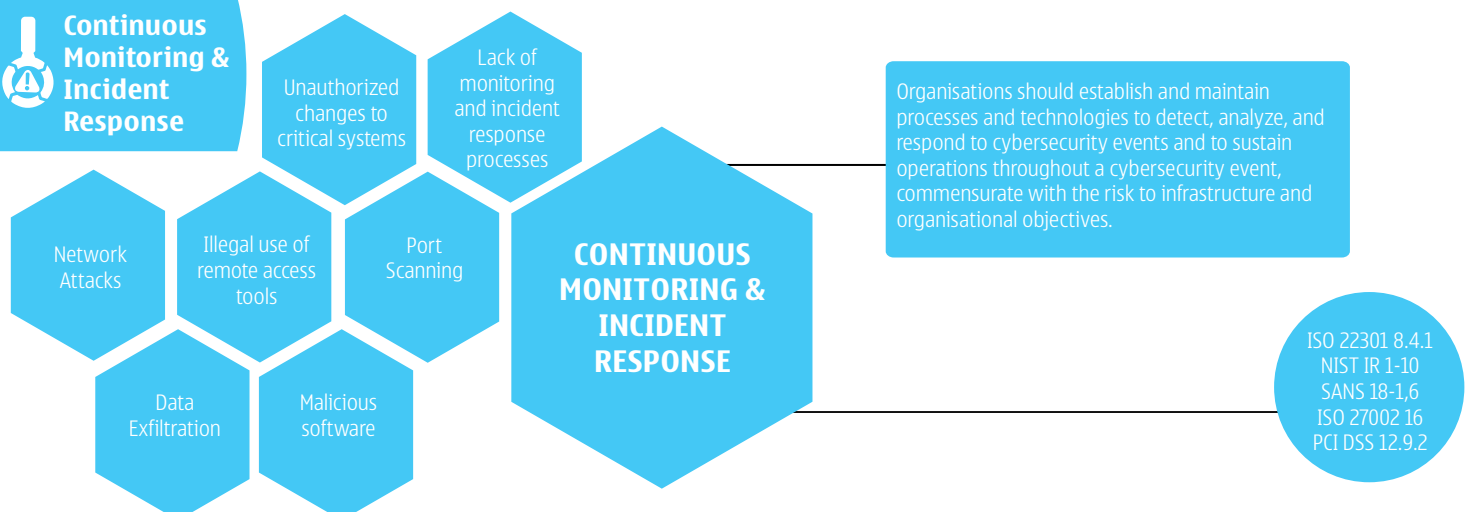
## CONTROLS

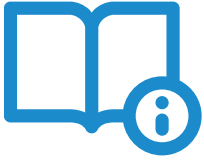
## Definitions

## Global Frameworks Reference



## Continuous Monitoring & Incident Response





## References

<https://www.today.ng/business/144562/bank-fraud-increase-15-71-percent-ndic>

<http://www.nigeriacommunicationsweek.com.ng/telecom/ncc-to-establish-computer-security-response-teams-for-telecoms>

<https://www.cert.gov.ng/news-events/details/104>

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

[https://cert.gov.ng/images/uploads/NATIONAL\\_CYBESECURITY\\_STRATEGY.pdf](https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf)

## Government

Vanguard (2013) Nigeria edges closer to strict legislation on cyber security, ICT vandalism. Available online at

<http://www.vanguardngr.com/2013/09/nigeria-edges-closer-to-strict-legislation-on-cyber-security-ict-vandalism/>.

## Top ICT Trends Affecting Cybersecurity in Africa

<http://rachelbotsman.com/work/mobile-money-the-african-lesson-we-can-learn/>

<http://www.mckinsey.com/industries/financial-services/our-insights/sub-saharan-africa-a-major-potential-revenue-opportunity-for-digital-payments>

## Cyber Security Risk Ranking by Sector across Africa

<http://www.cybercrimelaw.net/Cybercrimelaws.html>

## Summarized Findings Report

<http://www.cyberroad-project.eu>

## Regional IP Attackers Analysis (AccelOps)

<https://www.projecthoneypot.org/>





## 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 I, Lagos.

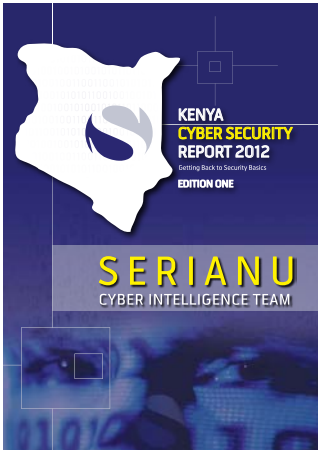
01-3426493, 08033013614; [eppan@e-ppan.org](mailto:eppan@e-ppan.org), [info@e-ppan.org](mailto:info@e-ppan.org)

 @eProviders  Electronic Payment Providers Association of Nigeria





2012



2013 — 2014



2015



Hon  
 virus  
 Risk  
 COBIT  
 DMZ  
 Firewall  
 Phishing  
 Outsourcing  
 attack  
 infection  
 Risk  
 warfare  
 websites  
 router  
 Cyber  
 Financial fraud  
 child  
 Regulations  
 Csoc  
 cyberspace  
 computers  
 social engineering  
 intrusion prevention system  
 organised  
 spam  
 Business disruption  
 Insider/disgruntled employee  
 defense  
 pornography  
 DMZ  
 access  
 port  
 Botnet  
 Audit  
 spam  
 two-factor  
 IS  
 Enterprise  
 Intrusion  
 Prevention