SERIANU

AFRICA
CYBER SECURITY REPORT
2016

SERIANU

Achieving Cyber Security Resilience:

Enhancing Visibility and Increasing Awareness

United States International University-Africa

DEMADIUR

kabolik

www.paladion.net

PALADION
BETTER SECURITY OUTCOMES

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

For further details contact us at sales@paladion.net

Achieving Cyber Security Resilience

Contents

About the Report

The Africa Cyber Security Report 2016 was researched, analysed, compiled and published by the Serianu Cyber Threat Intelligence Team in partnership with 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 Africa 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 continent. 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 Africa.

Partnerships through the Serianu CyberThreat Command Centre (SC3) Initiative are warmly welcomed in an effort to improve the state of cyber security 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**

Acknowledgement

Authors

Paula Musuva-Kigen
Martin Ekpeke
Emmanuel Inkoom
Beatrice Inkoom
Dadi Masesa
Brencil Kaimba
Kevin Kimani
Martin Mwangi
Barbara Munyendo
Faith Mueni
Daniel Ndegwa
Stephen Wanjuki
Nabihah Rishad
Samuel Keige
Jeff Karanja
Hilary Soita
Andrew Njuguna Ngari
Bryan Mutethia Nturibi
Denzel Ndegwa
Edward Owino
Gloria Gesicho
Ian Omondi Bwana
James Waiharo
Joylyn Chepkurui Kirui
Kenneth Mbae

Contributors

Kenya

Francis Wangusi

Director General, Communications Authority of Kenya

Paula Musuva-Kigen

Research Associate Director, Centre for Informatics Research and Innovation (CIRI), Digital Forensics and Cyber Crime Lecturer – United States International University (USIU)

Joseph Mathenge

CISO Airtel Africa

Brencil Kaimba

Risk & Compliance Consultant, Serianu Limited

Nigeria

Muhammed Rudman

CEO of Nigerian Internet Exchange

Onajite Regha

Chief Executive Officer, Electronic Payment Providers

Dr. Nwonyi Polycarp Emeka

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

Abdul-Hakeem Ajijola

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

Tanzania

Neemayani Sanare Kaduma

ISACA Tanzania Chapter President

Associate Director in Risk Assurance Services - Pwc

Peter Kisa Baziwe

Information System Audit and Security Professional

Ghana

Yvette Atekpe

Regional Managing Director, Internet Solutions Ghana

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

For more information contact:

Serianu Limited, Turnkey House
14 Chalbi Drive, Lavington, Kenya

Tel: +234 803 347 1283

Email: info@serianu.com

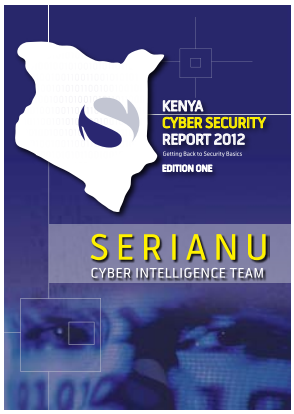
Website: www.serianu.com

William Makatiani

CEO, Serianu Ltd

Foreword

It is quite interesting how the meaning of a simple word like 'local' can change so fast in just four years.



In 2012, when we published the first ever **Serianu Cyber Security Report,** 'local' for us meant 'Kenya'. Back then, our focus was on understanding the state of cyber security in the country's industries and enabling our readers to make informed risk management decisions in an ever-changing cyber security environment.

Fast forward, four (4) years later and the same word now means 'Africa', with our report now covering multiple countries on the continent.

While its scope has expanded, its objective has remained the same – enabling our readers to make informed risk management decisions in an ever-changing cyber security environment.

The Africa Cyber Security Report 2016: Achieving Cyber Security Resilience; Enhancing visibility and increasing awareness summarizes our findings from our analysis of over 10million publicly accessible IP addresses and 40 million network security events.

This report focuses on four main countries – Kenya, Nigeria Ghana and Tanzania – representing East and West Africa, but also touches on a dozen other countries focusing on understanding how cyber security professionals in these countries deal with in-country specific challenges.

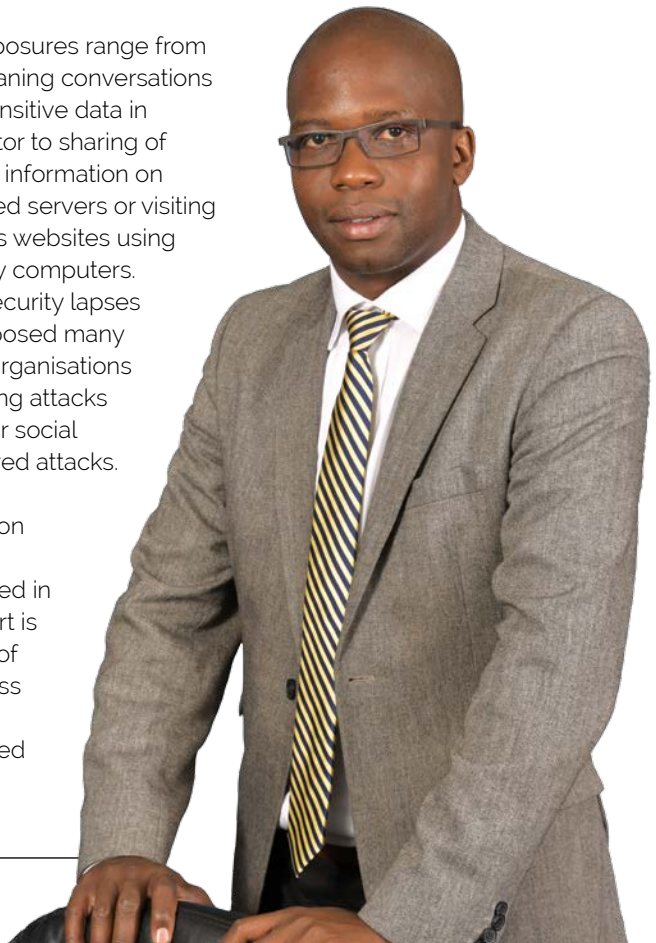
In future reports, we'll expand our scope to include more countries.

In just four (4) years since Serianu published its first cyber security report internet users across Africa has doubled from **167.3m people in 2012 to 448m as at June 2016**.

Many of these users – mostly customers and employees – have little knowledge of the level of risk they are exposing both themselves and the organisations they deal with online.

Such exposures range from well-meaning conversations about sensitive data in an elevator to sharing of sensitive information on unsecured servers or visiting malicious websites using company computers. These security lapses have exposed many African organisations to phishing attacks and other social engineered attacks.

A common theme highlighted in this report is the lack of awareness for users and limited



cyber security visibility for service providers. While there are high levels of investment in technologies and automation across governments and the private sector, the study found that there was no matching investment in cyber threat prevention tools. A majority of the organisations surveyed did not have clear visibility (ability to accurately and completely assess their posture) on the cyber security issues they needed to watch out for.

As more and more African governments and companies move to digitize their business process and connect to the internet, the potential of cyber-attacks has risen across the continent. **This requires more capacity on the part of these organisations to anticipate, detect, respond and contain (ADRC) such attacks.**

Unfortunately, a typical mid-sized business in Africa will have at least one or two systems exposed to the internet with little or no security to detect or prevent an attack. Such systems will have default passwords creating vulnerabilities that internal technology or ICT support are not aware of.

The Africa Cyber Security Report 2016 address these issues and focuses on raising cyber-threat visibility among African organisations and increasing awareness among employees and customers in ensuring they are well protected on and off the internet.

This study was made possible by the participation of our partners from research institutions, academia, businesses, legal enforcement agencies, Internet Service Providers (ISP), and professional bodies. We would like to thank all the professionals, organisations' and students who supported us in the development of this report. In the Africa Cyber security report 2016, we have summarized our research findings and provided country-by-country insights. The in-country sub-reports provides more detail on the state of cyber security in the four main countries.

Executive Summary

Technology has changed the business landscape in Africa dramatically. From strategic options to creation of new opportunities for innovation in products and services, technology is now incorporated in many if not all aspects of business. Internet usage has also seen a tremendous increase especially within the African region. However, as more businesses digitize their business processes and move to the internet, the potential attack vectors for these organisations expand.

The main objective for this study and in essence this report was to understand the top threats, risks and levels of awareness currently in Africa. Previously, we have been focusing solely on Kenya, however this year we expanded our scope to include other African Countries. In order to provide a more accurate image of the continent, we took a regional approach and analysed countries from both East and West Africa. Our decision for choosing to undertake this sample-based study was based predominantly on the recognition that complete enumeration through census-based study would impose huge costs that are unsustainable.

Breakdown of key statistics for In-Scope countries:

	Population (2016 Est.)	GDP (2016)	Internet users & subscribers (2016)	Estimated Cost of cyber-crime (2016)	Estimated No. of Certified Professionals
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.

Our findings have influenced the adoption of the Africa Cyber Security Report 2016 theme - Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness.

Highlights of the Report

- Local cyber criminals are getting more sophisticated. In one particular case this year, **cyber criminals employed a very complex cyber-attack targeting 10 organisations in banking, insurance, utilities and government across 3 countries in Africa.** The attack which took place for more than 12 months – starting October 2015 – August 2016 relied on a number of weaknesses in the organisations' ICT infrastructure and processes. As per our investigation, the cyber heist led to an estimated loss of USD4 million while the targeted amount in the heist was approximately USD15 million. Some of the organisations, especially in the banking sector were able to stop the attacks before the entire target amount was taken out.

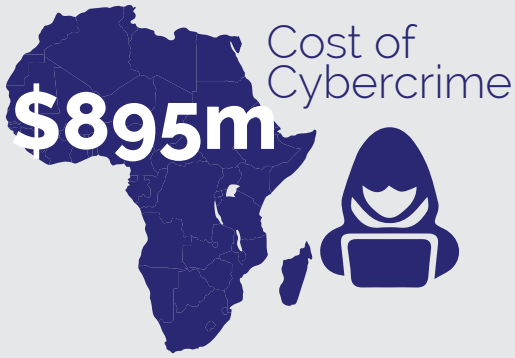
- **Business email scams led to losses amounting to USD 2 million in the African region in 2016.** Majority of these emails affected organisations that conduct international business and targeted financial managers who were instructed by their "CEO" to transfer money to foreign accounts.

- **The estimated cost of cyber-crime in Africa has soared with: Nigeria ($550 million), Kenya ($175 million), Tanzania ($85 million), Ghana ($50 million) and Uganda ($35 million).** This cost continues to grow as many organisations automate their processes. In some cases, like Kenya, the introduction of e-services by private and public sector has introduced new weaknesses that have allowed loss of money through these channels.

- **Ransomware (Locky and Zepto) has become a household name affecting thousands of organisations in the region and individual users.** Unfortunately, statistics still remain vague as organisations are reluctant to reveal the extent to which they have been targeted by it. Unlike other malware, ransomware directly targets financial profit by encrypting data on compromised devices and demanding payment often using bitcoins.

- **Insiders are a bigger security threat compared to outsiders for African Organisations.** Insider threats refer to fraud involving information or employee abuse of IT systems and information.

...at a glance



- **Local cyber criminals are getting more sophisticated.**
- **Business email scams led to losses amounting to USD 2 million in 2016.**
- **Estimated cost of cyber-crime in Africa has soared with: Nigeria ($550 million), Kenya ($175 million), Tanzania ($85 million), Ghana ($50 million) and Uganda ($35 million)**

- **Ransomware (Locky and Zepto) has affected thousands of organisations and individual users in the region.**
- **Insider threat is still the biggest security concern in organisations.**
- **Most organisations in Africa are ill prepared to deal with information security threats.**
- **Lack of practical regulatory guidance from industry regulators and government.**
- **Inadequate training and awareness amongst the law enforcement and judiciary fraternity.**

- Most organisations in Africa are ill prepared to deal with information security threats (Anticipate, Detect, Respond and Contain): This is brought about by **lack of sufficient budgets, lack of skilled professionals and lack of visibility within the organisation.**
- **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** is leading to poorly implemented and unenforceable security controls since they are not local focused and instead are copied and pasted regulations.
- **Inadequate training and awareness amongst the law enforcement and judiciary fraternity** make prosecution of these cases impossible.

Way Forward

Using the data from leading research firms and other sources we estimate that the ICT security expenditure in African countries will grow from approximately USD $1.24 billion in 2015 to USD $3.6 billion in 2020. Based on our research findings most African organisations are ill-equipped and unprepared 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 Africa, these initiatives cannot adequately address the current 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.

African countries need to focus on **four (4) key initiatives** to address information security challenges they face:

1 Harden Public and Private ICT Infrastructure and Services

African countries need to harden their infrastructure and services to enhance the resilience of the underlying foundation and combat information security threats.

2 Enhance ICT Security Competencies

African countries need to enhance the security competencies of technology users and ICT security practitioners. This will ensure that there is greater adoption of essential security practices among technology users and ensure that ICT security practitioners have adequate knowledge and capability in managing ICT security risks.

3 Cultivate Vibrant ICT Security Ecosystem

African countries need to develop local research on ICT security issues. Such research will enable the local organisations, universities and organisations to develop a vibrant ICT security ecosystem which will strengthen Africa's capability to protect their infrastructure and services. The research will also ensure the development of locally focused solutions.

4 Increase International Collaboration

Given the borderless nature of cyber threats, it is important for African countries to continue working closely with international counterparts and also encourage cross-border collaboration within the continent.

In conclusion

The challenges faced by African countries present great business opportunities for African entrepreneurs, researchers and vendors. For these countries to stay ahead of the threat curve, they 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. In their current state, they are unable to build these capabilities. African entrepreneurs need to step up, work together to build and provide information security services that enables these countries to address these challenges. African 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.

Africa 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 (African) cyber security threats, trends and insights concerning malware, spam and other potentially harmful business risks observed by the Serianu Cyberthreat Command Centre.

