SERIANU

# Africa Cyber Security Report 2017

## Demystifying Africa's Cyber Security Poverty Line

United States International University-Africa

ISACA
Trust in, and value from, information systems

DataposIT

DEMADIUR

kabolik

African Cyber Security
Botswana

LIQUID TELECOM

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

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


**For more information contact;**

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

# Content

# Editor's Note and Acknowledgement

**Brencil Kaimba**
Editor-in-chief

We are excited to present the 5th edition of Africa Cyber Security Report. Over the last 5 years, we have consistently strived to demystify the state of cyber security in Africa. In this edition themed **'Demystifying Africa's Cyber Security Poverty Line',** we take a deeper look at the financial limitations impacting many African organisations. We also provide a comprehensive analysis of the top Cyber security questions for Board members and Executives. This report comes at a time when African organisations are grappling with evolutionary changes in their social, technological, economic and regulatory environments.

The report contains content from a variety of sources and covers highly critical topics in Cyber Intelligence, Cyber Security trends, Industry Risk Ranking and Home Security.

Our research is broken down into the following key areas:

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

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

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

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

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

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

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

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

### What can our readers look forward to in this report?

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

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

## Appreciation

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

United States International University-Africa

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

**Our key partners in the various countries in scope provided immense support through their network of members spread across Africa. Key statistics, survey responses, local intelligence on top issues and trends highlighted in the report were as a result of our partnership. These are:**

ISACA
Trust in, and value from, information systems

DataposIT

DEMADIUR

kaboli

African Cyber Security
Botswana

### The Serianu CyberThreat Intelligence Team

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

Joseph Mathenge
Jackie Madowo
Kevin Kimani
Martin Mwangi
Barbara Munyendo
Daniel Ndegwa
Faith Mueni
Stephen Wanjuki
Jeff Karanja
Nabihah Rishad
Samuel Keige
George Kiio
Morris Ndung'u
Margaret Ndung'u
Paul Ingari
Ayub Mwangi
Samuel Momanyi
Bonface Shisakha

### USIU Team

Osemeke Onyibe Shalom
Stephen Maina
Gitau Polly Mugure
Lucy Nathan
Kuta, Jamilla Uchi

## Commentaries

**Eng. Haru Al Hassan**

Director, New Media and Information Security Department, Nigerian Communications Commission - Nigeria

**Kaleem Ahmed Usmani**

Officer in Charge, Mauritian National Computer Security Incident Response Team, Mauritius

**Aashiq Shariff**

CEO, Raha - Liquid Telecom Limited, Tanzania

**Henry Kayiza**

Ag. Assistant Commissioner, Cyber Crime Unit, Uganda Police

**Ibrahim Lamorde**

Commisioner of Police, Police Special Fraud Unit, Lagos- Nigeria

**John Sergon**

Ag, Chief Executive Officer, ICT Authority, Kenya

**Fredric Bobo**

IT Audit Manager, African Organisation of English-speaking Supreme Audit Institutions, South Africa

**John Ayora**

Director, Information Systems Security, Bank of Africa Group, Senegal

**Shimelis Gebremedhin Kassa**

CISA, MSCS,CEH - General Manager, MASSK Consulting PLC, Ethiopia

**Baidy Sy**

Associate Director, Digital Transformation and Cybersecurity Lead of Finetech Groupe, Senegal

**Ben Roberts**

Chief Technical Officer, Liquid Telecom Group, Kenya

**Arnold Mangemi**

Director Information Security, National Information Technology Authority Uganda (NITA-U) - Uganda

**Kenneth Ogwang**

Group Head of IT, East African Breweries Limited (EABL), a subsidiary of Diageo PLC, Kenya

**Dr. Peter Tobin**

Privacy and Compliance Expert, BDO Consulting, Mauritius


## Building Data Partnerships

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

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

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

Design, layout and production: Tonn Kriation

**Disclaimer**



**For more information contact:**


**Serianu Limited:**

info@serianu.com | www.serianu.com

Africa
Cyber Security
Report 2017

# Foreword

THE GLOBAL CYBER SECURITY LANDSCAPE IS EVOLVING AND BECOMING COMPLEX. THIS EVOLUTION IS LARGELY BEING DRIVEN BY THE RAPID CHANGE AND QUICK ADOPTION OF TECHNOLOGY INNOVATIONS. SINCE THE LAUNCH OF OUR INAUGURAL REPORT IN 2012, THE AFRICA CYBER SECURITY REPORT (ACSR) HAS FOCUSED ON UNRAVELLING THE AFRICAN CYBER SECURITY LANDSCAPE. WE HAVE FOCUSED ON UNDERSTANDING HOW AFRICAN ORGANISATIONS IN PRIVATE AND PUBLIC SECTOR PERCEIVE AND RESPOND TO THE CYBER SECURITY CHALLENGE. THIS APPROACH HAS ENABLED US TO INFLUENCE AND ENHANCE THE QUALITY OF DISCUSSIONS AROUND CYBER SECURITY ACROSS THE CONTINENT.

Through six years of research, we have grappled with a critical question that still puzzles the cyber security industry across the world. **What is the right level of cyber security for an organisation?** One clear output of our research is that most African organisations perceive Cyber security as a very technical and expensive affair. They are struggling to determine the right level of security and adequate budgets for security initiatives. These questions, coupled with numerous requests from readers of our reports across Africa informed our 2017 cyber security report theme; **Demystifying the Africa Cyber Security Poverty Line.** The theme borrowed from the term **"Security Poverty Line."** The Security Poverty Line means the point below which an organisation cannot effectively protect itself against losses to cyber attackers.


In our quest to answer this question, we surveyed over 700 business professionals from various businesses in 10 countries across Africa. We then cross-examined their annual expenditure on Cyber security. The findings from this survey shockingly point that most businesses, especially SMEs, are struggling to put in place basic cyber security structures. More than 95% of African organisations in private and public sectors are either operating on or below the **"Security Poverty Line".** Most of these organisations spend a maximum of **USD 1,500** annually on cyber security technologies and services.

In Africa, Small and Medium Enterprises (SMEs) create around 80% of the continent's employment (World Economic Forum, 2010), which clearly shows the importance of SMEs to African economies. The lack of adequate Cyber security controls in these organisations is an economic threat that the entire SME sector must address. Businesses within the SME sector are continually automating their processes and as a result their continued dependency on technology is driving them deeper into risk. Our research reveals that the most vulnerable SMEs are those in the financial services sector such as cooperatives, Saccos, micro-finance institutions, Fin-tech service providers and mobile money transfer services.

"The 2017 Cyber security survey shockingly reveals that **over 95%** of African businesses are operating **below** the **cyber 'security poverty line'.** "

**William Makatiani**

CEO, Serianu Limited

The 2017 Ransomware attack is a good case in point, where many cyber security professionals in Africa were contracted by established organisations. At the height of the crisis, the small Cyber security professionals' talent pool were snapped up by huge multi-nationals that offered better incentives. This left the vulnerable SME sector completely at the Cyber criminals' mercy. Considering the skills and technical resource challenge in the continent, who was taking care of the SMEs?

SMEs in Africa are facing a several challenges including the prohibitive cost of Cyber security solutions and services, limited budgets, lack of skilled personnel. With these challenges, it's become prohibitive for these companies to adopt complex Cyber security frameworks, leaving them exposed and vulnerable to attacks.

The 2017 Africa Cyber security report is a call to action. The African Cyber security ecosystem – government, consultants, vendors, academia – need to find cheaper and practical ways to address the continent's cyber security challenges. The continued reliance on overly expensive and elaborate frameworks is not working for 95% of the key constituents – SMEs. We need to develop new approaches and attitudes towards the problem and build self-reliance and self-sufficiency to adequately address the Cyber security challenge in the continent.

# Executive Summary

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

Our research is broken down into 8 key areas:

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

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

## What is the cyber security poverty line?

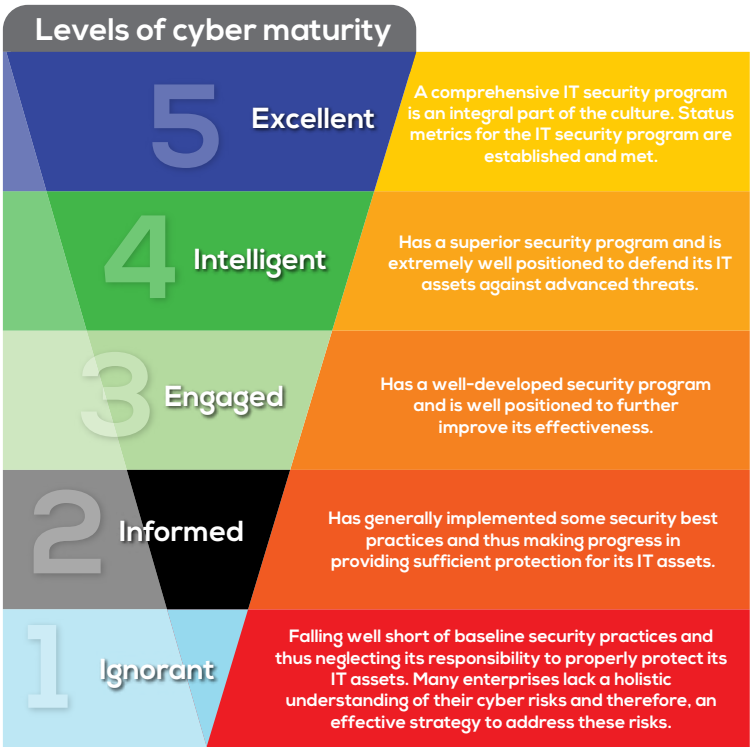
Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

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

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

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

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




## What is the impact of operating below the poverty line?

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

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

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

**What does the future hold for this problem?**

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

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

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

# Key Highlights

## Breakdown of key statistics for different countries:

| | Population (2017 Est.) | GDP (2017) in USD | Penetration % Population (2017) | Estimated Cost of cyber-crime (2017) | Estimated No. of Certified Professionals |
|---|---|---|---|---|---|
| Africa | 1,300,000,000 | $3.3T | 35% | $3.5B | 10,000 |
| Nigeria | 195,875,237 | $405B | 50% | $649M | 1800 |
| Tanzania | 59,091,392 | $47B | 39% | $99M | 300 |
| Kenya | 50,950,879 | $70.5B | 85% | $210M | 1600 |
| Uganda | 44,270,563 | $24B | 43% | $67M | 350 |
| Ghana | 29,463,643 | $43B | 34% | $54M | 500 |
| Namibia | 2,587,801 | $11B | 31% | * | 75 |
| Botswana | 2,333,201 | $15.6B | 40% | * | 60 |
| Lesotho | 2,263,010 | $2.3B | 28% | * | 30 |
| Mauritius | 1,268,315 | $12.2B | 63% | * | 125 |

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

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

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

Cost of cyber-attacks **$3.5B** annually


Fake News has hit Africa's media streams as we increasingly see unverified and often conjured up news being circulated through various medium.

over **90%** of parents don't understand what measures to take to protect their children against in Cyber bullying

Banking Sector is still the most targeted industry in Africa

Most organisations' Cyber security programs are **Tool Oriented**

**96%** Cyber security incidents either go unreported or unsolved

**Eng. Haru Al Hassan**

Director, New Media and Information Security Department

Nigerian Communications Commission

Nigeria

**What is fake news?**

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

**How did fake news become such a big problem?**

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

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

**What will ultimately get brands to fight fake news?**

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

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

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

**What happens when fake news spreads?**

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

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

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

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

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

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

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

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

### What are some of the pros?

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

### Why is Ransomware so effective?

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

### What is the possible impact of Ransomware?

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

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

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

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

No.

### How often do you transact using your mobile phone?

Daily.

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

No.

### Why does the cyber skills shortage need immediate attention?

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

### How many unfilled security jobs are estimated to exist today?

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

### How does collaboration help enrich the students' learning?

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

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

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

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

Once a year, albeit rarely.

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

- High
- Medium
- Low

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

Yes.

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

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

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

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

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

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


# Top Trends

## **Fake News:** Vulnerability of truth

A lie can travel half way around the world while the truth is putting on its shoes', they say.

In 2017 our media platforms were overwhelmed by rogue politics, misinformation and dubious claims. From videos of post-election violence to news about politicians who have deflated from their political parties, the real impact of the growing interest in fake news has been the realization that the public might not be well-equipped to separate quality information from false information.