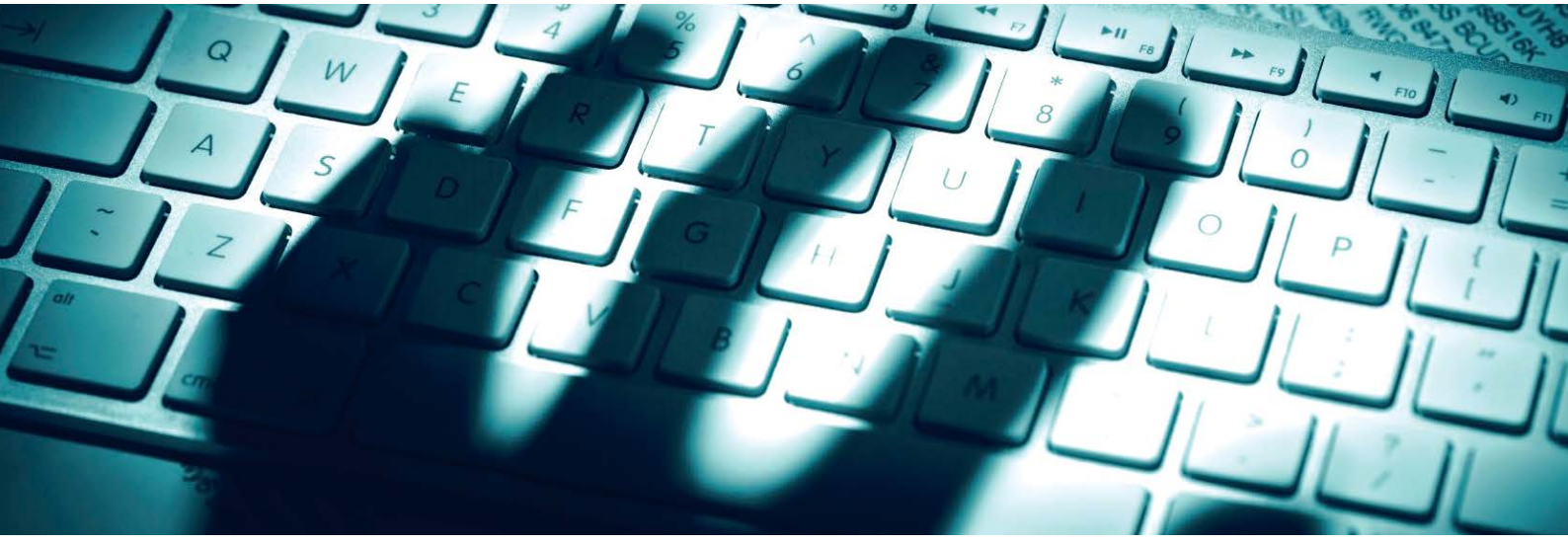
For the purposes of this report, we inspected network traffic inside a representative of African Organisations, reviewed contents of online network monitoring sites such as Project honeypot and reviewed information from several sensors deployed in Africa. The sensors perform the function of monitoring an organisation's network for malware, and cyber threat attacks such as brute-force attacks against the organisation's servers. In an effort to enrich the data we collected, we partnered with the Honeynet project and other global cyber intelligence partners to receive regular feeds on malicious activity within the continent.

External Cyber Threat Landscape

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

Project Honeypot Intelligence Analysis

This section covers data from the honeypot project, a global database of malicious IP addresses. We analysed data specific to the countries in scope of this report.



IP Statistics

Total Bad Events

***Bad Events**
These are all the malicious activities carried out over the internet. This may include spamming, DoS, Phishing, Spoofing etc

	Malicious IPs	Total	%
Kenya	196.200.31.178 41.203.214.239 212.22.183.162 41.206.60.146 41.215.143.126 41.220.120.108	103,134	55%
Uganda	41.190.143.182 196.0.42.18	75,593	40%
Tanzania	196.43.78.227 196.41.39.70	7,218	4%
Ghana	80.87.81.14	4,137	2%

Kenya reported the highest number of bad events with **55%** of all malicious traffic coming from the country

Top Spam Servers-Email

***Spam**
Electronic junk mail

***A spam server**
The computer used by a spammer in order to send messages

	Spam Server IPs	Total	%
Uganda	196.0.42.18 41.222.4.34	22,732	67%
Ghana	80.87.81.14	3,295	10%
Tanzania	196.43.78.227	2,959	9%
Kenya	41.215.127.10 41.215.75.82 41.215.36.114	2,353	7%
Nigeria	41.217.1.3 41.184.122.84	1,011	3%

67% of the top 10 spam servers used for spamming emails came from **Uganda**

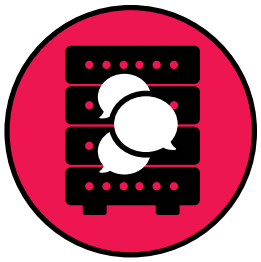
Dictionary Attackers

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

	Spam Server IPs	Total	%
Uganda	196.0.42.18 196.0.32.18	15,154	66%
Kenya	41.215.139.46 196.207.28.110 41.215.127.10 41.212.32.14	2,989	12%
Tanzania	196.43.78.227	2,347	10%
Ghana	41.204.60.22 80.87.81.14	2,340	10%

66% of the top 10 dictionary attackers came from **Uganda**

Top Comment Spammers



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

	Malicious IPs	Total	%
Uganda	196.0.42.18 196.0.32.18 41.222.4.34	38,755	67%
Tanzania	196.43.78.227 196.41.39.70 41.221.54.42	8,566	14%
Ghana	80.87.81.14 41.204.60.22	6,771	12%
Nigeria	41.222.208.33	2,069	4%
Kenya	41.215.127.10	1,765	3%

67% of the top 10 top comment spammers came from **Uganda.**

Total Harvester Yield

***Harvester**
A harvester is a computer program that surfs the internet looking for email addresses. Harvesting email addresses from the Internet is the primary way spammers build their lists.

Ghana

Nigeria

Malicious IPs	Total	%
212.96.7.234 80.87.92.52 41.218.224.247 41.218.238.119	7,194	69%
41.206.12.42 82.128.107.126 82.128.0.55 41.206.1.1 41.206.11.27 82.128.0.64	3,224	30%

Ghana reported **69%** of the top 10 harvesters.

External Public Infrastructure Vulnerability Assessment

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

Overall Ports Analysis - Africa

Top Open Ports

The following ports were identified as the top ports with running services open on the affected devices.

Port 80
22%

Port 443, 8080
11%

Port 3306, 3389
9%

Port 22, 23
8%

Port 21, 445, 139
7%

Regional IP Attackers Analysis (AccelOps)

Below are identified attacker IP addresses unique on telnet, RDP and VNC protocols.

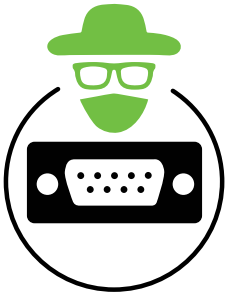
Telnet Attackers

IPs	%
93.174.93.50	**70%**
106.184.2.29	**16%**
61.240.144.64	**8%**
50.174.109.151	**4%**
61.151.214.71	**2%**

Remote Desktop Attackers

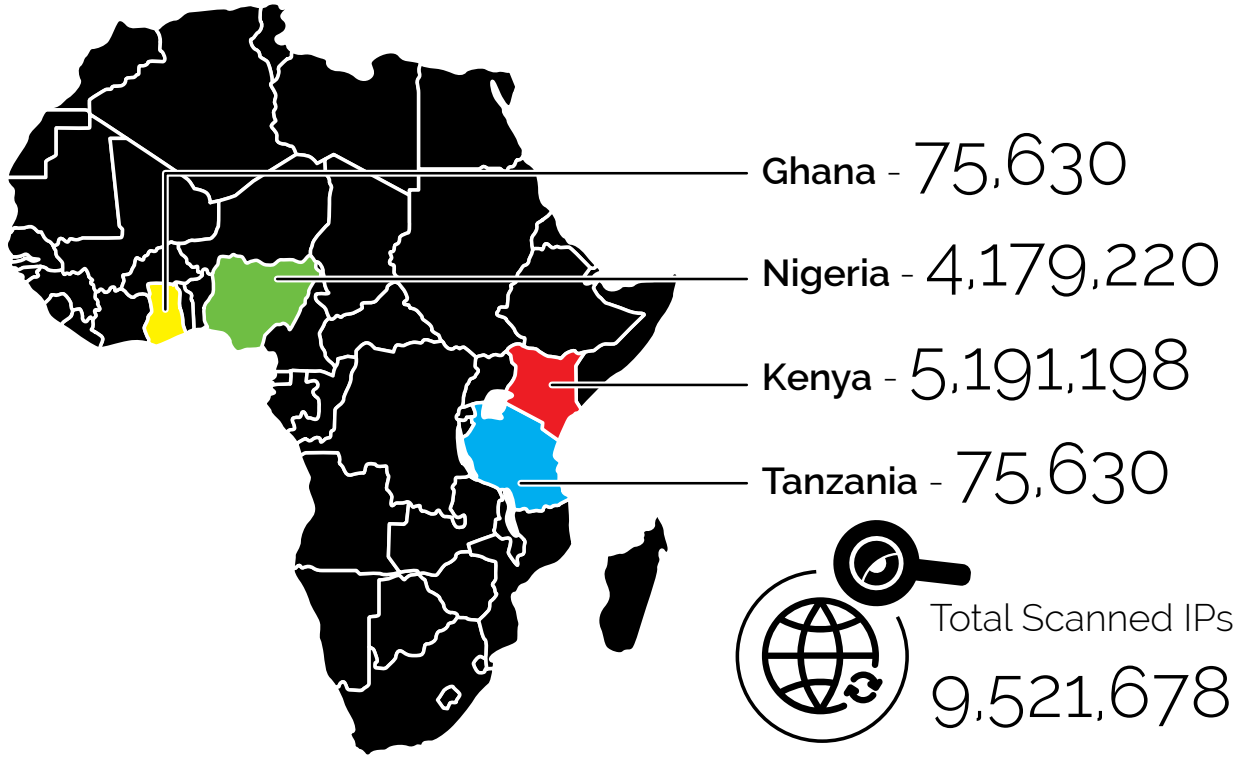
IPs	%
93.174.93.50	70%
106.184.2.29	16%
61.240.144.64	8%
50.174.109.151	4%
61.151.214.71	2%

VNC Attackers



IPs	%
61.240.144.64	50%
151.80.44.168	22%
80.82.65.61	16%
200.32.63.160	8%
80.48.104.217	4%

Africa Scanned IPs



Francis Wangusi

Director General, Communications Authority of Kenya

Do you think cyber security is a major problem in Kenya?

Yes

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

- Existing gaps in existing cyber security laws - policies, laws, regulations.
- Lack of awareness on information security matters.
- Shortage of information security experts in the country.
- Poor information security policies in organisations.
- Lack of adequate investments in information security.
- Lack of support from top-level management.

What can be done to improve the situational awareness in the country?

- Conduct aggressive awareness campaigns at all levels.
- Develop specialized information security courses in local universities and colleges and offer them at subsidized rates.
- Integrate information security in primary and secondary school curricula including music and drama festivals.
- Develop information security competitions for example hackathon.
- Enact and enforce cyber security laws.

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

Since the private sector is profit-oriented and information security investments cost a lot of money, there is tendency of the private sector to overlook matters related to cyber security only until an attack happens. However, this depends on the nature of the business. Sensitive businesses like banks tend to invest more in cyber security that other less sensitive businesses.

In your opinion, what drives criminals to commit cybercrime?

- Espionage.
- As a show of might or superiority.
- Cyber warfare.
- To commit financial fraud.
- To access confidential information to gain comparative advantage.
- For political reasons.
- Out of malice.

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

- Yes. Cybersecurity is a major global concern and a key item in the information agenda of many countries. Kenya takes cognizance of this and as a result facilitated the development of a national cybercrime management framework.
- This framework consists of the Kenya Information and Communications Technology Sector Policy of 2006, the Kenya Information and Communications Act of 1998 with its amendments and the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations of 2010, among other legal instruments.
- The enactment of the Kenya Information and Communications Act, 1998, as amended, mandates the Authority to:
    - Promote and facilitate the efficient management of Critical Internet Resources
    - Develop a framework to facilitating the investigation and prosecution of cybercrime offenses
    - To develop regulations with respect to enhancing cyber security

- Following the enactment of the Act, the Authority established the National Computer Incident Response Team Coordination Centre (National KE-CIRT/CC). The National KE-CIRT/CC offers technical advisories on cyber security matters to relevant stakeholders nationally and coordinates cyber incident response in collaboration with relevant actors locally, regionally and internationally. The National KE-CIRT/CC is also Kenya's National trusted point of contact for information security matters.

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

- Yes. There have been various cases of social media abuse, spam emails, ransomware, web applications attacks, and malware among others. These cases were reported to the National KE-CIRT/CC and appropriate and necessary action taken.
- Further, information sharing between the private and public sector is vital in addressing cybercrime.

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

- Cyber-crime is a complex yet relatively new phenomenon in the country. Cybercrime management must to be a consultative and concerted effort, involving all stakeholders – the public sector, private sector and the public at large. No single institution has the capacity to effectively deal with the challenges that are posed by cyber threats. Everybody has a stake in cybercrime management.

According to you, what is the most affected sector in the country regarding cybercrime?

- One of the most affected sectors in the economy is the financial sector. As at June 2016, the total number of mobile money transactions stood at 375.8 million with an equivalent of Ksh. 957.0 billion transacted. Furthermore, a total of 227.3 million mobile commerce transactions were made, which amounted to the cost of goods and services valued at Ksh. 404.1 billion. Person-to-person money transfers recorded in the period was valued at Ksh. 429.4 billion. It follows therefore, that cases of financial fraud have been on the rise and the financial sector is one of the most adversely affected.