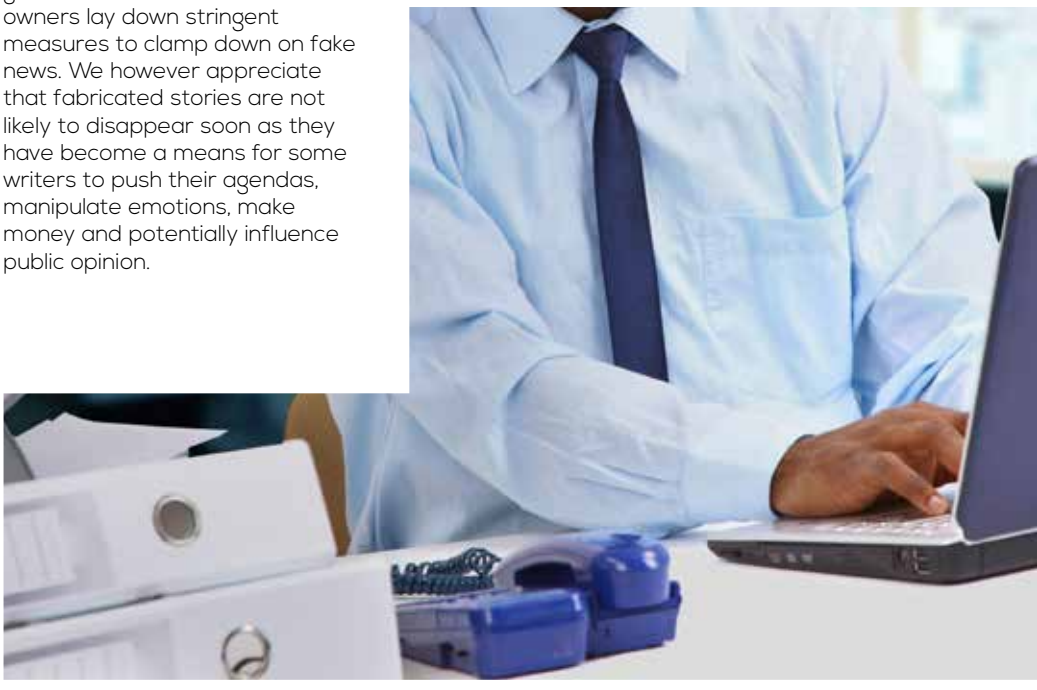
It is paramount that governments and social media owners lay down stringent measures to clamp down on fake news. We however appreciate that fabricated stories are not likely to disappear soon as they have become a means for some writers to push their agendas, manipulate emotions, make money and potentially influence public opinion.

## **Insider Threat:** The enemy within

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

Top insider threats:

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



## **Ransomware:** I don't WannaCry


Worldwide attack map

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

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

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

## **Cyber bullying:** It takes the entire Cyber Community to raise a child

From cases of ordinary citizens committing suicide to popular artists claiming to be victims of Cyber bullying, it goes without saying that the uncontrolled liberty to write messages on social media has brought with it social injustices.


Blue Whale Challenge is an example of an evolved Cyber bullying mechanism targeting vulnerable teenagers. The game assigned daily tasks for 50 days, thereafter encouraged the user to commit suicide. A number of children fell victim to this game- one teenager in Kenya.

It is critical that African organisations formulate laws to criminalize cyber buying. A number of countries have made strides in this and have criminalized Cyber bullying.

## **Skill gap:** What you do not know will hurt you

The cost of Cybercrime grew by approximately 20% but the skill gap is widening. Very few people know what they're doing, most IT and security staff are downloading templates from the internet and applying these in their organisations. From our analysis, a key contributor to this is that organisations tend to look for people with traditional technology credentials – IT, Computer Science. But when you look at the matter, we need Technology analysts, Cyber Risk Engineers, data analysts, Risk experts most of which do not necessarily warrant a technology course. Majority of organisations encourage their IT teams to take up courses that don't necessarily add value to the security of the organisations.

It is also concerning that companies would rather poach talent from each other and from training providers than develop it themselves.

This points to the sad fact that businesses are thinking in the short term. Rather than cultivating the needed talent, organisations are continuously relying on ready-made talent pool.

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

## **Mobile and Internet related services.** Battery is low is no longer the only warning

As the use of online services has risen - with more than half of the banking users using internet banking and three quarters using mobile banking services. Attackers are now leveraging these platforms to steal money from customers.

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

Mobile banking users have also become victims of social engineering attacks especially with the increased number of betting and Ponzi schemes.

There is a clear need to bridge the knowledge gap on mobile money operations among security teams and to identify common security, fraud and money laundering challenges confronting mobile money operations across the financial services sector. Mobile money users are also to be educated on identifying and evading phishing scams.

## Network Architecture: Defense In-depth

The success of most attacks in 2017 were in one way or another linked to one critical issue: Weak Security Architecture. Successful ransomware attacks were mainly due to missing patches. Other cases involved inadequate privilege account monitoring and poor third party risk management.

Yet these organisations have invested heavily in the latest Antivirus programs or SIEM solutions.

High technology solutions installed on top of weak architecture only equals one thing A WHITE ELEPHANT. Most organisations in 2017 focused a large part of their IT budgets on acquiring high end technologies but forget to set the foundation on which these technologies will effectively operate.

A SIEM tool is a useless investment if auditing is not enabled in network devices, no expertise exists for continuously analyzing and refining the alerts. Defense-in-depth means, applying multiple countermeasures in a layered or stepwise manner. Because there are ways around traditional protective systems such as firewall, it is imperative that individual systems be hardened from the Network, Application, Endpoint and Database levels.

This means, putting controls in place for Remote Access (see appendix for Remote access tools list), Change and vulnerability management.

## Phishing: The weakest Link

Phishing is one of the attacks that leverages the inadequacies of humans and remains worryingly effective. In quarter on 2017, Kaspersky Lab products blocked 51 million attempts to open a phishing page. Over 20% of these attacks targeted banks and other credit and financial organisations. With the evolution of phishing, it has become clear that basic awareness training may not be sufficient to safeguard your organisations. 2017 has proven that we need to leverage technology especially since education programs, awareness campaigns and product innovation on their own have failed.

## Cyber Pyramid Schemes: Easy come, Easy go

2017 has seen a fair share of Ponzi schemes. Notable example in Kenya is Public likes which cost Kenyans roughly Ksh. 2 trillion, D9 ponzi scheme in Tanzania, and crypto currency scams in Nigeria. These schemes rely on a constant flow of new investments to continue to provide returns to older investors. When this flow runs out, the scheme falls apart. In recent times, we have seen these schemes evolve to now include crypto currencies.

We have noted a few initiatives from the private sector including the "Nigeria Blockchain Alliance" (NBA) which brings together law enforcement agents, legal practitioners, forensic investigators and government in the fight against crypto currency related crimes and the CBK in Kenya and the Bank of Tanzania and capital market and Securities Authority issue warning on ponzi scheme. More awareness and initiatives needs to be put in place to ensure that citizens are protected from these scams.

## System Integrity: Eroding Public Trust

Government systems have become a target for hackers seeking to make news or disrupt service delivery. From Electoral systems to Integrated Financial Management Information System (IFMIS), 2017 registered the highest number of alleged election hacking in Africa, Europe and America. Whether the allegations for hacking are true or not, there is no denying that these systems have become a juicy for hackers. As such tighter controls need to be in place to ensure that the confidentiality, integrity and availability of these systems are maintained.

**Kaleem Ahmed Usmani**

Officer in Charge

Mauritian National Computer Security Incident Response Team

Mauritius

**In your opinion, what was the key cyber security issue facing your country or Africa, what is being done to address this issue?**

Wannacry and petya Ransomware were the biggest.

We took the following steps:

- Advisory: We circulated an advisory to organisations and people in the country 3-4 times.
- We actively monitored key systems within the country for any malicious indicators of compromise
- We engaged with our partners in the country to gather more intelligence on key indicators of compromise, statistics and patching of systems.

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

Yes it's a problem, especially on social media. Our internet penetration is well over 50% and majority of these users have access to social media. Social media has been used to spread false information and ignite unrest in the country.

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

This is a collective responsibility. Given that the channels used to transmit fake news are privately owned, Telcos only provide the connectivity and the privacy of users has to be maintained at the end of the day. This needs the combined effort of all involved stakeholders. We need to educate people and have systems in place to detect them. The police in Mauritius have done a good job ensuring that they inform people accordingly.

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

It varies from country to country. For Mauritius, whenever we identify these messages or fake news, we liaise with the relevant platform owners (Google/Facebook) to remove the messages. At times we are successful. For continued effectiveness, we need to enhance the relationship between law enforcement, private sector and government.

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

Education is crucial. We conducted a number of campaigns all year round for parents, senior citizens and children to sensitize them. We also liaise with various vendors such as IBM, Symantec to gather better intelligence and action on these.

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

We are in the digital transformation age where such automation is expected in order to improve efficiency and service delivery. There are a number of e-services that are working properly and some which still need to be secured.

In Mauritius particularly, we have made a number of strides in this regard, we are ranked 6th best in the world rankings, and we have strong legislations and cyber security strategy that we are implementing. E-government strategy addresses the security of systems. Security can never be 100% however, so we are continuously reviewing our strategies to minimize our cyber threat exposure.

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

Yes, mostly by the ransomware Wannacry and petya.

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

- Advisory: We circulated an advisory to organisations and people in the country 3-4 times.
- We actively monitored key systems within the country for any malicious indicators of compromise
- We engaged with our partners in the country to gather more intelligence on key indicators of compromise, statistics and patching of systems.

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

Education is key. We need to empower people with basic knowledge to understand what to do for example with an email attachment which is a ransomware. We also need to train our cyber security experts to have the capacity and competence to manage such cases.

**Do you think organisations are spending enough money on combating cyber-crime?**

This is subjective as it depends on the country. The Mauritian government is committed to ensuring that organisations are secure by putting in proper policies in place. Many organisations have different priorities, but over the years they have now started paying attention. Government budget has also increased in recent years.

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

This is true. African universities don't have specialized courses for cyber security while at the same time, we do not promote the culture of cyber security. As a country, Mauritius is working to address this challenge through its Software development strategy that is currently in draft. This will provide a framework for software development within the country.

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

It is important that we develop frameworks that support innovation within our countries and universities. Platforms such as COMESA, SADC should also be leveraged to promote partnerships for innovations in the cyber space.

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

We are lagging behind in legislation, organisational and national strategies, capacity building of professionals, alignment of our legislations with international standards, international cooperation.

Cyber security attacks are borderless, if we have a harmonized legislation (AU, SADC), it will be easier to contain these threats.

# Africa's TOP 10 priorities for 2018

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

## 1 Database Security: Secure the vault

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

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

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

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

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

## 3 Patch Management: To patch or not to patch

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

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

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

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

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

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

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

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

## 5 Endpoint Security: Cyber security front-line

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 10 **Continuous Monitoring:** Askari Vigilance

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

**Aashiq Shariff**

CEO

raha - Liquid Telecom Ltd

Tanzania

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

- Malware with worm capabilities
- Basics – Endpoint security, patching
- Weakness of mobile carriers
- Overwhelming client with alerts
- Adapting firewall to face new threats
- Monitoring Icloud configuration and Security

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

Yes

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

Initially government, Telco's, end users – collective efforts.

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

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

Platforms that can be confirmed – Government sites,

**Many governments in Africa are investing in e-services (e-government, e-voting, e-tax systems and many other portals.)**

**Do you think the African citizenry is ready to consume and utilize these systems without the worry of privacy, security and fraud?**

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

If there is no appropriate firewalls in place the information can be gathered by wrong entity.

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

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

Some ended up paying in order to get the data.

Some who had end point security worked with Antivirus owners to patch and recover the information.

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

Awareness, appropriate firewall that can mitigate such attacks.

Do you think organisations are spending enough money on combating cyber-crime?

No.

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

More awareness and risks involved, and guidance on appropriate systems to suggest comparing on the size of data and risks involved.

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

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

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

Conduct the awareness and ready with solutions.

Ready solutions depending on the organisations/entity.

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

- Technical Trainings
- Awareness & Information Sharing
- Collaboration – Government & Companies (Private)
- Government Policies
- Other collaboration – Universities, Cyber security experts, research institute, media houses.

# Engaging Board Members in African Organisations

Top Cyber Security Questions

ANTICIPATE

**The first core cyber security function is to identify your organisation's cyber security risk, which is the amount of risk posed by your institution's activities, connections, and operational procedures.**

*Questions Executive's should ask:*

**Does my institution fully understand what information it manages, where the information is stored, how sensitive is the information, and who has access to it?**

To identify risks that your organisation is exposed to require that you first and foremost identify all your assets and prioritize these based on their business need.

**What are my institution's key business assets? Do I have adequate protection for them?**

To adequately assess risk to your organisation, you must first identify what your organisation's "crown jewels" are, their location, and how they are being protected. These can be employees or customers, property (both tangible and intangible), or information (databases, software code, records).

**What types of connections does my institution have (VPNs, wireless, LAN, etc.) and how are we managing these connections?**

A leak of confidential data whether accidental or through thieving could lead to significant company losses. Organisations need to be aware of the kinds of connectivity allowed from both internal and external sources and have management policies and procedures around them.

**How are staff at my institution identifying risks, and providing me with accurate and timely information about those risks?**

At any given time your institution could be exposed to several different types of information security threats such as internal threats, like malicious or unaware employees; Physical threats by a potential intruder; and Internet threats, such as hackers. Consider the threats your organisation is exposed to and the vulnerabilities that may exist surrounding these threats.

**What is our ability to mitigate those risks?**

60% of all identified vulnerabilities go un-remediated/unmitigated. While 50% of successful attacks are as a result of previously identified vulnerabilities. It's critical that for every vulnerability identified, the organisation evaluates its ability to mitigate the risks

**How is my institution connecting to third parties and ensuring they are managing cyber security controls?**

Third party vendors not only have access to internal network but also sensitive data. There is need for third party vendor assessment and development of a third party management program.

**How effective are my organisation's policies and procedures for monitoring information inventory?**

There is need to validate that policies and procedures for information security exist, are up to date and reflect the organisation's current operating environment.

**Do my IT personnel have the appropriate knowledge or skills to protect against a potential cyber-attack?**

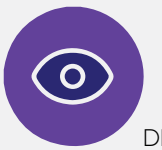
The IT team needs to be equipped with skills and techniques that they can leverage against cyber attackers.

**Are my staff informed about cyber threats?**

The people in an organisation are the weakest link when it comes to cyber security. A security awareness program enables organisations to improve their security posture by offering employees the knowledge they need to better protect the organisation's information through proactive, security-conscious behavior.

**Do they have an understanding of risk from their actions?**

There is need to conduct organisation wide training on cyber security awareness. Employees need to comprehend the significance of protecting company confidential and client confidential information. They need to be aware of the consequences of their actions as well as the penalties involved.



DETECT

**Although prevention is ideal, not all attacks can be prevented, making compromise inevitable. Therefore, a better approach to security is timely detection of the attack detection that will contain and control the damage.**

**Breaches are often detected after weeks, months or even years. Detecting breaches happening right now would of course be very desirable.**

*Questions Executives should ask:*

**How is our executive leadership informed about the current level and business impact of cyber risks to our company?**

There is need for executive leaders to be aware of the costs of cyber risks to the business. There should be a defined set of metrics used in reporting and making information security related business decisions.

**Are we prepared to prevent or limit the damage caused by these attacks?**

There is need for organisations to carry out risk assessments so as to identify critical business assets as well as their associated vulnerabilities. This will help in prioritizing risks as well as resource allocation.

RESPOND

**Effective incidence response is the backbone of any successful Cyber Security Program. It is important that organisations adequately prepare for a cyber-security incident, and this includes knowing how you will respond once an incident occurs. To do this, organisations must have an incident response plan.**

**Where to Start in Developing an Incident Response Plan.**

*Questions Executives should ask:*

**Have we created an effective incident response plan?**

It is crucial that as an executive, you ensure that there is an incident response plan and team to support it. At a minimum, the incident response

plan should address the preservation of evidence, step by step guide on handling different incidents and optimum duration for incident handling and escalation.

### How often is it tested?

Regular testing of the Incidence response plan ensures timely containment of security incidents. Testing of the Incident response plan ensures that it remains current and useful. Testing may include the following steps;

1. Updating the contact lists for incidence response team, vendors
2. Performing table top exercises what are facilitated
3. Carrying out discussion based exercises where employees get to discuss their various roles and responsibilities in case of a disaster.

### What would we do if we were hacked today?

The incidence response plan should cover steps provide an answer to this very critical question. The following are three steps that should be addressed within the Incident response plan:

1. Evaluation of the Cyber-event; answer the following critical questions such as were high value assets compromised? Were any data altered/stolen?
2. Invoke the Incident Response Plan; this steps helps to prevent further damage or loss. More often than not, at this points it's often too late to develop the right procedures.

### Do we have a plan to inform internal and external stakeholders?

Stakeholders need to be defined and documented. A communication mechanism needs to be established and documented in an incidence response plan.

### Conduct preparedness training for the incident response team.

There is need for Training and resource requirements need to be defined. The incident response team needs to be aware of the action plan that is to be executed when a crisis is discovered.

CONTAIN

**Getting to the root cause involves a level of understanding beyond that of simply identifying that a system in infected.**

**Executives need to understand what specifically enabled or facilitated the infection or compromise. Identifying the root cause allows us to understand why the malicious activity succeeded. This is then followed by precise measures to prevent the reoccurrence of the issue.**

*Questions Executives should ask:*

### Does my organisation's incident response plan include steps for recovering after a cyber-attack?

A good incidence response plan will contain a step by step plan for:

- Rebuilding network devices that may have been compromised and restoring baseline configurations.
- Restoring the integrity of data that may have been compromised
- Restoring normal business critical operations

### When did we last test our incident response plan?

Testing of the incidence response plan should be done at least annually or whenever any major changes occur in the business environment. This ensures that the plan and its user's remains updated on the activities that are critical for business process recovery.

### How will we communicate with internal staff, customers, third parties, regulators and law enforcement of a data breach at my organisation?

A good response plan should provide details of how and what to communicate during an incident. This should cover the following:

- Proper Incident notification channels
- Communication to customers, regulators, media, law enforcement, and other stakeholders.
- Evaluation of the event and documentation – Evaluation is done by answering and recording critical questions, such as were high-value assets compromised? Were any data altered?

**Henry Kayiza**

Assistant Commissioner

Cyber Crime Unit, Uganda Police

**In your opinion, what was the key cyber security issue facing your country/Africa, what is being done to address this issue?**

Yes, indeed.

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

- The Laws are relatively new and have been already challenged in the Constitutional court (e.g. the computer misuse act was challenged in UG vs. Dr.Stella Nyanzi among others)
- Limited knowledge about cybercrime / security
- Technological advancement is good but criminals are taking advantage. It's easier to commit 'old crimes' such as fraud

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

- Public – private partnerships are vital to carryout awareness campaigns.
- Improve on the laws to close the gaps that criminals are taking advantage of.
- Increase expenditure on information systems security.

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

- I don't think so because most of the cases I have handled, the companies use third vendor system products which can also be accessed by criminals to analyse them and capitalise on their vulnerabilities to commit crime where they are being used.
- Private sector businesses tend to spend less on I.T security so as to as to minimise costs in the short run but end up losing more in the long run.

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

- The financial gain is high and it comes with less physical danger
- The anonymity that comes with the Internet makes criminals feel more secure when committing the crime.
- Cybercrime in its nature is not hampered by physical borders or territorial jurisdictions.
- Malice
- Espionage
- Egoism

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

Yes there are laws in Uganda:-

- Computer Misuse Act
- Electronic Signatures Act
- Lawful Interception Act

There are also government parastatals in place:-

- NITA-U
- UCC

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

Yes. Several individuals, companies, banks, NGOs, Service Providers and including government ministries have all reported to us cases such as electronic fraud, impersonations, defamations, unlawful access hacking and pyramid scheme scheme fraud.

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

Yes most of the cases are reported and prosecuted; however financial institutions tend to hide their cases preferring 'the insurance solution' to reimburse their client victims so as not to alarm their other clients.

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

The best approach is a combined approach, partnerships such as international, regional, governmental, public and private are very vital and should be emphasized to fight this new trend of crime which is increasing at an alarming rate not only in Africa but globally as well. No one can fight Cyber crime as a single entity.

## According to you, what is the most affected sector in the country regarding cyber crime?

When you say 'most affected', it sounds relative because you have to consider two things:-

- In terms of amounts involved
- In terms of number cases (quantity)

Therefore according to my experience; I have cases of banks, service providers (mobile money platforms), government ministries, NGOs as having most affected in terms of the huge sums of money they lose annually. Then individuals and savings groups have lost more in terms of the number of cases reported and when summed up they also make huge amounts of losses.

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

- Enact and harmonise laws on cybercrime across the Continent borrowing from more advanced countries in the World but domesticating them to the local situations.
- MOUs for cooperation among countries should be established. This is because cybercrime cuts across borders/territories and jurisdictions.
- Invest more resources on training cyber security and investigation experts.
- Public and Private Organisations to intensify awareness campaigns.
- Investment should be increased in securing I.T systems.

# Cyber Intelligence Statistics, Analysis, & Trends

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.

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

Project Honeypot Intelligence Analysis

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

# Cyber Attack Timeline

2017

FEB

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

Makerere system hacked, 50 students deleted from 2017 graduation list

MAR

Man charged with hacking KRA and causing Sh4b loss

Man suspected of hacking into Safaricom's systems

Ministry of Finance, Uganda website hacked impacting service delivery

APR

Detectives link Ugandan Ronnie Nsale to Kenyan IEBC hacking

Alleged hacking of JAMB website

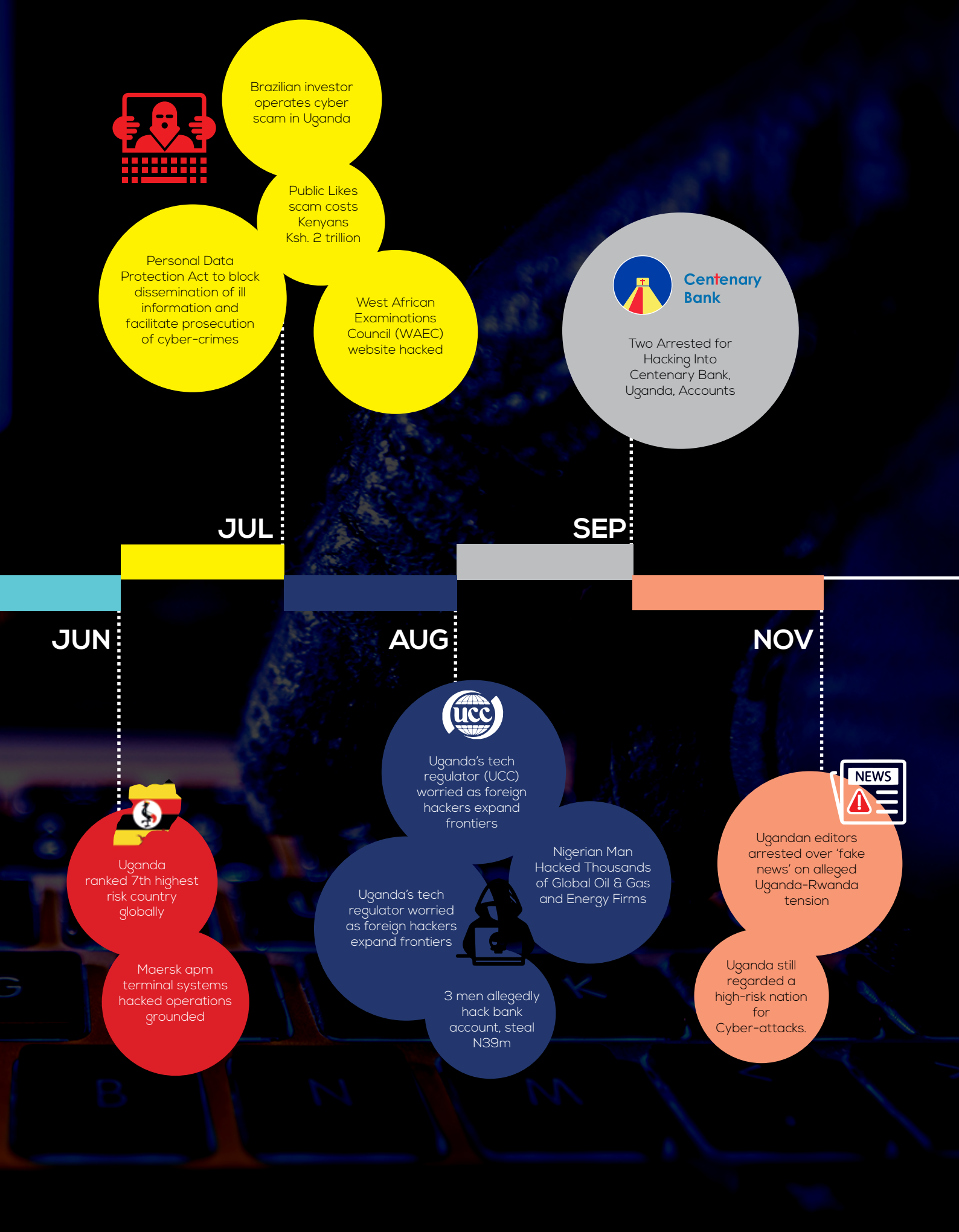
All Not So Quiet On the Business Front As Cyber Crime Slowly Takes Shape

Cyber- bullying to earn you 10 years in prison

MAY

Bank of Uganda warns of Cyber-attacks in commercial Banks

Kenya bans 'Blue Whale Challenge' after Nairobi teen suicide


Brazilian investor operates cyber scam in Uganda
Public Likes scam costs Kenyans Ksh. 2 trillion
Personal Data Protection Act to block dissemination of ill information and facilitate prosecution of cyber-crimes
West African Examinations Council (WAEC) website hacked
Centenary Bank
Two Arrested for Hacking Into Centenary Bank, Uganda, Accounts
JUL
SEP
JUN
AUG
NOV
Uganda's tech regulator (UCC) worried as foreign hackers expand frontiers
Uganda ranked 7th highest risk country globally
Nigerian Man Hacked Thousands of Global Oil & Gas and Energy Firms
Uganda's tech regulator worried as foreign hackers expand frontiers
Maersk apm terminal systems hacked operations grounded
3 men allegedly hack bank account, steal N39m
NEWS
Ugandan editors arrested over 'fake news' on alleged Uganda-Rwanda tension
Uganda still regarded a high-risk nation for Cyber-attacks.