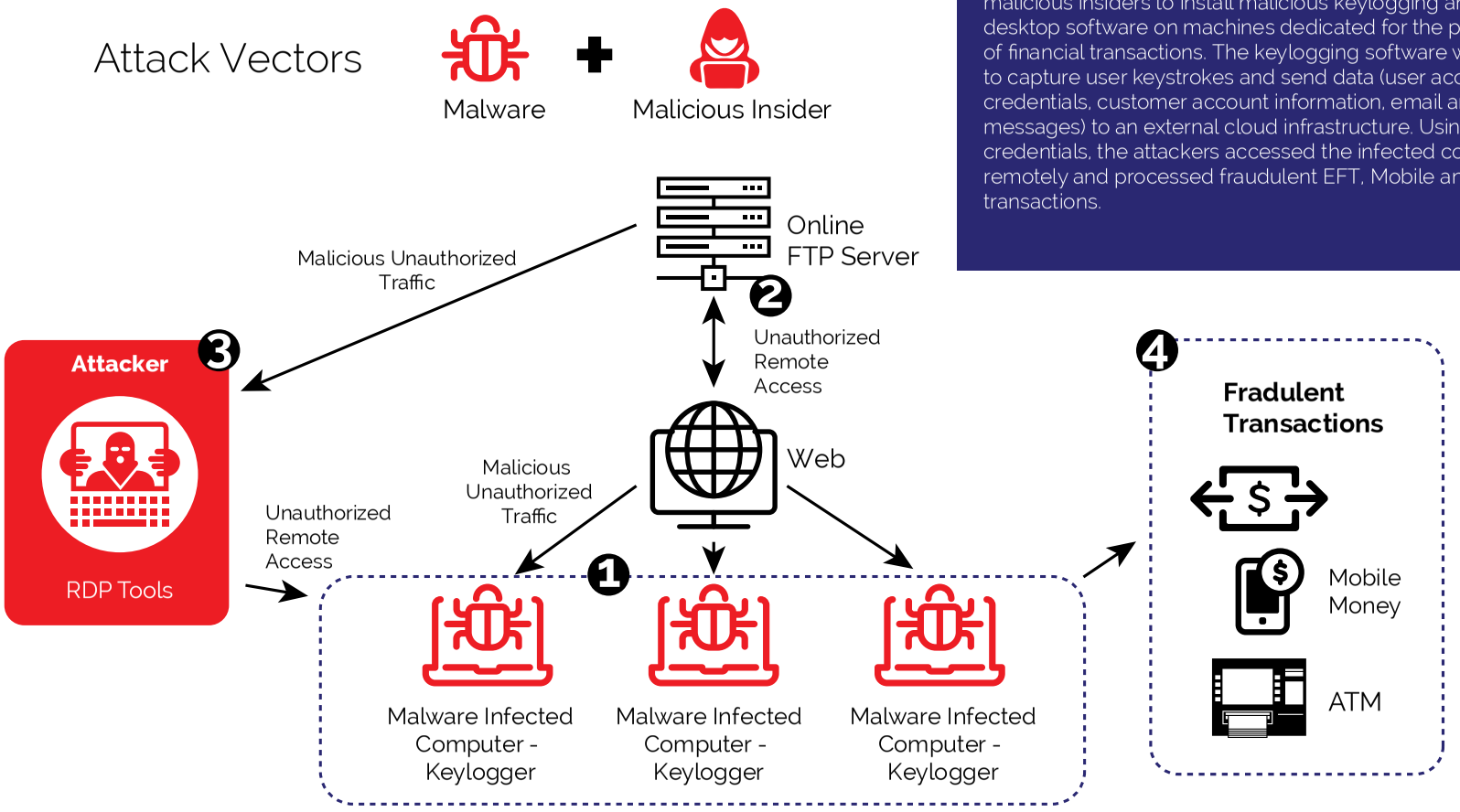
From an African context, what would be the top priority to address cybercrime across the continent?

- Legislative frameworks on cyber security – policies, laws, regulations
- Capacity building in cyber security
- Enhanced monitoring of national infrastructures
- Promote an information society as an enabler for sustainable development
- Awareness campaigns amongst all stakeholders
- Investment in research and development

.

Anatomy of an African Cyber Heist

In 2016, a number of institutions in African countries were targeted. In one particular case, the attack took place for more than 12 months – starting October 2015 – August 2016 and it relied on a number of weaknesses in the organisations' ICT infrastructure and processes. The hackers conspired with malicious insiders to install malicious keylogging and remote desktop software on machines dedicated for the processing of financial transactions. The keylogging software was used to capture user keystrokes and send data (user account credentials, customer account information, email and chat messages) to an external cloud infrastructure. Using these credentials, the attackers accessed the infected computers remotely and processed fraudulent EFT, Mobile and ATM transactions.



Victims

- Financial Services Organisations
- Banks
- Insurance
- Government Agencies

Malicious Insider

1. Infected PCs with malware (keylogger)
2. Malware logs keystrokes and screenshots and sends to the cloud account
3. Hacker retrieves and analyses keystrokes for user passwords
4. Attacker processes fraudulent transactions using acquired credentials

Internal Cyber Threat Landscape

The data provided in this section is based on our internal vulnerability assessment conducted in various countries and inspection of network traffic in 10 different organisations across Africa.

Throughout our analysis, we distinguished between several specific malware attack vectors employed against the representative African organisations. The three identified attack vectors included: **BYOD, Insider threats, and Phishing Scams.** By comparing observed cyber events inside the resident sample, we identified malicious threats in their infrastructure that current information security solutions or practices do not detect or prevent.

- We found that in all organisations, traditional antivirus software's can no longer match the new strains of malware targeting African organisations. Malware authors are now creating unique malware crafted for different targets in order to obstruct detection or prevention by malware vendors. Malware authors are also manipulating commonly used application software's and distributing the infected files through the trusted application owner's websites.

- Some of the top malware types identified during our analysis included: Botnets, Ransomware, Spyware, Trojans and Worms. Symptoms exhibited during the infection period included increased CPU usage and network latency, mass port scanning, file modifications, creation of unknown files, email spamming, FTP connections to cloud servers, connections to blacklisted IP addresses and multiple login failures or blocked/ dropped access requests.

- Common distribution channels included malicious files and links to malware hosting sites embedded in emails, social media sites, portable drives and BYOD devices.

- Peer to Peer (P2P) connections have also been widely used for communications between infected machines and botnets. P2P connections are hard to detect and block at the network level using traditional methods. Attackers have also weaponized torrent software which are well-known for their P2P file sharing capability, to deliver malware and enhance private communication capabilities with infected machines.

We identified the following trends:

- There are also new spawns of attackers that use little or no malware to breach an organisation's network. Remote Access Software used to remotely access or control a computer are now being used for malicious purposes without the knowledge of the victim. Remote desktop tools are being used by hackers to infiltrate the network. Tools like port scanners, are also used for network discovery and security auditing.

- Other methods used to evade traditional antivirus and achieve persistency include:

    - Use of fileless malware which hide in locations that are hard to scan.
    - Deployment of unsupported malware variants on windows platforms by installing portable interpreters of the required language e.g. Python, Perl or Ruby.
    - Use of malicious password protected documents to prevent scanning.

- Key loggers are also on the rise. Keyloggers are software programs designed to secretly monitor and log all keystrokes. They are embedded within Trojans to capture user keystrokes and later send this data to the attackers' command and control (CnC) servers. With these Trojans, attackers are able to collect a user's passwords, PIN codes, account numbers and other personal data. Unlike other forms of malware, key logging does not present any direct threat to the machine, just to its user.

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 organisations 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 organisation 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

2016 Africa Cyber Security Survey

The purpose of the 2016 Africa cyber security survey was to explore and identify the needs of African businesses and to find out what they see as the potential cyber security threats both now and in the future. As perceived threats may be different from real threats, it is important to try to correlate local organisation' experiences of cybercrime with the situations as reflected in the current report and analyses.

About the Survey

This survey was prepared based on data collected from over 700 (respondents) organisations in Africa. This included companies from the following sectors:

- **Academic**
- **Government**
- **Private Sector**
- **Banking**
- **Healthcare Services**
- **Professional Services**
- **Cyber Security**
- **Insurance**
- **Telecommunication**
- **Financial Services**
- **Legal Advisory**
- **Others**

The respondents who participated in this survey included technical personnel (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 African organisations and the security awareness and expectations of their employees.

Summary of findings

According to the survey findings, 99% of respondents have a general understanding of what cybercrime is.

01 **92% of organisations are concerned by Cybercrime**

92% are concerned

while 8% Not Concerned

02 **93% acknowledge that cybercrime is an issue affecting organizations**

while 7% Not Concerned

03 **CyberCrime is a problem rooted in technology says 36% of the organizations**

while 20% believe it's rooted in the society

04 **85% of respondents' research on information on cybercrime regularly.**

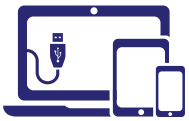
while 15% have no time allocated to this

05 **50% of respondents are not given training or get ad hoc training when an incident occurs**

28% are annually trained

22% not given training

06 **59% of organisations have adopted BYOD**

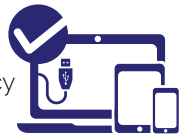


59% allow

41% dont allow

07 **Only 45% of the respondents have an internal device usage policy or BYOD policy**

45% Have a BYOD Policy



while 38% dont have

08 **50% of the respondents have experience cyber-crime either through work or at personal capacity**

50% have experienced work or at personal capacity

09 Over 50% of those who had been victims of cybercrime experienced negative impact

over **50%** experienced loss of money, down time, inconvenience, psychologically harmful and loss of reputation

10 97.7% of respondents either did not report cases of cyber-crime to the police or reported with no further actions taken

55.6% did not report cases of cybercrime to the police

11 96% of organizations spend less than $5,000 annually on Cyber security products

96% spend less than **$5000** on cyber security annually

12 83.4% of organisations manage cyber security internally or lack management systems in place

16.6% outsourced to either an ISP or Managed Services providers

while

83.4% manage cyber security internally or don't have any management system in place.

13 Over 62% of organisations don't base their policies on international standards such as PCI and ISO

over **62%** don't base their policies on International standards like ISO 27001, PCI DSS, NIST etc

while

38% have defined security frameworks based on these standards.

14 Majority of organisations have sensitive data in their Databases

26% Databases contain the most critical information

followed by Emails at **20%**

15 21% feel that more research needs to be conducted on the area of better laws and regulations

21% Better laws and regulations

17% Improve our understanding of society and the cyber community

16% Improved technology for our networks and operating systems

16% Better education of users of the Internet

15% Better encryption & improved privacy

Summary of Findings

- According to the survey findings, majority of respondents have a general understanding of what cybercrime is. **92.4% indicated that they are concerned with the issue of cybercrime.**
- **96% of African organisations spend less than $5000 on cyber security annually.** Monetary investments in cyber security products doesn't match up to the levels of concern registered earlier.
- More than half of the respondents **(54.9%) either don't have or don't know whether their organisations have a BYOD policy.**
- When it comes to management of cyber security, **83.4% either manage cyber security internally or don't have any management system in place.** 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 organisation and/or lack the necessary skill set to handle cyber incidents.
- Experiences of cybercrime within the African region are on the high with **61.7% stating that they have experienced cybercrime in one way or another.** Out of these, 60% was through work while 40% at a personal capacity.
- There are low levels of awareness within the African region, hence it is no surprise that when it comes to reporting of cybercrime to the police, **96.1% of cyber security incidents either go unreported or unsolved.** Only 3.9% of the reported cases were reported and followed through to a successful prosecution.
- **External infrastructure vulnerabilities** identified during the survey include non-business-critical services enabled, including **content management and remote administration, misconfigured SSL certificates and encryption settings.** With these vulnerabilities an unauthorized user gains access to critical systems
- The results of our Internal Traffic Analysis revealed that there are **numerous forms of Malware on systems, these include; Trojan Dridex and Zeus malware.** Most of these go undetected malware on systems.

Inter Country Analysis

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

	Kenya	Nigeria	Tanzania	Ghana
Organisations that Conduct Regular Training of Employees	58%	40%	48%	45%
Organisations that allow BYOD usage	62%	56%	61%	56%
Organisations that Lack BYOD Policies	49%	53%	59%	61%
People who have experienced cyber crime	71%	37%	20%	64%
Successful prosecutions per country	3%	7%	1%	9%
Organisation that have Zero (0) Budget allocation for cyber security products	6%	41%	42%	11%

Industry Analysis

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

	Banking, Financial Services & Insurance	Government	Telecommunication	Other Industries
People who have experienced Cyber Crime	59%	63%	67%	48%
Organisations with Cyber Security Budget of USD 0	33%	45%	30%	48%
Organisations with Cyber Security budget of USD 1-1,000 annually	44%	42%	46%	39%
Organisation with In-house Cyber Security Management	63%	58%	71%	40%
Security Certificate Holders	28%	39%	33%	28%
Number of organisations that conduct regular training of employees	39%	45%	55%	38%
Number of organisations that allow BYOD usage	20%	61%	49%	60%
Number of organisations that Lack BYOD Policies	30%	74%	56%	57%

Cause(s) and Effect(s) of Cyber Security in Africa

Summarized Findings Report – What are cybersecurity Gaps in Africa?