**Ibrahim Lamorde**

Commissioner of Police,
Special Fraud Unit

Lagos, Nigeria

### What is fake news?

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

### How did fake news become such a big problem?

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

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

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

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

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

### What will ultimately get brands to fight fake news?

Public apathy, consumer resistance and mass platform boycott.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**What are some of the pros?**

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

**Why is ransomware so effective?**

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

We believe that ransomeware attacks in Nigeria are grossly under reported.

**What is the possible impact of Ransomware?**

Financial and personal data loss.

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

No.

**How often do you transact using your mobile phone?**

Rarely.

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

No.

**Why does the cyber skills shortage need immediate attention?**

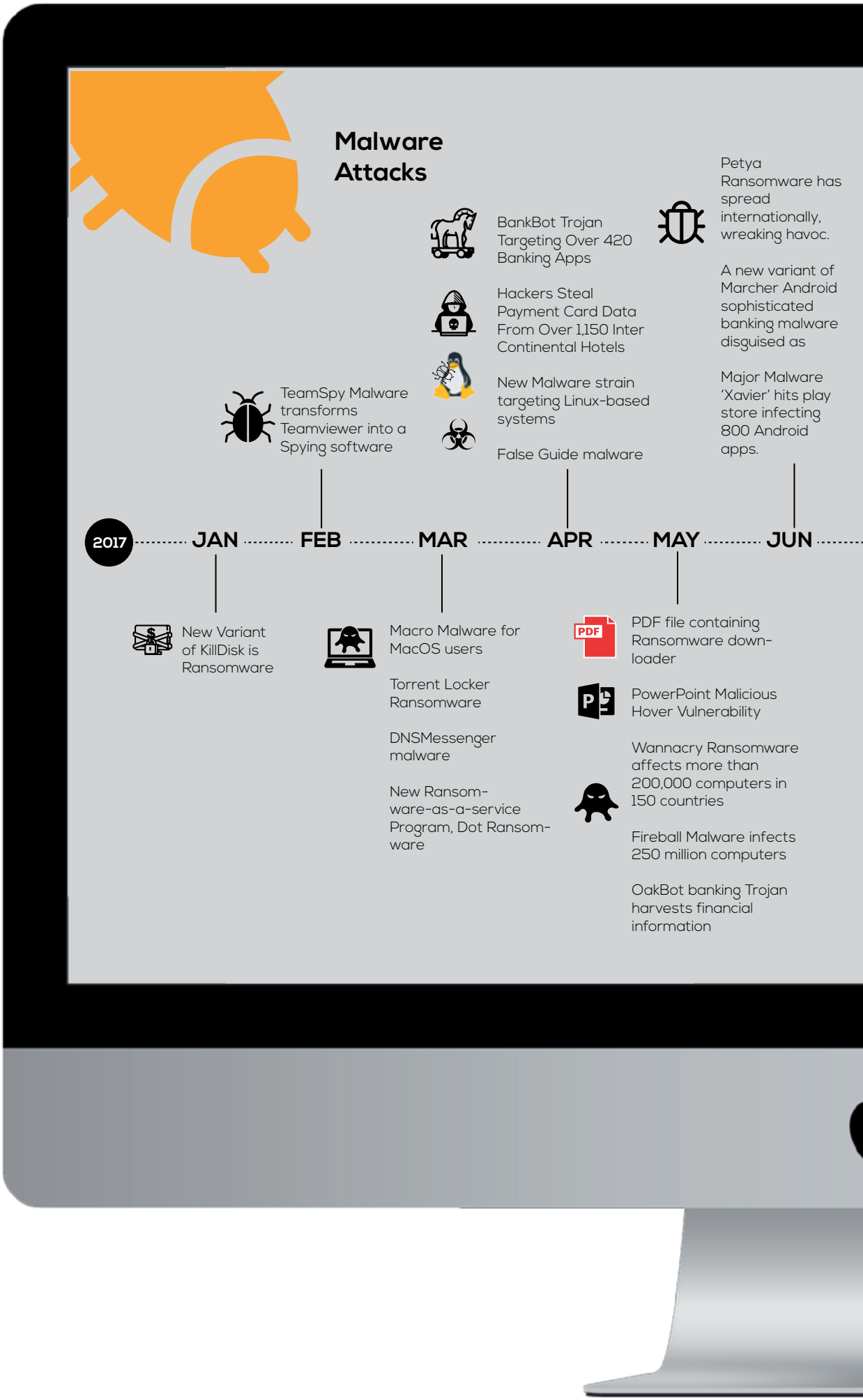
For law enforcement, critical mass is urgently needed to design vital disruption, intelligence, investigation and public education strategies, as well as criminal databases archiving.

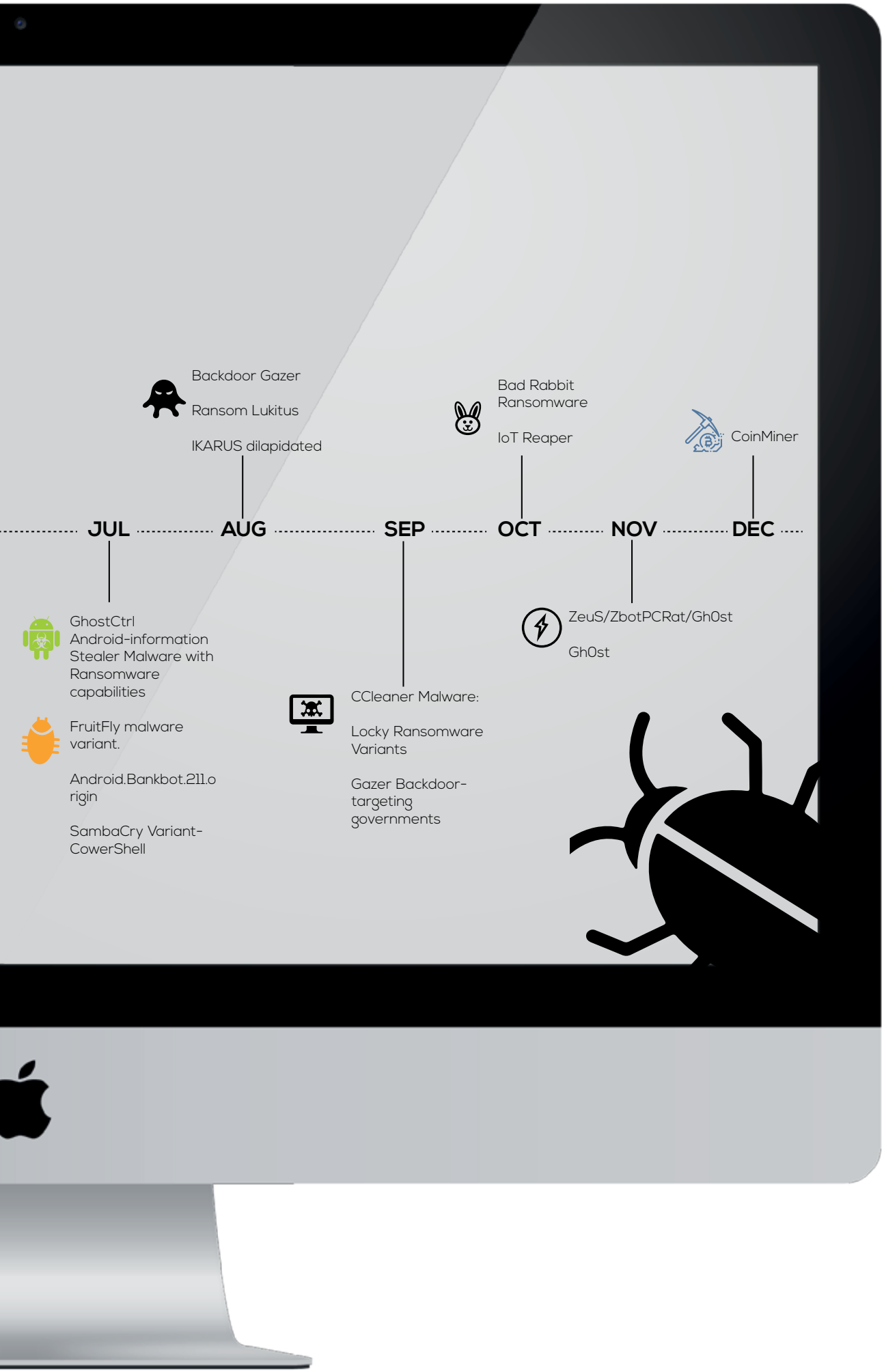
**How many unfilled security jobs are estimated to exist today?**

Unknown.

**How does collaboration help enrich the students' learning?**

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


Malware Attacks
2017
JAN
FEB
MAR
APR
MAY
JUN
New Variant of KillDisk is Ransomware
TeamSpy Malware transforms Teamviewer into a Spying software
Macro Malware for MacOS users
Torrent Locker Ransomware
DNSMessenger malware
New Ransom-ware-as-a-service Program, Dot Ransom-ware
BankBot Trojan Targeting Over 420 Banking Apps
Hackers Steal Payment Card Data From Over 1,150 Inter Continental Hotels
New Malware strain targeting Linux-based systems
False Guide malware
PDF file containing Ransomware down-loader
PDF
PowerPoint Malicious Hover Vulnerability
Wannacry Ransomware affects more than 200,000 computers in 150 countries
Fireball Malware infects 250 million computers
OakBot banking Trojan harvests financial information
Petya Ransomware has spread internationally, wreaking havoc.
A new variant of Marcher Android sophisticated banking malware disguised as
Major Malware 'Xavier' hits play store infecting 800 Android apps.


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

**John Ayora**

Director, Information Systems Security

Bank of Africa Group

Senegal

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

- Attack on SWIFT Money Transfer System
- Ransomware Attacks
- Fake News

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

Yes.

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

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

Yes.

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

Users should use traditional methods like Radio and Newspapers for news verification. While online, users can follow news especially on the verified accounts.

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

The e-services have made service delivery quicker. However, many African nations are still not very well covered technologically. Privacy is a major concern especially when the e-systems are hacked. Many governments have not invested in proper security solutions thereby putting the citizenry data at risk of data breaches.

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

Yes.

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

We had several cases of Ransomware attacks across our subsidiaries. Directors were the main targets. We carried out user awareness programs, upgraded and updated the Windows OS, applied patches issued by Microsoft and issued each director with an external hard drive to back up their data. For the affected ones, we did not recover the data as we didn't pay the ransomware. We simply issued new computers to the affected individuals.

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

User awareness is key. Organisations and users need to carry out patching as soon as critical vulnerabilities are discovered and patches issued. It is also important that users have effective Anti-malware applications.

**Do you think organisations are spending enough money on combating cyber-crime?**

No.

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

Organisations view security solutions as an expense with no real return on investment and this is where the problem lies. Security

solutions are an investment that is put in place to protect the organisation's key resources and properties.

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

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

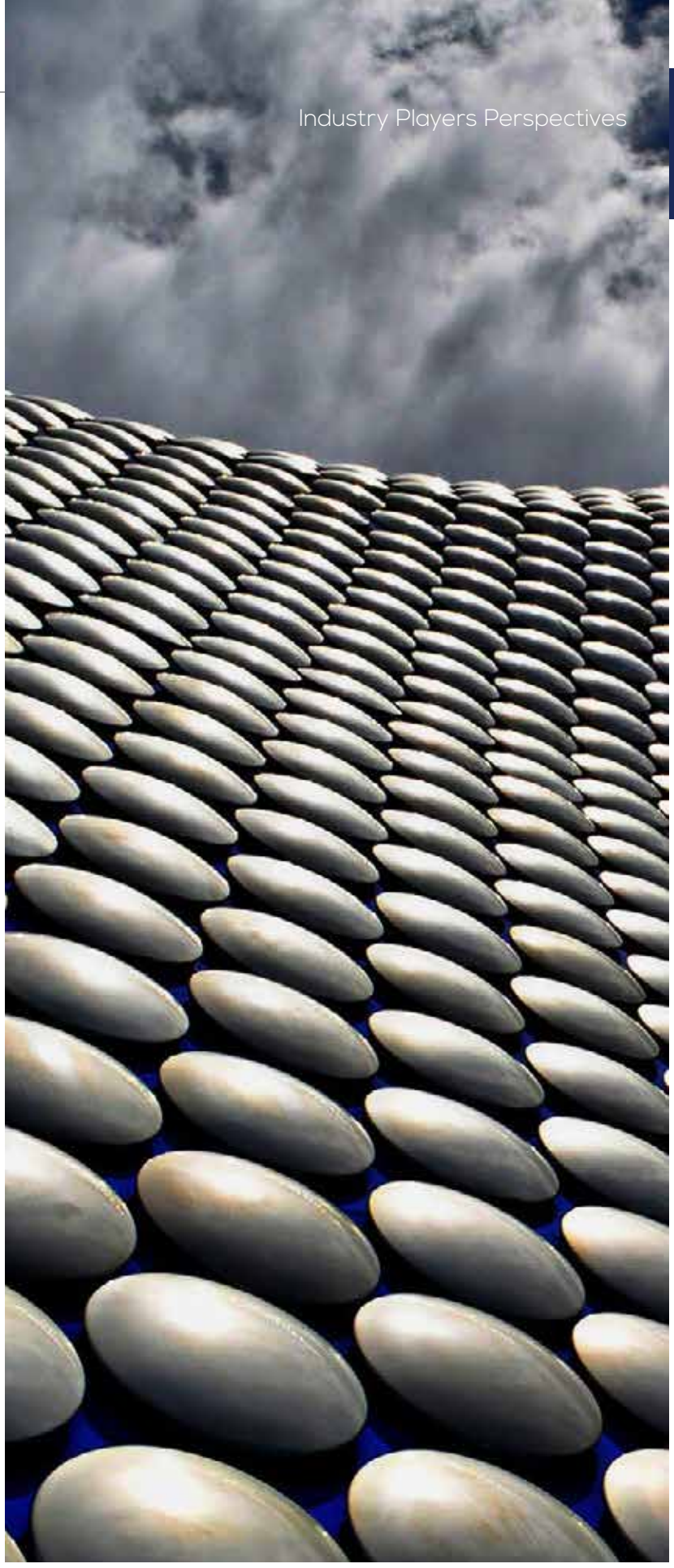
- Invest in up to date research centers and labs
- Send students and researchers for exchange programs across various countries.