*Reporting approach adopted from cyberroad-project and survey

Theme	Scenario	Consequence (s)	Mitigation	Identified Gap(s)
Understanding of Cyber Crime	Perceptions are different on what is an act of cybercrime.	♦ No standard definition ♦ No collaboration between countries to fight cyber crime	Clear-cut definitions of cybercrime and cross-border co-operation to improve legal sanctions	How African companies can collaborate and share information on cybercrime issues
Monetary investments in cyber security solutions	Limited or no investments in Cybersecurity solutions	Organisations are losing money through cyber-crime.	♦ Cater for cyber security during annual budgets ♦ Proactive Investments in analysis, analysts and incidence response.	Metrics to determine minimum budgetary allocations for Cyber security for different industries.
BYOD	High BYOD usage with low rates of best practice policies	♦ Acceptable usage of company resources not defined ♦ High risks associated with such devices	♦ Define BYOD policies ♦ Compliance within the workplace. Effective measures in place	Policies and best practices for the workplace
Cyber Security Management	♦ In-house management of cyber security ♦ Cyber security roles combined with other IT roles	Individuals assigned cyber security roles in organisations are more often overloaded with other tasks within the organisation 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.
Information Security Certification & Technical Training	Few individuals with sufficient security technical training	Company employees lack basic information about information security foundation principles, best practices, important tools and latest technologies.	♦ More training on different Information Security standards ♦ Acquire information security certifications.	Training more information security professionals
Employee Training	Employee training done mainly after a cyber security incident	♦ Sharing information with unknown entities ♦ Poor internet practices ♦ Lack of preparedness after an incident	♦ Conduct regular people based risk assessment ♦ Develop an employee security awareness program	♦ Developing and running and effective security awareness programs.

Theme	Scenario	Consequence (s)	Mitigation	Identified Gap(s)
Reporting of Cyber Crimes	High number of cybercrime is not reported to police, and for those that are reported, very few are followed through to prosecution.	• Immature cyber security bills, laws and processes. • Lack of user awareness	• Adopt more mature processes for cybercrime prosecution. • Involve more sectors during development of cyber laws; Universities, local groups, organisations and cyber security specialists. • Raise awareness to citizens on reporting of Cyber crimes	• Escalation matrix for country wide cybercrime reporting.
External Threat Analysis	• Publicly accessible IP infrastructure has unnecessary services enabled, including content management and remote administration • Misconfigured SSL certificates and encryption settings.	• Unauthorized access to critical systems • High rise of wide spread attacks leveraging vulnerable infrastructure	• Monitoring the latest security vulnerabilities published • Updating the security configuration guideline	• Standard Configuration for systems • Continuous testing and monitoring
Internal Cyber Threat Analysis	• Use of obsolete systems and Apps • Use of clear text and insecure protocols • Server misconfiguration • Use of default credentials	• Unauthorized access to critical systems • Vulnerable systems	• Configuring all security mechanisms • Turning off all unused services • Setting up roles, permissions, and accounts, including disabling all default accounts or changing their passwords • Applying the latest security patches • Regular vulnerability scanning from both internal and external perspectives	• Password management and best practice • Patch management best practice • Emergency patch management practices
Internal Traffic Analysis	• Malware on systems • Botnets in private infrastructures	• Undetected malware on systems • Delayed incidence response	• Continuous monitoring Incidence response plan	• Managing 24X7 monitoring • Traffic monitoring and analysis

Yvette Atekpe

Regional Managing Director, Internet Solutions - Ghana

Do you think cyber security is a major problem in Kenya?

Yes.

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

Cybersecurity is certainly a major problem in Ghana, the main cause of which in my opinion is the high rate of unemployment among the youth.

What can be done to improve the situational awareness in the country?

In order to improve the situational awareness in the country, government and private sector must actively engage in threat sharing in order to avert possible crime, ensure heightened awareness and security compliance amongst network providers; publicly expose and appropriately sanction cyber criminals when caught to serve as a deterrent to the public.

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

Although some level of investment in cyber security has been made in a bid to combat cybercrime, I believe this has been inadequate as a result of the low awareness rate of threats to cyber security. Cyber fraud is increasingly being perpetuated on the blind side of individuals and institutions. This low awareness often creates an impression of the non-existence of the situation, and in most instances individuals and organisations are unwilling to expose the crime.

In your option, what drives criminals to commit cybercrime?

In my opinion, criminals are driven to commit cybercrime primarily out of greed and avarice and the perception of anonymity in cyberspace.

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

I believe the government of Ghana has put processes and infrastructure in place to support the private sector in combating cyber security issues most laudable amongst which are the establishment of the Cybercrime Unit of the Criminal Investigation Department of the Ghana Police Service and the Data Protection Commission.

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

I personally know a number of people who have been affected by cybercrime and reported the cases to the government authorities. Unfortunately most of the perpetuators were never found, but the few who were traced were prosecuted and are serving jail sentences.

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

The best approach to address the cybercrime issue in Ghana is to heighten public education in this regard, provide in-depth training and ICT tools to the law enforcement agencies and of course employment creation for the youth.

According to you, what is the most affected sector in the country regarding cybercrime?

The most affected sector in the country regarding cybercrime is the financial sector

Neemayani Sanare Kaduma

ISACA Tanzania Chapter President
Associate Director in Risk Assurance Services- Pwc

With the proliferation of systems, various apps and automated services such as mobile money, cybercrime is closer to home than it ever used to be. Talks around user accounts been hacked, corporate frauds propagated through information systems and tampering of e-money or cash losses in the mobile money space are becoming all too common. Much as these risks are known and in most cases managed, each entity does so in isolation and there is very little (if any) sharing of information including common incidents and cyberattacks that is done across entities and the country as a whole. It is therefore common to find someone who committed fraud in the cyberspace in one entity, getting employed within months in another entity. We need a mechanism that will facilitate sharing of information in order to have collective measures to deter these attacks and also reduce them from spreading. The passing of the Cybercrimes Act 2015 is one good step forward, however more needs to be done to create awareness in the society (user community) in general as this is still very low in Tanzania. As noted in the 2017 Global State of State of Information Security Survey conducted by PwC, a combination of good policies, sophisticated tools, skills and continuous awareness and training of people is what is needed to address and manage cybersecurity.

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

Given the increased level of automation and technology across industries particularly banks and telecoms, there is certainly an increase in cybersecurity related issues. Similarly, the increased penetration of internet usage and social media also attracts cybersecurity issues not only in an office setting but socially.

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

If we are to measure the investment made on preventive and detective tools and software companies have made against cybersecurity, I believe the amount will be significant. However, the question is, "is this spend on the right solution?" As mentioned above, to manage cybersecurity effectively, investments need to be made in user awareness and training of IT resources in addition to tools. Currently, most entities have invested more on the latter.

In your opinion what drives criminals to commit cybercrime?

With technology there are many reasons, aside pure theft, there are those who are fascinated by the ability to break into a system. This is particularly so for some hackers particularly the tech-savvy people who get excitement with the more security layers they can break into. Some are driven by temptation in cases where loopholes exist such as weak or written passwords (stuck under the keyboard!)

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

The recent passing of the Cybercrimes Act 2015 is a good step that the government has taken. This will facilitate the acceptance of electronic evidence which means that criminals in the cyberspace can now be prosecuted. However, the level of awareness around cybersecurity is still very low and more can be done to educate the public (which will impact both the private and public sector). In terms of infrastructure, we still have more to do.

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 and I believe many would say the same as this is becoming more prevalent especially with the use of smartphones. In most cases, companies will "quietly" lay off the staff who committed the cybercrime, it is only in large cases where the amount stolen/swindled is significant that companies will take these to court.

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

Like most crimes, deterrence starts with greater awareness. Most (if not all) of us would not sleep with the door open. Similarly, for any end user, company, public sector entity etc., one should always take the right measures to protect their information (data) and systems. This includes basic measures such as good user authentication measures right through more complex practices of DMZs, IDSs and regular monitoring mechanisms particularly for companies that are highly automated. However, all this must be cemented with user awareness. A well-proofed system can still be gained access to through an employee letting in unidentified visitors into the office block! One may frown upon this, but how many times have you let in a stranger into your office block without questioning?

What is the estimated number of certified professionals in the Tanzania - CISSP, CISA, CCNA etc?

If you focus on certified professionals in the cybersecurity space (e.g. CISM, CISSP, CEH etc.), the number will be very low, perhaps not more than 200-300. For example, based on ISACA Tanzania's records, we have less than 20 CISMs in the country! However, if we are to expand this to professionals with relevant IT certifications (CISA, ITIL, CCNA, MCITP, MCSE, etc.), this number will be much larger and (I can only estimate) to be in several thousands... However, when you project these numbers against the population even if this is narrowed down to those in employment including self-employment, the number of certified professionals is very low. We therefore have a lot to do to upskill and train the right individuals in cybersecurity as this subject is here to stay and attacks are likely to increase if not in volume, then in the level of sophistication. A recent Cybersecurity Venture report already predicts a large shortage of cybersecurity experts.

Top priorities for the Continent

Technical Training

With the many reported cases of system misconfiguration, open ports, default passwords, there is a need for technical staff to be equipped with hands on technical training in the concepts, principles and techniques required to successfully prevent and/or mitigate security issues on computing devices in a networked environment. In this day and age, it's evident that adversaries are not beating us because they have more technology, it's because they're more creative, patient, single minded and they explore limitless pathways. Organisation's should leverage their own creative, curious analysts and set them free to explore. If you don't have hunters, grow them. Free your people to chase the Why? Empower them with tools and education to enable them get relevant skills.

Awareness and Information Sharing

The levels of awareness and information sharing in Africa needs to increase. What we know today will never be enough. Just like in sports, in order to have a good strategy you should know who you are playing against. In today's African organisation, most employees don't know who they are defending against and they sometimes don't even know the game being played. Our information sharing is too slow. As a continent therefore, there is need to raise awareness through online programs, class based trainings and workshops. With regards to information sharing, we need to create a "Wikipedia" sort of phenomena where we can share information about incidents that have occurred and ways of mitigating them.

Collaboration

With everything moving to the cloud, physical barriers no longer hold water when it comes to the fight against cybercrime. African organisations need realize this and work together in order to realize reduced cybercrime rates.

This will require leadership at country level, although teams can work collaboratively to obtain greater resources, and expertise in this fight against cybercrime.

Government Policies

African governments need to strengthen the implementation of their existing cybercrime laws and policies. This will involve adopting more mature processes for cybercrime prosecution and raising awareness to citizens on reporting of Cybercrimes. Another critical areas that governments should focus on is involving more sectors during development of these cyber policies and laws; Universities, local groups, organisations and cyber security specialists.

Eco System Engagement

There is need for each member of the Cyber security eco systems to be first, aware that they are part of the eco system and second, understand their role in the eco systems. As Serianu, we have defined this ecosystem to contain but not limited to Universities, research Institutions, Government Department of Defense, cyber security experts, Media houses etc.

Joseph Mathenge

CISO Airtel Africa

Cyber security continues to capture and enthrall people from all walks of life. Cyber security loosely defined refers to criminal activity perpetuated through use of a computer and in what is commonly referred to as cyber space. The fascination in this vector of crime is no different than the reports of any other crime such as robbery, burglary or fraud. The very nature of cyber-crime being in the cyber space however, appears to provide fodder on which morbidly attracts so many. Africa is no different in falling victim to cybercrime. However, there simply is not enough information out to inform both government and individuals of what specific crimes to guard against as well as how to effectively respond when one falls victim. Herein lies the chief problem in dealing with Cyber Security in Africa; a lack of adequate knowledge of what to protect in cyber space and how to deal with security incidences.

To deal with these key issues, both government and private sector need to invest in continuous education informing both citizens and clients of the specific threats to their use of cyber space as well as build frameworks and guidance on how best to attain this.

While the private sector appears to lead in the charge of addressing cyber security threats, not nearly enough is being done. Not unlike global trends, private sector in Africa in most instances invest in security controls after falling victim to cyber-crimes. Taking the example of Heartland Payment systems that were victims of a credit data loss back in mid-2000, the company's CEO reported in quadrupling their spending in system security controls solutions.

The Africa market is projected to grow from **$0.92 Billion** in 2015 to **$2.32 Billion** by 2020.

The major force driving the growth of the African market is expected to be the increasing focus on government regulations and compliance requirements. Regions that will probably lead in this (South Africa, Nigeria and Kenya) have had several laws enacted in the recent past requiring private sectors to do more in protecting the data they collect, process and store. Again there are simply not enough laws, regulations and stiff consequences put in place to improve cyber security. While the Telecommunications industry in Africa doesn't necessarily have laws or frameworks written for them, they are a big target for cyber-attacks because they communicate and store large amounts of sensitive data. This very nature makes them subject to a wide range of the clauses included in many of laws by the nature of their industry. According to findings from The Global State of Information Security Survey 2015, many telecommunications companies are not doing enough to address cyber threats. The survey lists statistics showing that the number of security incidents detected by telecommunications companies dropped by almost 20% in 2014, however this drop doesn't indicate a reduction in intrusion but rather an increase in sophistication of attack vectors that make detection very difficult.

Addressing cyber security in Africa particularly in the Telco sectors would entail a replay of number of fundamentals successfully carried out in other fields globally.

I will outline just three (3) items that I believe are key in improving security posture.

First, a commitment to cyber security that builds process with security in focus. An organisation must be willing to implement the right tools to detect, analyze and respond to threats and these tools do not exceed in cost of the asset their created to protect.

Secondly, since ICT has been implemented as a solution to large number of the key challenges in Africa, we must build on ensuring that these solutions do not inherently increase the attack surface and are deployed in a secure model. In this I refer to use of applications (mobile or otherwise) that adhere to fundamentals of storing and processing personal information privately, can effectively log and provide accountability of activities done on them and are continuously monitored, tested and risks mitigated for new or previously unknown vulnerabilities.

Thirdly and this is perhaps most critical, is a continuous education and awareness campaign to all users of the risks posed in use of the cyber world. As use of these ICT objects provides greater power, so should great responsibility be on each individual to understand this power and to protect his or her self in using it.