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

The private sector and consumers should give an opportunity to the African Grown Cyber-security products in their sectors.

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

- Invest in user training and awareness programs
- Update and or upgrade outdated systems, especially the non-supported Microsoft Systems
- Invest in effective Cyber security products and solutions.



# Threat Intelligence

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

We broke down the findings into the following sections:

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

## Open Ports

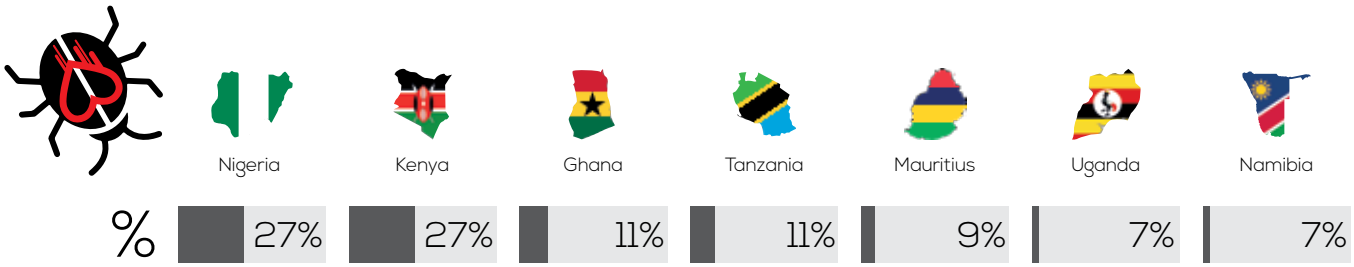
There is a total of 65,535 TCP ports and another 65,535 UDP ports, we examined risky network ports based on related applications, vulnerabilities, and attacks.


| TCP PORTS | Kenya | Tanzania | Ghana | Uganda | Nigeria | Namibia | Mauritius |
|---|---|---|---|---|---|---|---|
| Port 80 | 29% | 28% | 24% | 22% | 29% | 23% | 26% |
| Port 23 | 19% | 13% | 6% | 16% | 10% | 6% | 9% |
| Port 443 | 18% | 18% | 15% | 15% | 16% | 20% | 20% |
| Port 8080 | 3% | 9% | 4% | 3% | 2% | 3% | 2% |
| Port 22 | 14% | 15% | 12% | 10% | 10% | 18% | 16% |
| Port 21 | 6% | 7% | 10% | 4% | 6% | 11% | 12% |
| Port 53 | 4% | 3% | 4% | 18% | 3% | 5% | 5% |
| Port 445 | 1% | 1% | 3% | 3% | 2% | 3% | 2% |
| Port 135 | 1% | 2% | 3% | 3% | 2% | 3% | 4% |
| Port 25 | 3% | 2% | 1% | 4% | 10% | 5% | 2% |
| Port 110 | 2% | 2% | 1% | 2% | 10% | 3% | 2% |

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

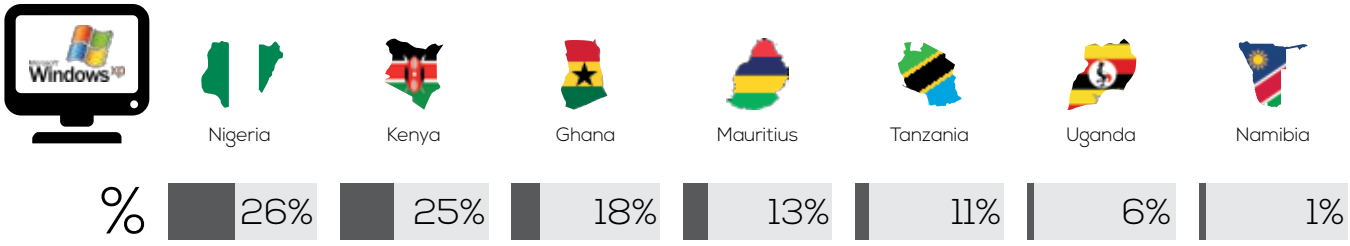
## Heartbleed Vulnerability

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.




## Vulnerable OS

A computer running XP today is a castle with doors flung open. Microsoft first introduced in 2001 and hasn't supported since 2014. Hackers have targeted XP for years. Its lack of defenses and persistent popularity make it a popular target.

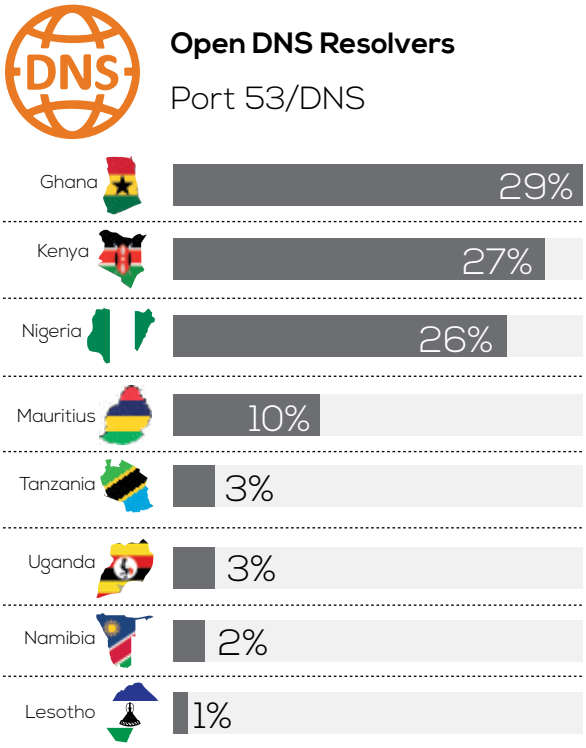


## Web Defacements in 2016 and 2017

Nigeria was the most affected by web defacement in 2017

| | '16 | '17 | %change |
|---|---|---|---|
| Kenya | 38% | 11% | -28% |
| Nigeria | 11% | 23% | 12% |
| Ghana | 2% | 7% | 5% |
| Tanzania | 17% | 5% | -12% |
| Uganda | 11% | 23% | 12% |
| Mauritius | 2% | 1% | 1% |
| Namibia | 12% | 18% | 6% |
| Lesotho | 2% | 2% | -1% |
| Ethiopia | 2% | 2% | 4% |
| Rwanda | 2% | 3% | 1% |

## Open DNS Resolvers




Why is an Open DNS resolver a bad thing?

An Open DNS Resolver is any DNS resolver that is publicly accessible, and willing to resolve recursive queries for anyone on the internet. While this sounds like the good Samaritan thing to do, the DNS protocol is one of a few that can turn a very small query into a large response (in both size, and required computing power). Because of this, having an open resolver opens your server up to be used in DNS Amplification Attacks.

**Shimelis Gebremedhin Kassa**

CISA, MSCS, CEH - General Manager

MASSK Consulting PLC

Ethiopia

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

No formal information or statistics are available. However, based on the informal information that I receive and my personal experience, the impact of cyber security is crippling.

The following are issues that we faced in 2017:

- Compromise or misuse of personal and companies files/data due to malwares, Worms, viruses etc
- Individuals personal information theft (like copy of films, music, book etc)
- Insiders attack attempted on some financial institutions of the country in collaboration with outsiders.
- We are aware of the ransom ware attacks which happened during May 2017,though did not impact our country.

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

Yes, to some extent.

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

Actually, depending on the situation, everyone would bear the responsibility. End users are usually responsible for the creation and distribution of fake news, government, Media and ISPs will take second degree responsibility in relation to stopping the distribution.

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

In our case, regulators do not have direct influence on these sites. However, they can report such cases to the platform owners (Google/Facebook) who in turn have the ability to remove the fake news. It is also possible to use filters and different technologies that can assist in fixing this issue.

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

I think the main solution is enhancing awareness using different mechanisms like radio, TV's, journals, magazine, telephone SMS etc both by government and private organisations. In addition, for highly susceptible and sensitive organisations like financial industries, airlines, medical centers etc, the government/regulators should set some enforcement to create regular awareness on how to use their products by customers/ end users.

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

Consuming and utilizing these systems without considering the risk of security, fraud and privacy issues is not praiseworthy. Organisations often rush to implement complex technologies without considering the Cyber security risks present. As a result, most of these projects tend to be exploited by Cyber attackers to commit fraud.

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

Most of the African countries including Ethiopia are now moving to E-services without considering the security gaps and attack vectors such as denial of service, disruption, loss of critical customers, loss of confidential information and loss of user interest in general. A good example is the dissatisfaction created by school net and woreda net e-service projects.

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

NO, we were not affected directly. This is because of a number of reasons key being lack of e-commerce, credit card facilities and the strict financial policy that we have.

Also, banks have enforced a number of controls that ensure loss of money is reduced. For example the Limited amount of fund transfer/withdrawal which was enforced. It was made mandatory that users had to inform the central bank to withdraw more than 7,500USD/200,000ETB, lengthening authorization process. Limits were also set such that it's only possible to withdraw from ATM terminals a maximum of 10,000ETB/370USD.

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

- Need to create strong collaboration between professionals throughout Africa.
- Establish professional security associations to defend security issues together and share experiences
- Create current status security awareness frequently through publications like Serianu's journal (Africans Cyber Security Report).

**Do you think organisations are spending enough money on combating cyber-crime?**

No, most organisations invest a lot on technology implementation without considering the security aspect.

**Based on our research the Africa cyber security market will be worth USD 2 billion dollars by 2020. Despite this opportunity, Africa has not produced a single commercially viable cyber security product or solution.**

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

Cyber security is a global issue and no country/continent (Africa, Asia, Europe or America) can manage on their own. We need to collaborate. Also, Cyber security not only requires knowledge but also skill, talent and interest. So, engaging youngsters and kids will improve our innovation. Further, government should organize different security innovation competition and encourage private investors in the area.

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

I think Ransomware will get the first attention in African then, DDOS, Social engineering, Email phishing attack will take next priority on 2018.

# 2017 Africa Cyber Security Survey


Africa


**700**
respondents


**12**
Industry Sectors

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

## About the Survey

This survey was prepared based on data collected from a survey of over 700 respondents across organisations in Africa.