Top priorities for the individual organisations

Awareness and Training

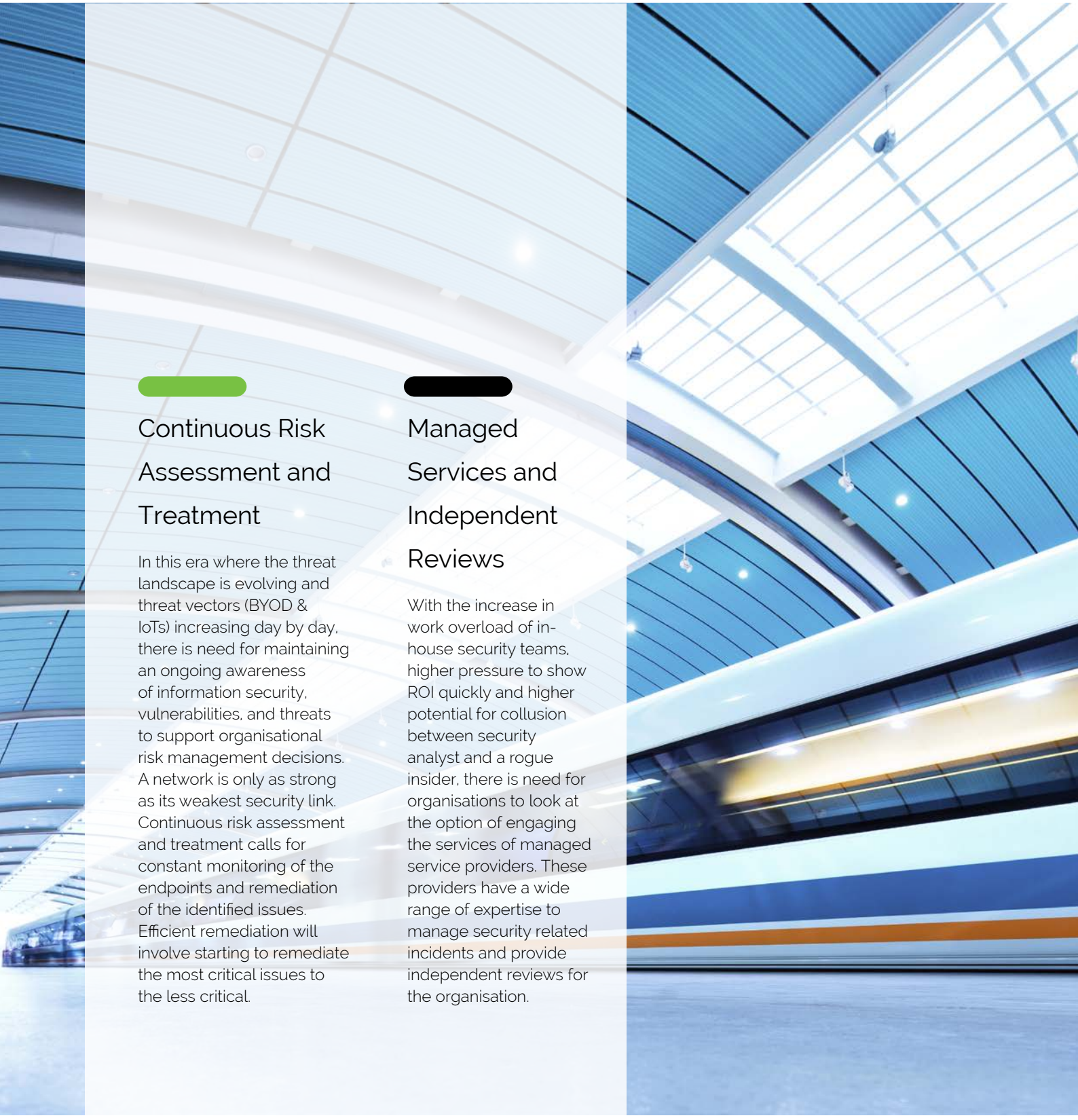
It is evident that attackers are now performing more targeted attacks against specific targets in organisations. It is crucial that organisations develop and implement security awareness training programs. This can be done in-house or outsourced to qualified service providers. Regardless of the mode of training, organisations should ensure that a needs assessment is conducted before adopting any form of employee training programs. 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 organisations should conduct continuous monitoring on all critical systems. Standards such as NIST identify a three-tier impact system-low, moderate and high impact-to use when developing monitoring policies. Continuous monitoring does not imply true, real-time 24x7, nonstop monitoring and reporting. Instead, it means implementing monitoring and oversight processes that provide a clear picture of the state of security at a given time while 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 African organisations 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 organisational 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 a rogue insider, there is need for organisations to look at the option of engaging the services of managed service providers. These providers have a wide range of expertise to manage security related incidents and provide independent reviews for the organisation.

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 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.

> > >

Top Cyber Security Incedences

December 2015 - the Nigerian Lagos State Government website brought down by unknown hackers. The website hacked, all the data dumped online and the link made available for everyone to see and download at will.

18th February 2016 - Fraudsters Hacked Central Bank of Nigeria Governor's Email and swindled $441,000.

February 15th 2016 –Anonymous leaks details of 64,000 employees of Tanzania Telecommunications Company Limited (TTLC)

27th March 2016 - Kenya petroleum company website defaced.

25th April 2016 - Internal fraud bleeds Kenyan banks dry. Most of these incidents are kept in the dark and never get to the public domain.

28th April 2016 - Ministry of Foreign Affairs hacked and ITB of data containing confidential information leaked.

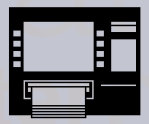
April 2016 - Woman conned out of £20,000 by Nigerian gang in online dating scam

22nd May 2016- Government of Ghana website defaced by a group calling its self 'ShadowTeam. The website homepage was changed and custom messages written on the new page.

27th May 2016 - Nigerian man nabbed in India for defrauding 90 people via online lottery scam.

30th May 2016 - National Oil Corporation of Kenya website hacked.

11th July 2016 - University of Nairobi twitter account hacked and hackers demand a Kshs. 700,000 ransom



July 14, 2016 – Some former bank employees/ ICT experts forge automated teller machine (ATM) cards and use them to steal from customers account.

July 2016 - Policemen in Ghana arrest six (6) Nigerian nationals who are believed to be members of a large group moving around and withdrawing money of VISA ATMs in the country with over 150 stolen ATM cards.

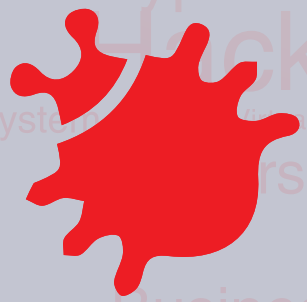
1st August 2016 - A Nigerian Man arrested for involvement in global scam worth more than $60 million dollars. He was arrested for hacking, conspiracy and obtaining money under false pretenses and money laundering.

On 8th August - a Nigerian blogger arrested by the anticorruption body Economic and Financial Crimes Commission (EFCC) on claims of cyber stalking

9th August - Nigerian hackers embed key logger into emails to capture user keystrokes.

August 27th 2016 - The Economic and Financial Crimes Commission arrested four students of Federal University of Technology, Akure, and one student of AdekunleAjasin University, Akungba, for their alleged role in N16m fraud.

16th September 2016 – 5 arrested for insulting president in Tanzania



26th September - Hackers open a fake Facebook account and impersonate Minister of Science and Technology, Dr. Ogbonnaya Onu in order to defraud unsuspecting individuals.

> > >

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

Paula Musuva-Kigen

Research Associate Director, Centre for Informatics Research and Innovation (CIRI), Digital Forensics and Cyber Crime Lecturer – United States International University (USIU)

Yet again we present the Serianu Cyber Security report but this time with a broader coverage that extends beyond Kenya to 4 other countries in Africa - Nigeria, Ghana, Tanzania and Uganda. The report presents an East-to-West Africa perspective that reveals trends that may have been overlooked. The collaborative effort in putting together this report also symbolizes the approach needed to address the cyber security challenge that presents itself across our interconnected economies.

Academia plays a leading role in the current strengthening of our cyber security posture but also in delivering the desired future. Equipping the current industry workforce can be done through well focused cyber security programs and also delivering practitioner certifications in collaboration with professional bodies. Delivering the desired future will be done through research and innovation. Africa is trailing in the investment on research and development as compared to other continents.

Analysis of 2014 statistics of R&D expenditure as a percentage of GDP from theglobaleconomy.com shows South Korea leading at 4.29% but of the top 50 countries the only African country is Egypt at 0.68% of GDP investment in research and development. Africa's challenges will only truly be solved by Africans. We need to invest our intellectual capacities and resources in addressing cyber security challenges with a proper understanding of our environment. Collaboration with academia is key in achieving this. It is my vision that one day Kenya will host a Center of Excellence in Cyber Security Research that will bring in collaboration between academia and industry in presenting solutions for the continent.

This year's report builds on the theme of **"Achieving Cyber Security Resilience"** that is largely achieved when we build in strategic capacity to spring back from disastrous events. Many organisations have understood that it is just a matter of time before they experience a potentially disastrous security attack. Our capacity to protect, detect, respond and restore systems back to full operation depends on our cyber security situational awareness.

This year's report has brought together a perspective of the African cyber security context that can help us;

(i) perceive what the key cyber security events are

(ii) comprehend what these events are indicative of

(ii) projecting into the future the impact of these events and their implications to our current organisational setting.

It is truly my hope that this Cyber Security report will help your organisation perceive, comprehend and project into the future what strategic steps it needs to take.

Top Cyber Security Issues in Africa - 2016

From high profile targeted attacks to simple scams, this section highlights our findings on some of the top issues that African organisations are facing. In the process, we have been able to identify the root cause for the success of these cyber-attacks.

1

Low Security Awareness

Most organisations don't budget for awareness and training programs for their staff. As a result, numerous breaches are now attributed to unintended employee error and or compromise.

2

Increased Insider Threats

In 2016, majority of cybercrimes reported across African organisations were caused by malicious employees. Organisations deploy state of the art technology to safeguard their environment but overlook the threat posed by malicious employees.

3

Inadequate budgets and management support.

The budgets allocated to cyber security in comparison to the other areas of ICT or business is inadequate to address security risks. Although there is increased management support and interest in tackling cyber security, the level of funding is still inadequate.

4

Emerging Technology and Enterprise Resource Planning

African organisations are implementing new technologies and automating their business processes without ensuring adequate security controls are put in place to safeguard these systems.

5

Increase in IoT Threats

IoTs refers to the ever – growing network of physical objects that feature internet connectivity. Increased smart devices carry associated risks as they are poorly managed/configured leading to the likelihood of compromise. Compromised IoTs have been used to propagate further attacks on other IT infrastructure.

6

Poor Vulnerability and Patch Management

Most organisations in Africa don't have vulnerability and patch management programs. These weaknesses lead to unpatched systems and insecure applications, exposing organisations to attacks.

7

Poor Implementation of regulation and Policies

Most countries in Africa are working to develop regulations and policies to address cybersecurity issues. However, there is still a huge gap in the effective implementation of these regulations and policies.

8

Ineffective Identity and Access Management Practices

Ineffective identity and access management practices are exposing organisations to a range of cyber security threats. The lack of effective controls around who and what level of access is provided within organisations is exposing organisations to cyber risks.

9

Cyberbullying, Stalking and Harassment

The pervasiveness of internet has on one side introduced an online community via instant communication while endangering the lives of those exposed to it on the other. The amount of personal information that internet users publish on social sites has been used against them in cases of cyber bullying, stalking and harassment, with some cases leading to offenses like kidnapping.

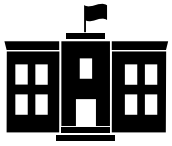
Cyber Security Risk Ranking by Sector across Africa

1. Banking

The interconnection and complexity of modern banking systems has led to complex regulatory requirements, greater exposure to internal and external cybersecurity threats and intensified concerns around data security and privacy across virtual borders.

In 2016, we witnessed more advanced attacks in banks mostly perpetrated by insiders, raising the concern that the banking sector is unprepared to deal with insider threats.

2. Government



Government institutions across Africa have increased their adoption of technology in a bid to improve services to their citizens. In this adoption process, the importance of cybersecurity issues around new technology is a growing concern.

3. Telecommunications

The threat map and cyber risks for Telcos in Africa remain high ranked as they control infrastructure that store and transmit large amounts of confidential customer data. However, the many risky protocols that these companies must handle expose them to attacks such as DDoS which would basically cripple operations of such a company. The impact of an attack against such a company can be very far reaching and devastating.

4. Mobile Money Services

The revolution of Mobile Money in Africa comes with unprecedented levels of fraud. Of the top twenty (20) countries in the world that are leading in mobile money usage, fifteen (15) are in Africa. These services have been integrated fully into numerous platforms such as banking, insurance and e-commerce, among others. Unfortunately, the adoption of these technologies has not been supplemented by secure controls, with most mobile money applications lacking basic security controls such as encryption of data.

5. SACCOs, Microfinance and Cooperatives

SACCOs and Cooperatives in Africa are quickly gaining a larger customer base and greater transactional amounts due to their competitive rates compared to larger financial institutions. This has led them in an effort to automate their processes manage their growing scope. This uptake has led to increased exposure to technology based fraud risks.

6. E-Commerce and Online Markets

The rapid growth of online sales and marketing platforms has created a growing range of security challenges for many of these organisations. In Africa, trading and marketing on online platforms has increased exponentially with the rising internet penetration rates and affordability. Cases of cybercrime and fraud have also risen in these markets due to poor security practices during the system development life cycles and implementations.

7. Utilities - Energy, Water and Electricity

African countries are experiencing an increase in the use of SCADA systems driven by the current efforts to automate public utilities services such as water, electricity, gas and rail. Most of these organisations are failing to address the security requirements of the SCADA systems during installation thereby increasing their exposure to cyber threats such as malware and insider infiltration.

8. Manufacturing

For many years, manufacturing organisations in Africa have relied on simple accounting or manual controls to mitigate fraud. This has changed over the past 5 years as these firms have implemented ERP systems that automate the entire manufacturing lifecycle. Unfortunately, majority of these organisations have not implemented the requisite controls to ensure they can detect and prevent system fraud. The lack of controls has led to a huge and sudden increase in system fraud targeting key financial processes in the manufacturing sector.