This included companies from the following sectors:


Academic


Banking


Cyber Security


Financial Services


Government


Healthcare Services


Insurance


Legal Advisory


Professional Services


Telecommunication

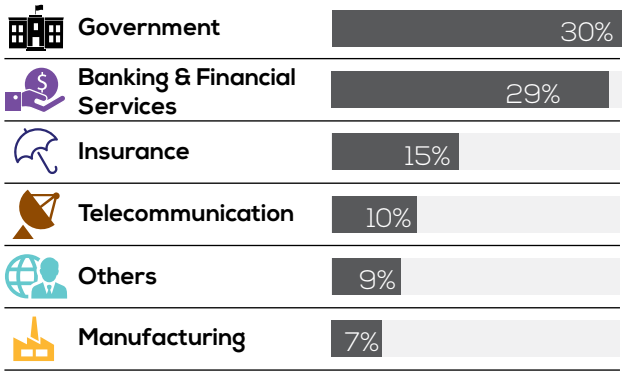

Others

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

## Summary of Findings

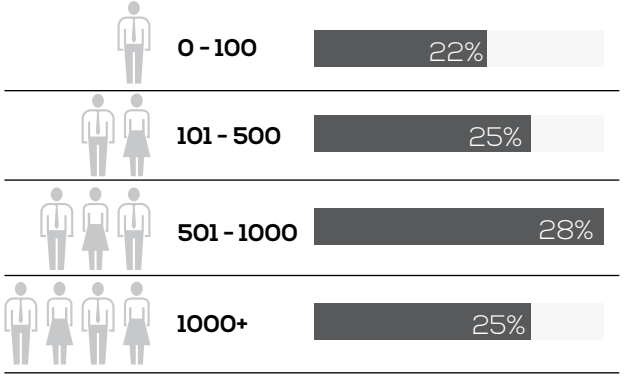
According to the survey findings, 99.4% of respondents have a general understanding of what cybercrime is. With the many advances in information technology and the transition of social and economic interactions from the physical world to cyberspace, it is expected that majority of individuals have a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

### Majority of the respondents were from the government sector




### 25% of the respondents are organisations with 1000+ employees

25% of the respondents are employees of organisations with 1000+ employees




### 62% of the organisations allow the use of IoTs

Organisations that allow/utilize Cloud Services or IoTs Tech **62%**

**58%** lack policies to govern the usage of Cloud Services or IoTs Tech

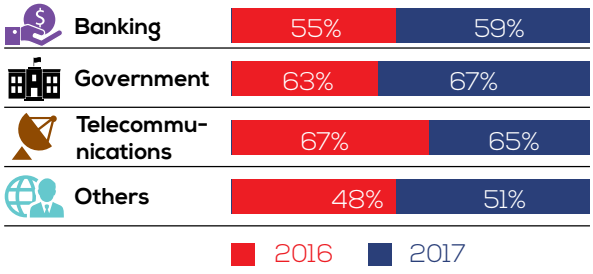
It is paramount that organisations which have adopted cloud and IoT services implement policies and procedures to govern the adoption, maintenance and retirement of these technologies.

### 58% of organisations are concerned about cybercrime

**58%** extremely concerned about cybercrime in their organisation

### The telecommunications sector experienced a 2% decrease of cybercrime in their organisations

there was a relative increase in cyber crime in 2017

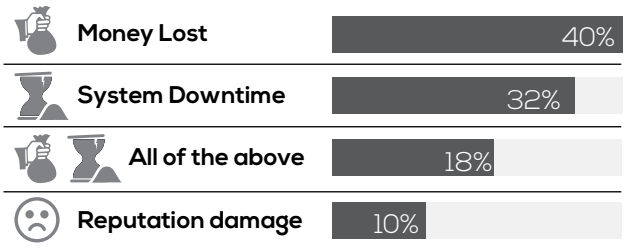


this can be attributed to two main issues:

- Internet penetration in Africa is still low
- majority of people do not understand what qualifies as Cyber-crime. As such, a huge percentage of people lack the ability to recognize a Cyber-attack when it occurs.

### 90% have been impacted by cybercrime

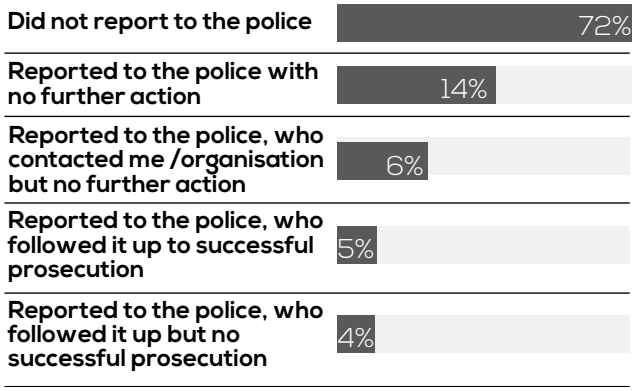
90% of the respondents have had an impact of Cyber crime




Financial institutions, Saccos and organisations that deal with transaction processing are the primary targets for the Cyber-attacks.

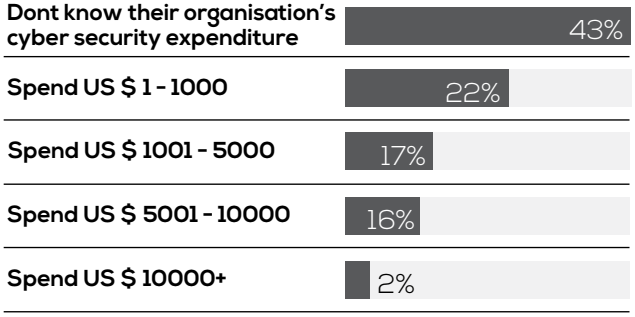
### 72% did not report cybercrime to the authorities

5% Reported cyber crime to the police and followed it through to successfull prosecution



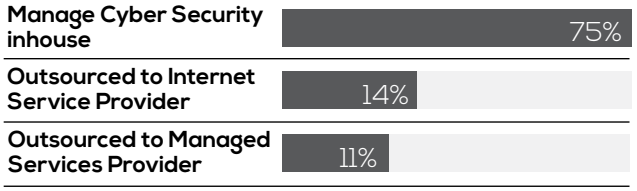

### 90% of organisations spend less than US $10000 annually for cyber security. Majority of these organisations came from the Banking and Financial sectors

90% spend less < US $10000 on cyber security




### 75% of the organisations manage their entire security functions inhouse

25% of the respondents outsource the entire security function for their organisations



## 75% of the organisations do not carry out a combination of security testing techniques

25% of the respondents carry out security testing techniques in their organisations simultaneously

| | |
|---|---|
| Audits | 30% |
| Penetration testing, Vulnerability Assessments and Audits | 25% |
| Vulnerability Assessments | 25% |
| Penetration testing | 20% |

## 15% of the organisations do not train their employees on cyber security isssues

50% of organisations do not have an established Cyber security training program on cyber risks

| | |
|---|---|
| Staff trained yearly | 35% |
| Staff trained only if there is a problem | 35% |
| Staff trained monthly | 15% |
| Staff never trained | 15% |

## 40% of the respondents do not keep upto date with cyber security news

60% of organisations in Africa do not keep up to date with Cyber security trends and attacks

| | |
|---|---|
| I do not keep upto date | 22% |
| Specialised news sources | 18% |
| Generic newspapers and news broadcasters | 16% |
| Social media networks contacts | 15% |
| Outsourced services | 15% |
| Consulting companies | 14% |

## 72% believe that cyber crime has increased in Africa

28% DO NOT think that cyber crime has increased in Africa

| | |
|---|---|
| Has increased in the last year | 72% |
| Has not changed since last year | 15% |
| Not much of an issue | 9% |
| Has reduced in the past year | 4% |

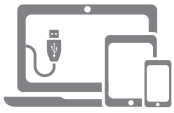
## 66% of the respondents do not believe that cyber crime is rooted in technology

34% of the respondents believed cyber crime is rooted in technology

| | |
|---|---|
| Technology | 34% |
| Security Education | 22% |
| Economic Interests (Financial gain) | 17% |
| Business Competition Sabotage, IP theft | 15% |
| Lack of Intergrity (Corruption) | 12% |

## 59% of organisations have a best practise policy for BYOD

41% of organisations allow the use of Bring Your Own Devices



while

59% of the respondents have a best practice policy for BYOD in their oganistions

**John Sergon**

Ag, Chief Executive Officer

ICT Authority

Kenya

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

We saw attacks on systems in general, Information theft especially from the financial institutions and hackers going ahead to use this information to further cybercrime.

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

It is an issue in this country. Social media news is very versatile we seem not to be ready for it. It is hard to tell the source a lot of times. The fake news "industry" growing and wanting to be felt.

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

Every organisation should have a responsibility to counter fake news seen on social media that regards them. Fake news is actually a threat to organisations that users need to learn how to identify.

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

Regulators should put responsibility on these platforms for accountability and to ability to follow up on custodians on these platforms who should be accountable for the content they post. Regulators should put in place mechanisms to know from these platforms to know who these people are.

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

All institutions should have general user awareness on issues that impact them through the society. They should be taught how to identify fake news.

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

**People have adapted to using these systems. However, the rapid use has been without the thought, is my data safe?**

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

There are risks but people trust the government with their data.

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

No. We were not impacted, but there were reports of attacks elsewhere.

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

Awareness and build capacity be able to deal with such incidences.

**Do you think organisations are spending enough money on combating cyber-crime?**

No. First of all it is very expensive and second they don't know it is an issue to prioritize on.

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

Create awareness for all involved stakeholders as encourage people to push up the agenda of why investing in cyber security is important.

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

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

Putting in more effort in research and development and allocating resources for this. Already existing innovation centers should also dedicate resources solely for cyber security research and development, say a lab solely for cyber security practice.

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

As local consumers it is our responsibility to "Buy Kenya, Grow kenya". The government also needs to encourage local players through policies to ensure there is a capacity to produce local cyber security solutions.

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

I am not in a positions to fully comment on this, but I believe going forward there needs to be frameworks through government to private sector that cut through the cyber security space.

Cyber security is an area we cannot ignore anymore, and since technology is always growing, people need to always catch up cyber security wise.

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

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

## Inter Industry Analysis - Africa

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

* No statistical analysis done in 2016 on this section.

**Baidy Sy**

Associate Director

Digital Transformation and Cybersecurity Lead of Finetech Groupe

Senegal

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

Senegalese companies seldom share the Cyber security issues that they face. The rare cases known to the general public are those on whom legal action has been taken and for which media is aware.

Of these cases we can mention the case of a high school student named Assane Lopy charged for fraudulent intrusion into bank accounts.

In early 2017, one of the major banks in Senegal called CBAO GAWB fell victim to a vast network of cyber criminals aided by an insider that resulted in brand erosion and financial loss.

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

Fake news is currently one of the biggest nuisances of the cyber space, especially in the online press and social networks.

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

First of all there should be a state regulator in-charge of following up and investigating such cases. In Senegal for example, a new press code was voted in the National Assembly this year after eight years of negotiations. One point, in particular, was blocking the discussion: specific measures of deprivation of liberty for press offenders resulting in possible "liberticidal" shift from professionalism. This code also gives rise to better supervision of the online press, as Senegal has more than 200 news sites. Most online sites tend to pick information from other media - without citing them. Others simply broadcast "fake news" and unsubstantiated rumors.

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

We need more campaigns that incorporate Cyber awareness from as early as primary and secondary school. We also need to create a culture and sense of responsibility by the media and information sector actors.

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

African citizens are actually ready to fully digitize their operations. However, limited knowledge and training has provided opportunities for cyber criminals to exploit vulnerabilities and weaknesses in these digitized platforms. Most of the crimes committed against these systems include data leakage, defacement and fraud.

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

During the WannaCry attack, Senegal was affected 4 hours after the first case was detected. As mentioned earlier, it is possible many more companies were affected but due to the low rate of information sharing, many did not report.

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

Beyond the skills, African countries should invest more in raising awareness and training end-users who are, as always, the weakest link of the chain. Offline backups, Disaster Recovering Plan and Business Continuity Plan are also important.

**Do you think organisations are spending enough money on combating cyber-crime?**

Not enough unfortunately.

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

Train security managers and directors.

Educate the technical teams on how to communicate to the Board of Directors to show return on investment for Cyber Security spending.