9. Other Financial Services – Insurance, Investments, Brokerage etc

The continued growth and popularity of financial services has led these companies to allocate most of their budgets to marketing and other operational activities. ICT spending is mainly focused on automation ignoring cyber security risk management processes.

10. Hospitality

The hospitality industry is primarily client facing and as such deals with a great deal of sensitive customer information from reservation details, payment, travel and consumer information collected from multiple systems. 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

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. .

Peter Kisa Baziwe

Information System Audit and Security Professional, Tanzania

Cybersecurity is a Global problem that has had local implications in Tanzania. For me the Year 2015 stands out for me as a turning point that brought cybersecurity to the forefront. In early quarter of 2015 Tanzania enacted the Cybercrime Act 2015 and Electronic transactions Act 2015. These have defined and continue to shape consequences of cybercrime and electronic fraud in Tanzania's cyberspace.

Later in October we had a General Election which also showcased the growing importance of the digital and social media in politics of the country.

The biggest indicator for me though was the Threat Cloud report from Checkpoint in 2015 that showed that in the Month of October 2015 Tanzania was one of the most cyberattacked countries in the world! What were all these hackers looking for? What did they find? What did they gain?

Some of the trends feeding the Cybersecurity problem in my opinion are;

1. **The geometric growth of internet connections,** mainly by new mobile phone users predominantly on the android platform. The rise of sub $100 smartphones with touchscreen and internet capabilities is driving use of applications like Facebook, Whatsapp, Instagram and Twitter to new heights. Many of these are not necessarily the latest android operating system and are susceptible to malware let alone little user cybersecurity awareness.

2. **The presence of National fiber optic backbone infrastructure** that is connecting more Multinational companies especially Banks, Oil and Gas , Telecom creates opportunities for hackers to attack these firms from here and pivot to their parent companies or headquarters. This is a real threat. Incidents involving the hacking group anonymous this year with a local telco and academic institution are a case in point. Whatever we think we are now targets of attacks by cyber adversaries acting on a global scale.

3. **There is a current drive for digital and electronic payments** for everything through mobile and the web by private banks and government institutions to improve efficiency and accountability. This also comes with its own risks and requires cybersecurity measures. Am talking about SMS banking interfaces between banks and telco systems; electronic and mobile trading platforms at the DSE ; ticketing payment platforms ;Electronic revenue collection platforms for both government institutions and private sector like banks and utilities will all face new cybersecurity challenges.

4. **Consumer technology is growing at a phenomenal pace** with digital internet capacities in radios, TV, watches, fridges, cars, and buildings….etc. The Internet of things is about and is and exploding like the Galaxy Note7! This has implications on our privacy from a personal level to and national security. Think a drone flying over unauthorized areas or using smart watches to record, transmit and leak sensitive data and conversations in real time.

5. **Big Data and the Cloud:** The financial Institutions, businesses and Government are collecting more and more data about us phenomenally. As a result the need for data analytics and mining and cloud capabilities will inevitably take center stage. The cyber risk of a compromise on a national databases or records in both government and private sectors is imminent. It can be local or international. More cyber adversaries especially nation state actors will want to have this data. The consequence of identity theft will have big implications in the lives of the local unsuspecting citizen.

Solutions

1. **National Cybersecurity Strategy.** This is urgently needed to direct resources and plans to securing our critical national cybersecurity infrastructure. I am glad to say thus is already in the works as announced by the Permanent Secretary Ministry of Transport Communications and Works in September.

2. **Education**. Cybersecurity awareness for citizens in use of internet, mobile banking and payment services; training of cybersecurity professionals and defenders, the Judiciary and Military; encouraging cybersecurity competitions and cyber clinics like one held at BUNI tech hub at Costech. These are crucial steps in boosting our incidence response and remediation capabilities. ISACA Tanzania is planning to be at the forefront of this by pushing the ISACA Cybersecurity certification-CSX.

3. **Collaboration.** There is need for both Government, Private Sector and Academic institutions to have forums that discuss and tackle these cybersecurity challenges. In the Private sector we have and see different challenges and threat actors. Sharing of solutions trends, intelligence and research is vital to keeping abreast in this dynamic field. As shown in the Costech funded – State of website security report -April 2016 of Gilbert Kilimba. It enables us to gauge where we have gaps in IT Security Practices.

Threat intelligence on particular in different sectors is of importance when shared to find out who persistent threat actors to both private are and Government Institutions.

Top Trends Influencing Cybersecurity in Africa

Mobile and Internet Usage and Costs

Africa is quickly catching up to Western countries with the rapid spread of mobile networks and internet usage. Sub-Saharan Africa is now the world's third-largest mobile market in terms of unique subscribers, closely following Asia Pacific and Europe. This has increased the exposure to cybersecurity issues.

Outsourcing-Vendor Risk

There is a growing dependence on third parties by organisations in Africa which has resulted in introduction of new attack vectors. African organisations are not adequately performing risk assessment on their service providers before or during their engagements.

BYOD

BYOD acceptance in African companies has risen substantially with specific gains with — client-facing employees. This trend is continuing to grow in all but the most security-restricted organisations. This is reflected by the 59.3% of respondents of the Africa Cyber Security Report Survey 2016 who were allowed BYOD within their organisations.

Industry Regulation

African countries are adopting laws and policies to regulate the ever increasing cybercrimes. A number of countries have passed or are in the process of establishing guidelines to deal with cybercrime. Even with these guides, most African countries still lack effective implementation mechanisms of these laws.

Cloud – Based Solutions

SMEs and public services in Africa 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 ICT costs. This trend has given rise to two security issues; traditional security controls won't help protect business critical systems and companies are losing visibility of their security posture.

IoT

The Internet of Things (IoTs) or Internet-connected devices are growing at an exponential rate and so are related 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.

Cyber Insurance

Several insurance companies in Africa 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.

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 Al Shabaab, Boko Haram and other terrorist organisations move to the internet.

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 adoption has created new security vulnerabilities that directly impact the users.

Poverty rates- Unemployment Rates

The high rate of unemployment in African countries 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. Unlike regions with low unemployment rates where sabotage and espionage are the main concern, African organisations are operating in environments with very high unemployment rates.

Cost of Cybercrime

Estimating the Cost of Cyber Crime for the Countries in Scope

As internet penetration in Africa rises, so does the rate of cybercrime. Individuals, groups and countries with malicious intent are now targeting sensitive information generated by different organisations/entities. Past estimates of the cost of cybercrime have failed to address the breadth of the problem and have not been able to provide a justifiable estimate of economic impact. In this section, we look more closely at the cost of cybercrime in Africa and try to gain better insights of the costs to the African economy.

From our research and analysis, we estimate that cyber-attacks cost African businesses (collectively in Nigeria, Kenya, Ghana, Uganda and Tanzania) around **$895 million a year**, which includes direct damage and loss, post-attack disruption to the normal course of business and reputational loss.

Analysis Methodology

Our analysis is based on information in the public domain, law enforcement and economics experts from a range of public and private-sector organisations and our tremendous knowledge of numerous cyber security attacks in the region.

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

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

A significant proportion of the **$895M losses is attributed to insider threats,** which we estimate at **$179,000,000** (50%% of all direct costs) and **$284,400,000** (32% of overall costs) per annum. In all probability, and in line with our worst-case scenarios, the real impact of cybercrime is likely to be much greater. As for measuring costs, this report decomposes the cost based on these 4 categories:

a. **Costs in anticipation of cybercrime,** such as antivirus software, insurance and compliance;

b. **Costs as a consequence of cybercrime,** such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise;

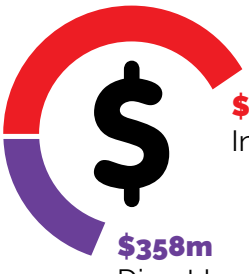
c. **Costs in response to cybercrime,** such as compensation payments to victims and fines paid to regulatory bodies;

d. **Indirect costs such as reputational damage to firms,** loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.

Cost of cyber-attacks in Africa

$895m

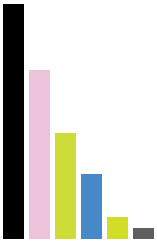
a year



Breakdown of Indirect Costs

Total Cost of Indirect Loss

$537m



- Technical Controls
  $252m | 47%
- Security Consulting Services
  $118m | 22%
- Loss of trust in e-services
  $84m | 16%
- Training
  $59m | 11%
- Reputational Damage
  $17m | 3%
- Insurance and Compliance Costs
  $7 | 1%

Breakdown of Direct Cost

Total Cost of Direct Loss

$358m

- Compensations to Victims of Breaches
  $154m | 43%
- Money withdrawn from victim accounts
  $154m | 43%
- Investigation and Remediation Costs
  $50m | 14%

Types of Cyber Crime Considered and Their Costs

Insider Threat	**$286m | 32%**	**Total Costs**
	$179m | 50%	Direct Costs
	$107m | 20%	Indirect Costs
Attacks on Computer Systems (Unauthorized Access and Malware)	**$234m | 26%**	**Total Costs**
	$79m | 22%	Direct Costs
	$155m | 29%	Indirect Costs
Social Engineering and Identity Theft	**$138m | 15%**	**Total Costs**
	$36m | 10%	Direct Costs
	$102m | 19%	Indirect Costs
Email Spam & Phishing	**$89m | 10%**	**Total Costs**
	$25m | 7%	Direct Costs
	$64m | 12%	Indirect Costs
Data Exfiltration	**$79m | 9%**	**Total Costs**
	$25m | 7%	Direct Costs
	$54m | 7%	Indirect Costs
Online Fraud Scams	**$68m | 8%**	**Total Costs**
	$14m | 4%	Direct Costs
	$54m | 10%	Indirect Costs

Cost of Cyber Crime **$895m**

Breakdown per Industry

$206m | 23%

Banking & Financial Services

$170m | 19%

Government

$143m | 16%

E-Commerce

$116m | 13%

Mobile based transactions/ e-commerce/e-payment

$98m | 11%

Telecommunications

$90m | 10%

Hospitality

$72m | 8%

Other Sectors/ Industries

Breakdown of the Statistical Analysis per Industry

For our statistical analysis, we computed the number of reported incidents *the average cost of an incident * estimate number of under-reporting (we estimated that only one in 15 incidents are reported i.e. 7%).

Cost to Banking and Financial Services Sector

Banking & Financial Services

$206m | 23%

Type of cost: Direct/Indirect costs

1. Banking malware (Keyloggers and other malware)
2. ATM Skimming
3. Insider threat
4. Investments in technologies to detect and prevent cybercrimes such as Antivirus, SIEM Tools, IDS/IPS
5. Audit and compliance with regulators

Cost of Cyber Crime to African Governments

Government

$170m | 19%

Source: Reported losses resulting from:

1. Tax fraud
2. Benefits fraud
3. Local-government fraud
4. Website defacements and
5. Ransom demands

Although we have used the most up-to-date information available, we believe that this is an underestimation of the total level of cybercrime against government systems. With many cases of tax evasion being reported such as the panama papers scandal, we believe that African governments are losing much more.

Cost of Cyber Crime to E-Commerce

E-Commerce

$143m | 16%

Type of cost: Direct cost
1. Online fraud
2. Credit card fraud
3. Social Engineering

Cost of Cyber Crime to other Sectors

Telecom-munications

$98m | 11%

Type of cost: Direct/Indirect cost
1. Advanced Persistent threats
2. Spam
3. DoS

Cost to Mobile based transactions

Mobile based transactions/ e-commerce/ e-payment

$116m | 13%

Type of cost:
Direct consequence of cybercrime. These were:
1. Malware
2. Social Engineering
3. Insider Fraud

Cost of Cyber Crime to other Sectors

Other Sectors/ Industries

$72m | 8%

Type of cost: Direct consequence of cybercrime. These were:
1. Malware
2. Social Engineering
3. Insider Fraud

Abdul-Hakeem Ajijola

Chair, Consultancy Support Services Ltd., Abuja, Nigeria.
A Cybersecurity & Cybercrime Advisors 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.

Brencil Kaimba

Risk and Compliance Consultant, Serianu Limited

Building Resilience in The African Cybersecurity Ecosystem

Ecosystem is a useful metaphor that points to a deep interdependence of many players that interact for multiple purposes. Businesses now operate in an increasingly interconnected and interdependent environment where information is the life blood and connectivity and innovation drive competitive advantage. Resilience in the eco system not only helps to extend the focus beyond resistance to shocks, but also supports long-term thinking about new risks and opportunities.

The Need for an Eco System

The problems we face outpace our abilities to solve them. These problems are cross cutting defying country and industry boundaries and no one organisation has all the solutions. We have witnessed the entire internet infrastructure of Liberia brought down to a grinding halt and numerous government websites, including Nigeria and Kenya, hacked by the Anonymous group.

One of the other critical issues that African organisations are facing, especially management, is the pressure to drive growth. Just getting profits is no longer enough. Previously, this growth was only achievable either internally or through mergers and acquisitions. However, if you add the eco system dimension to this, we get a third path to growth- leveraged growth. This is where you create growth by mobilizing complementary resources that add value to your market place and customers and in the process create value for yourself.

The key is understanding your role in the ecosystem and what steps you can take in that role to help improve it:

1. **IT Staff:** The IT team needs to embrace best practice in the development lifecycle, threat modelling and system hardening.This will ensure that protection is provided in the various network levels in an organisation.

2. **Non-IT Staff:** Upholding the requirements of the Information Security policy and by so doing, promoting the security posture of the organisation.

3. **Organisations** – Organisations need to document information security policies with relevant controls that will guide the implementation and operation of information security.

4. **Supply Chain** – To ensure confidentiality of business critical information assets is maintained, third parties should incorporate information security controls during system development and service delivery. Vendors also need to provide vulnerability reporting platforms to their respective clients in order to ensure that critical vulnerabilities are reported and remediated on time.