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

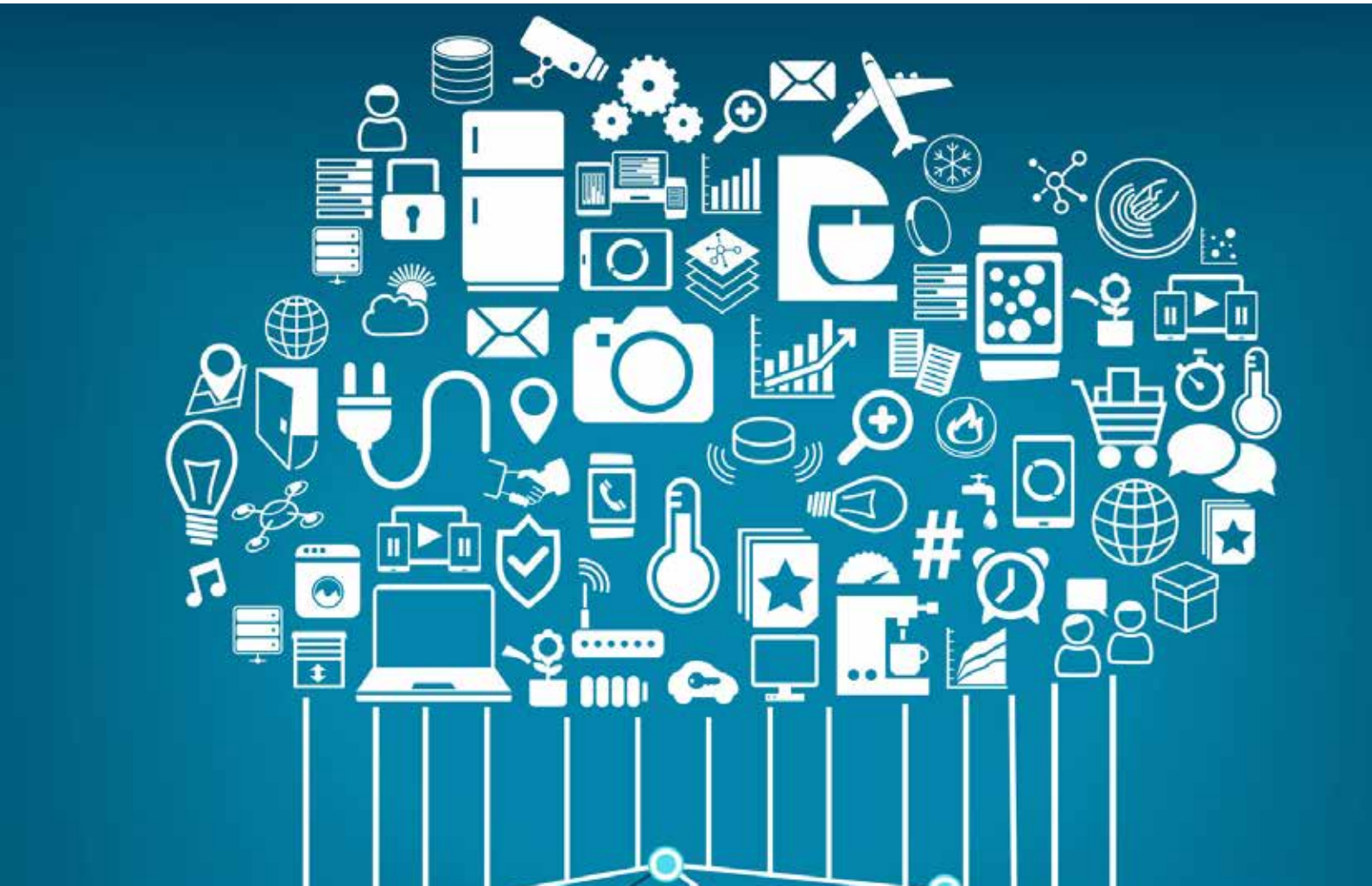
**In your opinion, what should African countries or universities focus on to encourage innovation in the development of Cyber security solutions?**

In my opinion, African countries must invest in university training and research centers specializing in Cyber security. They also need to develop national cyber security cultures.

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

The top 2018 cyber security priorities for African countries are to:

- define a national cyber security plan.
- create a national cyber security agency.
- set up a national CERT (Computer Emergency Response Team).
- identify and protect national critical infrastructure.
- awareness and training.



## Inter Country Analysis - Africa

| Country | Kenya | Uganda | Tanzania | Nigeria | Ghana |
|---|---|---|---|---|---|
| % of organisations who Conduct Regular Training of Employees | 64% | 60% | 55% | 50% | 55% |
| % of organisations who allow Bring Your Own Devices (BYODs) usage | 73% | 62% | 67% | 65% | 67% |
| % of organisations who lack BYOD policy | 48% | 58% | 60% | 50% | 58% |
| % of people who have experienced cyber crime | 72% | 40% | 32% | 80% | 30% |
| % of successful prosecutions per country | 11% | 4% | 6% | 4% | 4% |
| % of organisations who have Zero (0) budget allocation for cyber security products | 10% | 15% | 13% | 43% | 43% |

## Trend Analysis - Africa

| Country | Kenya | | Nigeria | | Ghana | | Tanzania | | Uganda | |
|---|---|---|---|---|---|---|---|---|---|---|
| Year | '16 | '17 | '16 | '17 | '16 | '17 | '16 | '17 | '16 | '17 |
| % of organisations who Conduct Regular Training of Employees | 58% ↑ | 64% | 40% ↑ | 50% | 48% ↑ | 55% | 45% ↑ | 55% | * | 60% |
| % of organisations who allow Bring Your Own Devices (BYODs) usage | 62% ↑ | 73% | 56% ↑ | 65% | 61% ↑ | 67% | 56% ↑ | 67% | * | 62% |
| % of organisations who lack BYOD policy | 49% ↓ | 48% | 53% ↓ | 50% | 59% ↓ | 58% | 61% ↓ | 60% | * | 58% |
| % of people who have experienced cyber crime | 71% ↑ | 72% | 37% ↑ | 80% | 20% ↑ | 30% | 64% ↓ | 32% | * | 40% |
| % of successful prosecutions per country | 3% ↑ | 11% | 7% ↓ | 4% | 1% ↑ | 4% | 9% ↓ | 6% | * | 4% |
| % of organisations who have Zero (0) budget allocation for cyber security products | 6% ↑ | 10% | 41% ↑ | 43% | 42% ↑ | 43% | 11% ↑ | 13% | * | 15% |

* No statistical analysis done in 2016 on this section.

**Ben Roberts**

Chief Technical Officer

Liquid Telecom Group

Kenya

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

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

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

Yes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Do you think organisations are spending enough money on combating cyber-crime and what can be done to encourage more spending on cyber security issues?**

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

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

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

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

I would refute that statement.

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

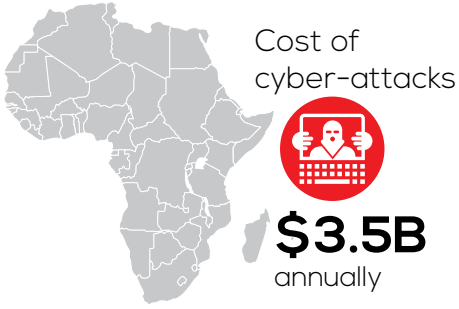
**In your opinion and from an African context, what are the top 2018 cyber security priorities for African countries and organisations?**

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

# Cost of Cyber Crime

## Estimating the Cost of Cyber Crime for the Countries in Scope

AS INTERNET AND DEVICE 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 $3.5 Billion. Further analysis of cost of Cybercrime for the countries; Nigeria, Kenya, Ghana, Uganda and Tanzania was estimated at $1.078 Billion 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 crimes unique to electronic networks, e.g. attacks against information systems, denial of service and hacking.

A significant proportion of the $ 1.08 Billion losses is attributed to insider threats, which we estimate at $216 Million (50% of all direct costs) and $352 Million (33% 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:

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

## Total Cost of cyber attacks

Cost of cyber-attacks

**$1.078B**
annually

| | | |
|---|---|---|
| **Direct Cost** | $431 Million | 40% |
| **Indirect Cost** | $647 Million | 60% |

## Breakdown of Indirect Cost of cyber attacks

$647 Million

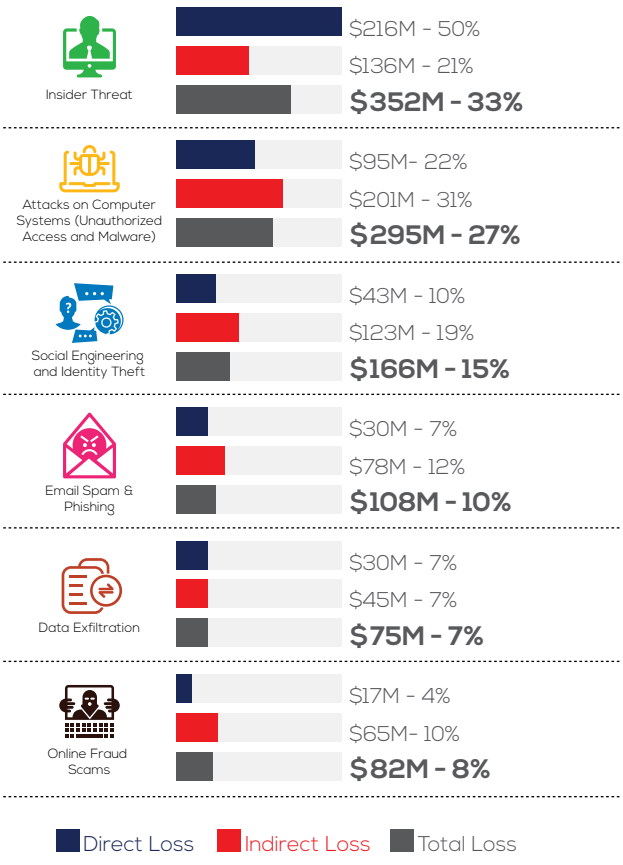
| | | |
|---|---|---|
| **Technical Controls** | 46% | **$304M** |
| **Security Consulting Services** | 22% | **$142M** |
| **Loss of trust in e-services** | 16% | **$103M** |
| **Training** | 11% | **$71M** |
| **Reputational Damage** | 3% | **$19M** |
| **Insurance and Compliance Costs** | 1% | **$6M** |

## Breakdown of Direct Cost of cyber attacks

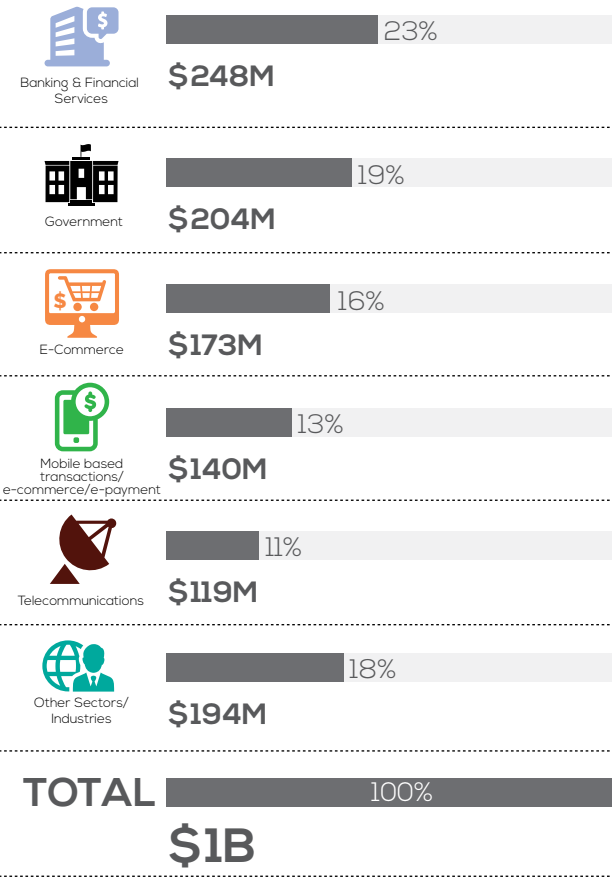
$431 Million

| | | |
|---|---|---|
| **Compensations to Victims of Breaches** | 43% | **$185M** |
| **Money withdrawn from victim accounts** | 43% | **$185M** |
| **Investigation and Remediation Costs** | 14% | **$61M** |

## Types of Cyber Crime by Cost



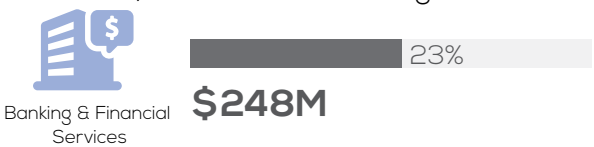
## Cyber crime cost for Industry Analysis




## 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 of Cyber crime to Banking Sector




**Type of cost**: Direct/indirect costs.

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

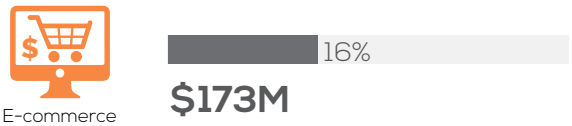
### Cost of Cyber crime to African Governments


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




Type of cost: Direct cost

1. Online fraud
2. Credit card fraud
3. Social Engineering

## Cost of Cyber crime to mobile based transactions

Mobile based transactions/ e-commerce/e-payment

13%

**$140M**

**Type of cost:** Direct consequence of cybercrime. These were:

1. SIM Card Swiping
2. Social Engineering
3. Insider Fraud

## Cost of Cyber crime to Telecommunication Sector

Telecommunication

11%

**$119M**

**Type of cost:** Direct/Indirect cost

1. Advanced Persistent threats
2. Spam
3. DoS

## Cost of Cyber crime to other sectors

Other Sectors/ Industries

18%

**$194M**

**Source**: Information from budget declarations, investments analysis and interviews with aviation experts.

**Type of Cost:** Costs in anticipation of cybercrime, such as:

1. Antivirus software and endpoint protection
2. Cyber insurance,
3. Adoption of NED (network extension device) solutions
4. Applying encryption standards
5. Securing communication technologies such as the flight management system (FMS).

**Arnold Mangeni**

Director, Information Security

National Information Technology Authority Uganda (NITA-U)

Uganda

**Do you think Cyber security is a major problem in Uganda/Africa?**

Yes.

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

Yes, Cyber security is a major problem in Africa in general and Uganda in particular.