5. **Government** – The government is mandated with formulating and implementing cyber laws and creation of nationwide CERTs for incidence response and forensic investigations. For international initiatives, government needs to establish platforms that promote healthy collaboration between countries.

6. **Professional Bodies** – Professional bodies need to encourage their members to participate in security awareness initiatives just as much as skill/ technical training.

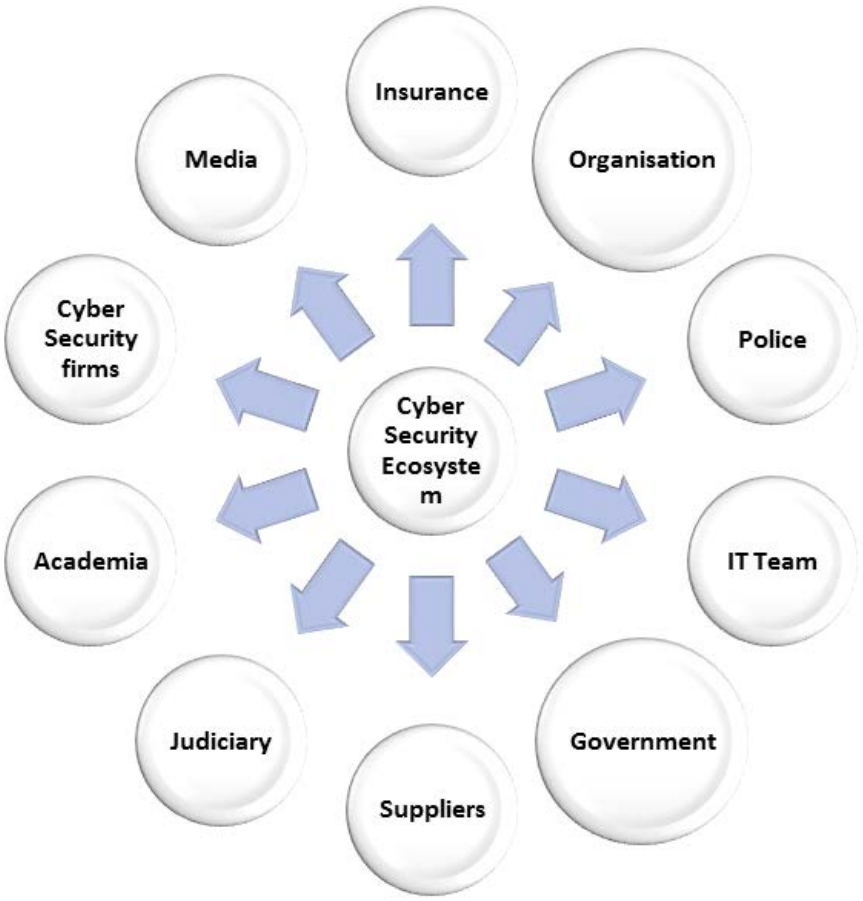
7. **Judiciary and Law Enforcement** – These bodies lack the skills and technology needed to identify cyber crimes and perform forensic investigations that will lead to successful prosecutions of cybercrimes.

8. **Academia** - The academia forms the backbone of information security research. More academic institutions need to incorporate security awareness in their curriculum to promote further research on emerging cyber threats in Africa and develop innovation hubs for young talent in the area of cyber security.

9. **Cyber Security Firms** – Cyber security firms have the advantage of large attack-knowledge base. This puts them in a unique and important position of providing visibility into the cyberthreat landscape for the other players in the ecosystem.

10. **Media** – The media plays an important role of spreading awareness to information system users by publishing cyber security events and providing information security awareness tips.

11. **Insurance** -. Insurance companies need to provide cyber insuranceand perform disaster preparedness drills. This will ensure that business continuity is assured for the various players in the ecosystem.



Serianu Cybersecurity Framework

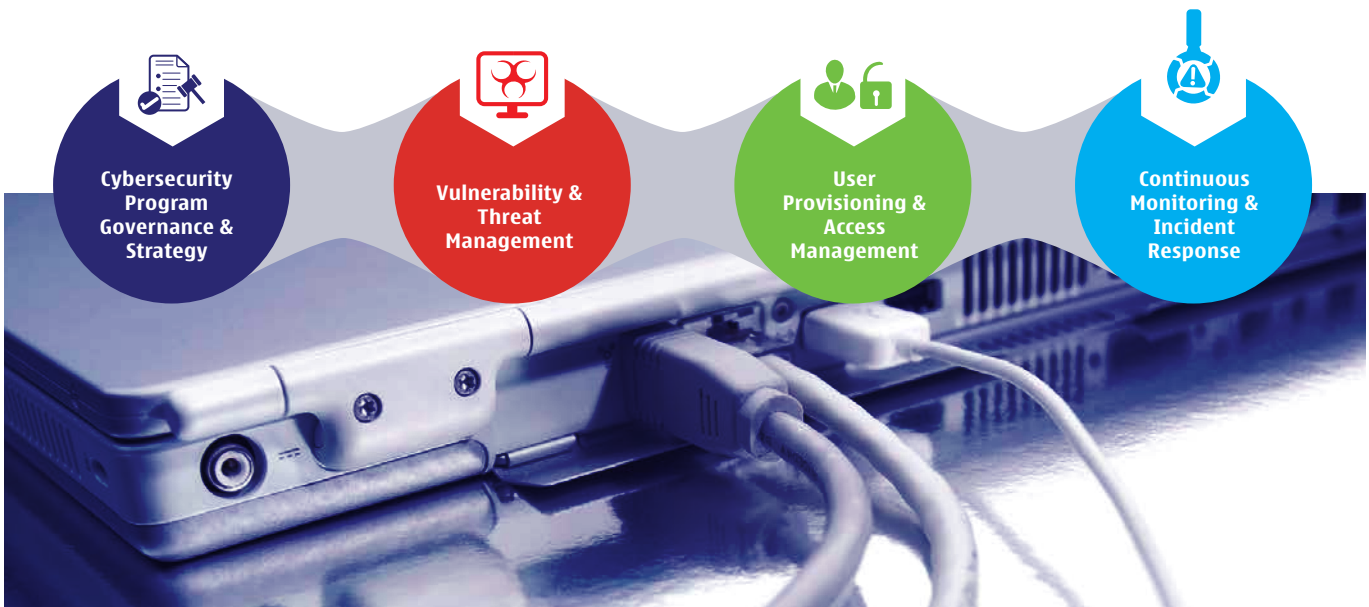
Introduction

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 organisations.

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.

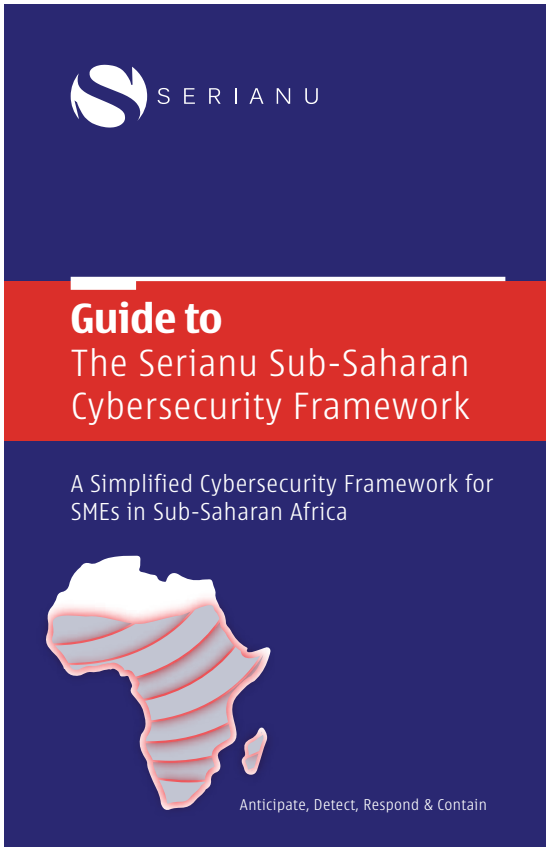


The framework is notably helpful also to small and medium-sized businesses seeking to implement global frameworks breaking down more complex categories and analysis into our four (4) domains namely: **Cyber Security Program Governance and Strategy, Vulnerability and Threat Management, User Provisioning 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 organisations operating in sub-Saharan Africa have implemented. As such it's important for organisations to understand that choosing to implement the framework solely means that the organisation 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


Cybersecurity Program Governance and Strategy
Inadequate security controls across the business
Limited budgets
Lack of management buy-in
Failure to identify & controls risks inherent to the organization
Inability to identify common threats with industries
Lack of security Awareness and Training
Social Engineering
Vulnerability & Threat Management
Failure to identify all possible risk prone assets to the organization
Misconfigurations
Unauthorized changes to critical systems
Lack of vulnerability and patch management
DDOs
Mobile Malware
Email Spoofing
Network Attacks
Port Scanning
Data Exfiltration
Inadequate Database Security
Failure to resume business operations
User Provisioning & Access Management
Insider Threats
Poor Identity and Access Management
Unauthorized changes to critical systems
Use of stolen user accounts
Abuse of privileged accounts
Inappropriate access to systems
Password sharing
Use of generic accounts
Continuous Monitoring & Incident Response
Lack of monitoring and incident response processes
Unauthorized changes to critical systems
Network Attacks
Port Scanning
Data Exfiltration
Malicious software
Illegal use of remote access tools

Cybersecurity Program Governance and Strategy

CONTROLS

Definitions

Global Frameworks Referenced

Inadequate security controls across the business

Limited budgets

CYBER SECURITY PROGRAM MANAGEMENT

Organisations should establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organisation's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to internal infrastructure.

ISO 27001:2013 A.6.1.5 NIST PM

SITUATIONAL AWARENESS

Organisations should establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cyber security information to form a common current state status of their environment and posture.

NIST SP 800-53, PCI DSS 12.6, ISO 27002 16.1.6 & SANS

Failure to identify and controls risks inherent to the organization.

RISK MANAGEMENT

Organisations should establish, operate and maintain an enterprise cyber security risk management program to identify, analyse and mitigate cyber secuirty risk.

NIST RA 1,6, ISO 22301 8.2.3 CNSSI 4009 PCI DSS 5 and SANS

Inability to identify common threats with industries.

INFORMATION SHARING

Organisations should establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience.

ISO 27002 16.1.2 NIST SI 5

Social Engineering

Lack of security Awareness and Training

AWARENESS AND TRAINING

Organizations should continuously provide adequate awareness, training and education to employees and partners are to enable them to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

ISO/IEC 17799:2005 8.2.2 SANS CSC 9-1,5 NIST AT 1,2

Vulnerability & Threat Management

CONTROLS

Definitions

Global Frameworks Referenced

Social Engineering

ASSET MANAGEMENT

Organisations should identify and maintain a risk-based inventory of the data, personnel, devices, systems, and facilities that enable them to achieve business purposes.

NIST SP 800-53, PCI DSS, ISO 27002 8.1 and SANS CSC 14.5

Configuration

CONFIGURATION MANAGEMENT

Organisations should establish processes to manage asset configuration. This should involve defining a configuration baseline for all critical IT assets and ensuring that assets are configured according to the baseline.

NIST CM 6, PCI DSS 2.2, ISO 27001 CNSSI 4009 and SANS CSC 3,10

Unauthorized changes to critical systems

CHANGE MANAGEMENT

Organisations should establish processes and technologies to manage changes to assets including analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes.

NIST CM 5, PCI DSS 6.4.5, ISO 27002 7.3.1 and SANS

Lack of vulnerability and patch management

THREAT AND VULNERABILITY MANAGEMENT

Organisations should establish and maintain processes and technologies to detect, identify, analyze, manage, and respond to cyber security threats and vulnerabilities, commensurate with the risk to the organisation's infrastructure (e.g., critical, IT, operational) and organizational objectives.

NIST RA 5, PCI DSS 5, ISO 27002 12.6CNSSI 4009 and SANS CSC 4-1,10

DDOs

Mobile Malware

Email Spoofing

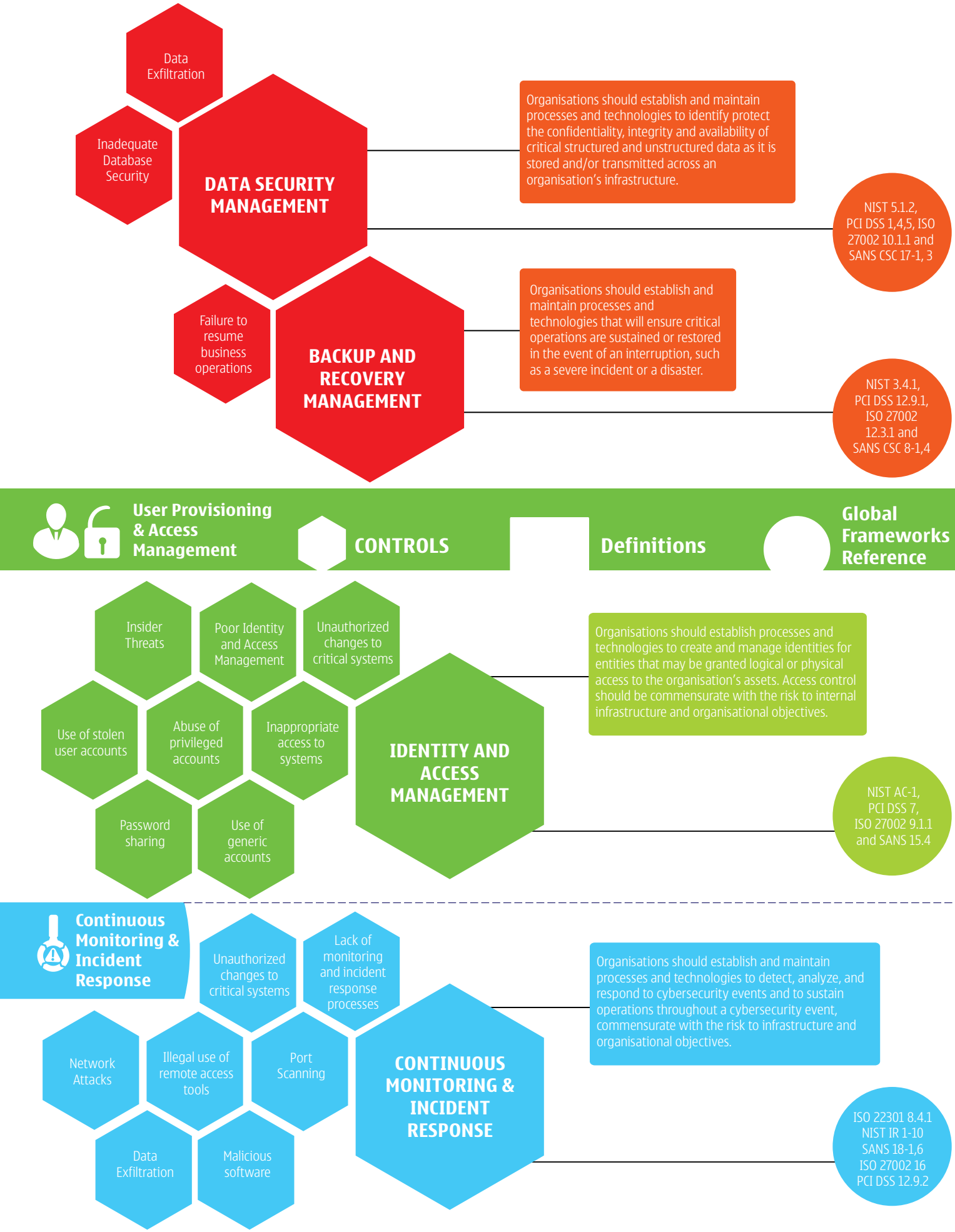
Network Attacks

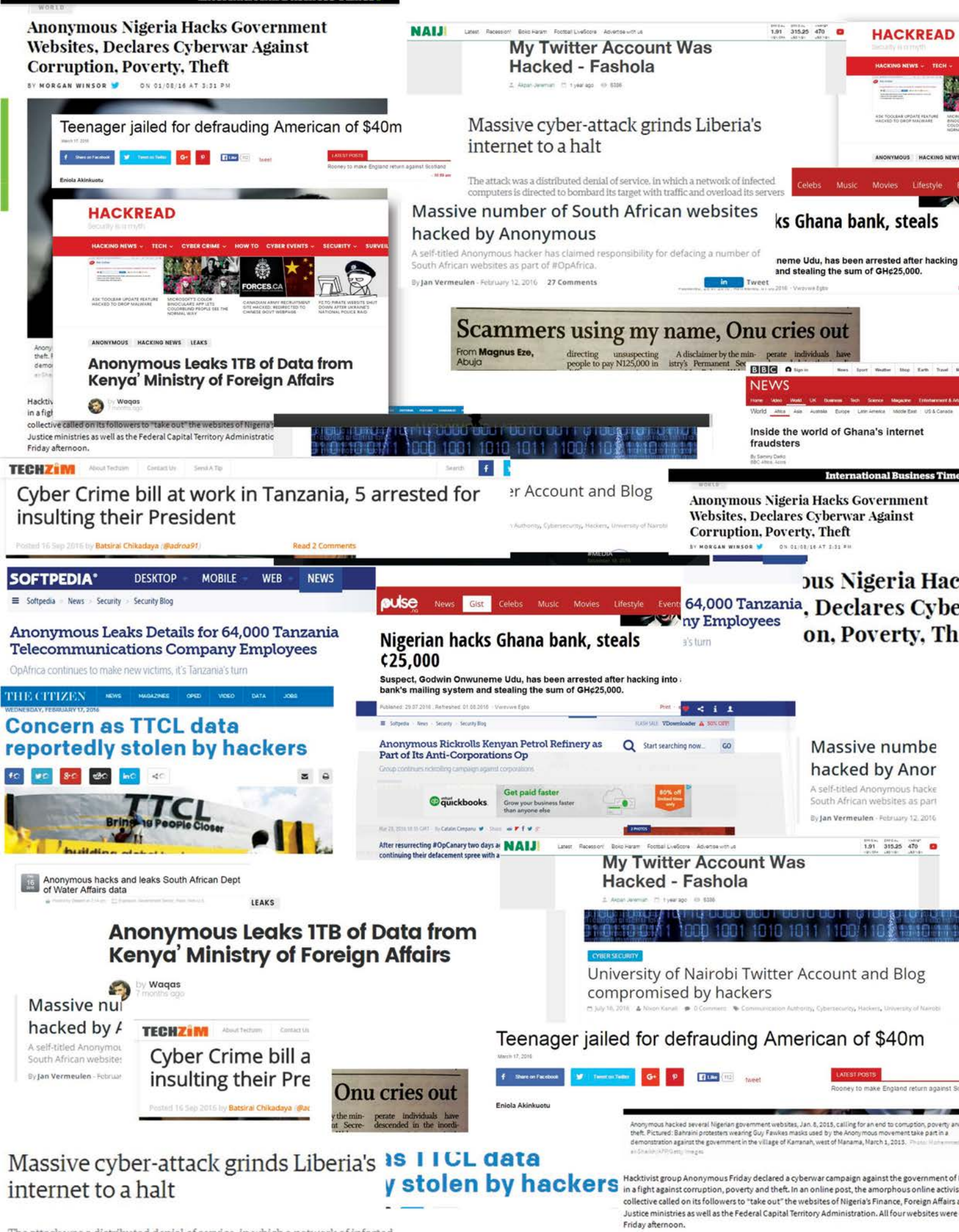
Port Scanning

BOUNDARY DEFENCE AND BRING YOUR OWN DEVICE (BYOD) MANAGEMENT

Organisations should establish and implement processes and technologies to prevent inappropriate or unauthorized access to an organisations network infrastructure including used of non-organisation owned devices.

NIST SP 800-53, PCI DSS 12.3 ISO 27002 6.2.2, CNSSI 4009 and SANS CSC 5-1,11


Data Exfiltration
Inadequate Database Security
DATA SECURITY MANAGEMENT
Organisations should establish and maintain processes and technologies to identify protect the confidentiality, integrity and availability of critical structured and unstructured data as it is stored and/or transmitted across an organisation's infrastructure.
NIST 5.1.2, PCI DSS 1,4,5, ISO 27002 10.1.1 and SANS CSC 17-1, 3
Failure to resume business operations
BACKUP AND RECOVERY MANAGEMENT
Organisations should establish and maintain processes and technologies that will ensure critical operations are sustained or restored in the event of an interruption, such as a severe incident or a disaster.
NIST 3.4.1, PCI DSS 12.9.1, ISO 27002 12.3.1 and SANS CSC 8-1,4
User Provisioning & Access Management
CONTROLS
Definitions
Global Frameworks Reference
Insider Threats
Poor Identity and Access Management
Unauthorized changes to critical systems
Use of stolen user accounts
Abuse of privileged accounts
Inappropriate access to systems
Password sharing
Use of generic accounts
IDENTITY AND ACCESS MANAGEMENT
Organisations should establish processes and technologies to create and manage identities for entities that may be granted logical or physical access to the organisation's assets. Access control should be commensurate with the risk to internal infrastructure and organisational objectives.
NIST AC-1, PCI DSS 7, ISO 27002 9.1.1 and SANS 15.4
Continuous Monitoring & Incident Response
Unauthorized changes to critical systems
Lack of monitoring and incident response processes
Network Attacks
Illegal use of remote access tools
Port Scanning
Data Exfiltration
Malicious software
CONTINUOUS MONITORING & INCIDENT RESPONSE
Organisations should establish and maintain processes and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to infrastructure and organisational objectives.
ISO 22301 8.4.1 NIST IR 1-10 SANS 18-1,6 ISO 27002 16 PCI DSS 12.9.2


Anonymous Nigeria Hacks Government Websites, Declares Cyberwar Against Corruption, Poverty, Theft
BY MORGAN WINSOR ON 01/08/16 AT 3:31 PM
NAIJ
My Twitter Account Was Hacked - Fashola
HACKREAD
Teenager jailed for defrauding American of $40m
Massive cyber-attack grinds Liberia's internet to a halt
The attack was a distributed denial of service, in which a network of infected computers is directed to bombard its target with traffic and overload its servers
Massive number of South African websites hacked by Anonymous
A self-titled Anonymous hacker has claimed responsibility for defacing a number of South African websites as part of #OpAfrica.
By Jan Vermeulen - February 12, 2016 27 Comments
ks Ghana bank, steals
neme Udu, has been arrested after hacking and stealing the sum of GH¢25,000.
HACKREAD
HACKING NEWS TECH CYBER CRIME HOW TO CYBER EVENTS SECURITY
ANONYMOUS HACKING NEWS LEAKS
Anonymous Leaks 1TB of Data from Kenya' Ministry of Foreign Affairs
by Waqas
Scammers using my name, Onu cries out
From Magnus Eze, Abuja
directing unsuspecting people to pay N125,000 in
A disclaimer by the ministry's Permanent
perate individuals have
BBC NEWS
Inside the world of Ghana's internet fraudsters
TECHZiM
Cyber Crime bill at work in Tanzania, 5 arrested for insulting their President
Posted 16 Sep 2016 by Batsirai Chikadaya (@adroa91)
Read 2 Comments
International Business Time
Anonymous Nigeria Hacks Government Websites, Declares Cyberwar Against Corruption, Poverty, Theft
BY MORGAN WINSOR ON 01/08/16 AT 3:31 PM
SOFTPEDIA DESKTOP MOBILE WEB NEWS
Softpedia News Security Security Blog
Anonymous Leaks Details for 64,000 Tanzania Telecommunications Company Employees
OpAfrica continues to make new victims, it's Tanzania's turn
pulse.ng News Gist Celebs Music Movies Lifestyle
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.
THE CITIZEN NEWS MAGAZINES OPED VIDEO DATA JOBS
WEDNESDAY, FEBRUARY 17, 2016
Concern as TTCL data reportedly stolen by hackers
TTCL Bring People Closer
Anonymous Rickrolls Kenyan Petrol Refinery as Part of Its Anti-Corporations Op
Group continues rickrolling campaign against corporations
Get paid faster
Grow your business faster than anyone else
quickbooks
80% off
Massive numbe
hacked by Anor
A self-titled Anonymous hacke
South African websites as part
By Jan Vermeulen - February 12, 2016
Anonymous hacks and leaks South African Dept of Water Affairs data
LEAKS
Anonymous Leaks 1TB of Data from Kenya' Ministry of Foreign Affairs
by Waqas
7 months ago
My Twitter Account Was Hacked - Fashola
CYBER SECURITY
University of Nairobi Twitter Account and Blog compromised by hackers
Communication Authority, Cybersecurity, Hackers, University of Nairobi
Massive nu
hacked by A
A self-titled Anonymou
South African website
By Jan Vermeulen - Februar
TECHZiM
Cyber Crime bill a
insulting their Pre
Posted 16 Sep 2016 by Batsirai Chikadaya (@ad
Onu cries out
perate individuals have
descended in the inordi-
Teenager jailed for defrauding American of $40m
March 17, 2016
Eniola Akinkuotu
LATEST POSTS
Rooney to make England return against Sc
Anonymous hacked several Nigerian government websites, Jan. 8, 2015, calling for an end to corruption, poverty an
theft. Pictured: Bahraini protesters wearing Guy Fawkes masks used by the Anonymous movement take part in a
demonstration against the government in the village of Karranah, west of Manama, March 1, 2013.
Massive cyber-attack grinds Liberia's internet to a halt
is TTCL data
y stolen by hackers
Hacktivist group Anonymous Friday declared a cyberwar campaign against the government of
in a fight against corruption, poverty and theft. In an online post, the amorphous online activis
collective called on its followers to "take out" the websites of Nigeria's Finance, Foreign Affairs
Justice ministries as well as the Federal Capital Territory Administration. All four websites were
Friday afternoon.

References

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

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

Summarized Findings Report

http://www.cyberroad-project.eu

Regional IP Attackers Analysis (AccelOps)

https://www.projecthoneypot.org/

Incidents

http://www.nation.co.ke/news/Govt-admits-hackers-stole-data-at-Foreign-Affairs-ministry/1056-3180962-90t2wyz/index.html

http://www.nation.co.ke/business/Internal-fraud-bleeds-banks-dry/996-3174878-mj8g4fz/index.html

http://realnewsmagazine.net/business/how-fraudsters-hacked-cbn-governors-email-swindle-441000/

http://www.mirror.co.uk/tv/tv-news/woman-conned-out-20000-nigerian-7785569

http://punchng.com/efcc-arrests-five-varsity-students-n16m-fraud/

http://pulse.ng/gist/evil-genius-nigerian-man-nabbed-in-india-for-defrauding-90-people-via-online-lottery-scam-id5083262.html

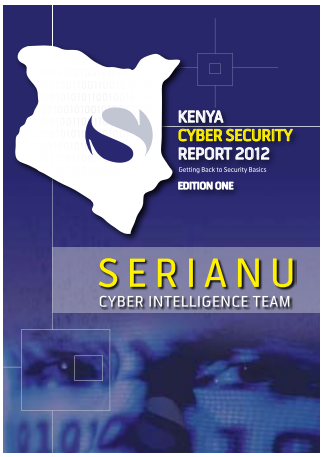
http://punchng.com/fraudster-using-onus-name-facebook-scam-ministry/

https://www.hackread.com/opafrica-anonymous-hacks-kenyan-oil-refinery-website/

http://www.standardmedia.co.ke/business/article/2000195162/equity-bank-hit-by-sh124m-fraud-in-tax-scam

http://x254.co/cyber-attack-on-the-university-of-nairobi-social-media-sites-been-contained/

2012



2013 + 2014

2015