The main causes of the cyber security problem are;

- Governance. In Uganda's public sector cyber security is still not on the agenda of top management. There is lack of accountability for and treatment of cyber security as a corporate – level risk. There are no personnel with cyber security responsibilities and majority of end users lack adequate awareness, education as well as training.
- Institutions lack cyber security strategizes and policies to guide matters cyber security. Security incidents are not reported both internally and externally. Cybersecurity is more reactive than proactive.
- There is inadequate skilled cyber security professionals to continually meet the cyber security needs in the country
- Inadequate risk assessment and compliance of organisations

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

4. First and foremost at the heart of improving the situational awareness in the country has been the National Information Security Framework (NISF). A framework that places cyber security at the top of the agenda of top management. Organisations, must assume accountability for and treat information security as a corporate – level risk.

Ultimately the NISF seeks to achieve the following amongst others;

i. Provide a conceptual structure for guiding information security activities

ii. Provide a common risk based approach for addressing information security issues

iii. Secure Government of Uganda information and other assets

iv. Improve understanding of information security risk, roles and responsibilities

v. Guarantee information security compliance by critical national information infrastructure operators

vi. Improve information security governance and the environment

The framework encompasses the domains of Governance, Information security, Physical security and personnel security. Below is a brief on what each domain addresses;

i. Governance; Structures must be created to enable people perform specified roles and responsibilities. The first step, thus, is to ensure that organisations create clear structures to enable staff at all levels to perform information security & risk roles effectively.

ii. Information Security; Organisations must protect both the information they handle internally and that which they share with external partners. Assuring the confidentiality, integrity and availability of information is a corporate-level concern because security incidents threaten organisational reputations, legal positions and the ability to conduct business operations.

iii. Personnel Security; Employees are the most important asset for any organisation. However, staff could also be potent threat sources and actors. Indeed, changes in national information security policies worldwide have roots in high-profile accidental and deliberate disclosures of sensitive national security and personal information. Therefore, it is vital to reduce the likelihood of staff exploiting legitimate access to critical infrastructure facilities, sites, information and staff for unauthorised use. Personnel security is important in the context of defending the cyber supply chain against State and industrial espionage threats.

iv. Physical Security; Managing unauthorised physical access, damage, and interference to information, premises and resources by a range of physical security threats including crime, espionage, natural disasters and acts of terrorism, must be of paramount importance to organisations. Physical security also protects personnel against violence and other sorts of harm.

5. Education, training and awareness sessions are routinely being carried out. Plans are underway to carry out massive nationwide awareness and training for the Financial Year 17/18.

6. Adoption of the National Cyber Security Strategy (NCSS) which has been drafted following the revision of the National Information Security Strategy (NISS). The NISS was implemented in 2011, to address matters of Information Security. Currently the NISS has been revised to establish the NCSS. The guiding principles for the National Cyber Security Strategy include but are not limited to the following:

   i. Enhancing private public partnership in development of cyber security capacity;

   ii. Ensuring trust and confidence of citizens in the use of Information Technology enabled services;

   iii. Taking into consideration international collaboration due to the borderless nature of cyber space;

   iv. Promoting a culture of cyber security across all levels of society;

   v. Promoting continuous improvement in cyber security and;

   vi. Promoting responsibility and action amongst CII operators as regards Cyber Security readiness.

7. Utilize the national Computer Emergency Response Team / Co-ordination Center (CERT / CC) (established in 2014) to:

   i. Ensure the protection of the nation's Critical Information Infrastructures through incident management amongst other measures;

   ii. Assist in drafting the overall plan on the country's approach to cyber security related issues; and

   iii. Serve as a focal point for further building and implementing the National Culture of Cyber security.

The National CERT/CC is complimented with sub sector CERTs to cater for constituents that have unique requirements for example, the communications and telecom sector.

8. Make the most out of our international and regional collaboration on cyber security with a number of liked minded organisations and governments. These include; Korea Internet Security Agency (KISA), the Government of Estonia, International Security Forum (ISF), Global Forum on Cyber Expertise (GFCE) , amongst others. Out of these collaborations is skilling of our information security professionals, technical support, information sharing, amongst other benefits.

9. Maximize the benefits from the National Information Security Advisory Group (NISAG), whose mandate is to advise, protect and respond to the nation's critical infrastructure, we are achieving collaboration with the private sector who run majority of the nation's critical infrastructure. This ensures robust Cybersecurity implementations.

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

Naturally, the private sector investment is guided by amongst others, the principal of return on Investment (ROI). In the private sector, security professionals are still struggling to demonstrate business value of investment in security to senior management. Management would be more willing to deal with consequences than mitigations. This is heavily affecting private sector investment in cyber security.

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

i. Monetary gain; like is the case with many crimes committed outside the internet, financial gain is a big motivator for many cyber criminals. Case in point; the

Ransomware attackers that were asking for payment in Bitcoin, banking systems that are hacked into.

ii. Hacktivism; activists have increasingly taken to breaking into computer systems demonstrate for political or social causes.

iii. Industrial Espionage; illegally and unethically obtaining confidential information from competitors with the intention of using the said information to gain a competitive edge.

iv. State Espionage; State sponsored cyber espionage is becoming a common occurrence and is being used as a form of intelligence gathering.

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

Yes, included among the initiatives is;

1. An Enabling legal and Regulatory environment. Included are the cyber laws;
    a. The Electronic Transactions Act (2011) to make provision for and to regulate the use of electronic signatures, to provide for the use, security, facilitation and regulation of electronic communications and transactions;
    b. The Electronic Signatures Act (2011) to encourage the use of e-Government and to make provision for the safety and security of electronic transactions and information systems; and
    c. The Computer Misuse Act (2011) to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment.
2. National Information Security Advisory Group (NISAG). This NISAG encourages collaboration between public and private stakeholders to ensure robust Cybersecurity is implementated.
3. The National Information Security Framework (NISF) with its 6 security standards;
    a. SS1 - Technical Risk Assessment
    b. SS2 – Risk Management & Accreditation
    c. SS3 – Security Classification
    d. SS4 – Personnel Security
    e. SS5 – Physical Security
    f. SS6- Incident Management

The NISF incorporates risk management as a delivery area within the executive management (both public and private enterprises) provides a strong foundation for cyber security implementation covering the areas of people, process and technology.

4. Capacity development on the application of the cyber laws for both investigating and prosecuting officers. Application of these cyber laws should be guided by adhering to principles of digital forensics as well as chain of custody.
5. Through the CERT/CC Identification and prioritization of key resources is being done. This is aimed at improving the country's security, resilience, operational capacities to effectively manage and respond to cyber incidents as well as protect against ever persistent threats.
6. Establishment of the Uganda Police Cyber Crime Unit, whose is to;
    a. provide enforcement of cyber security related laws
    b. provide efficient cybercrime investigation
    c. ensure collaboration with similar international institutions

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

Yes

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

Yes.

The Computer Misuse Act (2011) has so far been used to prosecute a number of cybercrime cases.

Some Notable case below:

Uganda v. Sentongo & 4 others criminal session case 123 of 2012) [2017] UGHCACD 1 (14 February 2017)

Electronic fraud C/S 19 of the Computer Misuse Act, 2011

Unauthorized disclosure of access codes C/S 17 of the Computer Misuse Act, 2011.

Court ruled that "For an offence to be committed, the disclosure must be unauthorized and likely to cause loss."

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

- Enabling environment. Enact laws and regulations to comprehensively address Cyber issues. This should be reinforced with awareness and

support through initiatives like capacity building for investigating, prosecuting and judicial officers.

- Actively support institutions with a role and mandate to play in the cyber-crime prevention ecosystem. For example, Police, Judiciary, sector regulators. This support can be in form of financial resources or other forms of resources, collaboration, and capacity development.
- Promotion of a culture of good practices like responsible sharing, reporting of incidents, education and awareness, amongst others.
- Encourage and focus on cooperation and collaboration (domestic, regional, and international) amongst the various stakeholders.

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

- Banking and Financial Services
- Telecommunication
- Government

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

- African states need to work closely and directly through the African Union and other regional frameworks to implement enhanced measures for cooperation, mutual assistance and coordination among security agencies, prosecutors and judges.
- A positive step was made during the development of the AU convention on Cyber Security and Data Protection (the Convention) adopted in July 2014. Unfortunately only Senegal has ratified the convention out of the required 15. If ratified this convention will go a long way in the harmonization of the African Cybersecurity policies.
- Harmonization of the cybercrime laws at regional and continental level.
- Establishment of missions to strengthen police and law enforcement capacities in handling, investigating and prosecuting cybercrime.
- Provision of mutual Legal Assistance
  - Collaboration during amongst others:
  - Investigations
  - Prosecutions
  - Capacity building
  - Bench marking
  - Formulation of laws
  - Incident response
- Establishment of regional cyber security centres to address the escalating cyber threats

# Sector Ranking

## Banking

Banks are top on our list of risk by sector. These institutions face two main issues: On one hand, they are increasingly being targeted by attackers and on the other, those who are attempting to stay ahead of the attackers are pulled back by malicious insiders and too many "false positives". This means issues being flagged that aren't actually fraudulent activities, taking up valuable analyst time. This year more attacks targeting banks ranging from insider threats to spear phishing and ransomware attacks were noted. Banks are getting hit through their web applications, Internet and Mobile banking platforms. While the attack vectors may differ, the execution of the attacks often the same. It is paramount that local banks continue to sharpen their Cyber resilience capabilities in order to Anticipate, Detect, Recover and contain Cybercrime.

## Government

African government have automated most of their systems: - IFMIS in Kenya, online visa applications, e-government platforms. This shift has made the government to become a prime target for Cyber-attacks. These systems hold vast amounts of personal data, process vast amounts of transactions making them a lucrative attack point for attackers. Although the government has heightened Cyber monitoring and surveillance mechanisms, there is still need for security awareness, hardening of systems and implementation of policies and laws around Cybercrime.

## Financial Services

In 2017, the number of successful attacks launched against financial services doubled. Sacco's, Cooperatives and microfinance institutions have seen rapid growth in Africa, however, these institutions, for the longest time, have not prioritized Cyber security. This has made them a popular target for Cybercriminals. Larger institutions have invested more in Cyber security in comparison to smaller institutions hence making them an easier attack target.

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

## Mobile Money

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.

## Hospitality & Retail

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

**Kenneth Ogwang**

CIO

East African Breweries Ltd

Kenya

**In your opinion, what are the key cyber security issues facing Kenya/ Africa, what is being done to address these issues and what is the best way forward?.**

I regard the following as the significant risks with respect to Cyber Security:- Denial of Service, Supplier Compromise due to inherent weaknesses with our partners, Securing our assets in the era of digital explosion, theft/loss of information, IP or corporate data and lastly system or data manipulation.

It is not helpful to look at these in isolation. Firstly, an organisation needs to have a broad Cyber Security strategy that then informs the execution of the plans. Overall, the ownership of Cyber Security and her inherent risks need to lie at the highest level either at the board level or within the Senior Executive Leadership Team. This is to ensure that the funding and drive is made at the right level with the right agility in terms of execution.

All this is in the context that Cyber Security is not an IT responsibility but since it is an enterprise wide risk, then the appropriate ownership within the business must be established. IT though remains a significant partner in terms of driving the agenda as the expertise on such matters usually rests with IT. It is important for the IT teams to demystify Cyber Security and break it down in the simplest of terms.

One cannot take ownership of something one may not comprehend and therefore cannot measure.

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

There has been a great focus on end user and end user technology such as emails, computers and mobile devices as the point of security weakness. Based on this, ransomware was a big issue. The increase in number and nature of attacks was a cause of worry to many organisations. Two technologies have emerged in recent years to mitigate the risks of malware and other malicious behavior on PCs and mobile devices. Endpoint Detection & Response (EDR) software complements antivirus software on PCs and uses machine learning to identify and stop malicious behavior (e.g., ransomware). And with the growth of "mobile first" strategies, organisations need to respond to growing mobile threats. Mobile Threat Defense (MTD) software also uses machine learning to identify and stop malicious behavior.

In addition, with all the automation happening in Industries, a major area of concern is on Operational Technology (OT) which encompasses industrial control systems. This is at the heart of the Supply Chain Operations of any organisation and more focus is needed to address the growing number of cybersecurity breaches in OT. I will refer to an article where a petro chemical company was hit by a Cyber-attack. The aim of the attack was to trigger an explosion. The implications of this are huge. To address this growing threat, we are seeing that information cyber-security is beginning to merge with OT security to ensure the availability and integrity of manufacturing processes.

On a personal front, I still meet several people with default WiFi passwords at their homes. If you consider that you connect your TV (some with camera), Mobile devices, CCTV equipment on that, you can imagine how much information can be stolen if it is hacked. Home automation technologies make it easy to control a number of home functions such as home entertainment systems, heating, lighting, and even exterior door locks. Home owners need to follow best practices to secure these devices and manufacturers of home automation systems need to ensure their devices can provide security or they will not survive.

**Do you think fake news is a major problem in Your Country?**

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

In my opinion, definitely. The concept of fake news is nothing new. Pre-digital era and even now, it was manifest in society through rumors carried orally from one person to the other. During the print era, it could be used as a propaganda tool against certain persons/ organisations. More credible print institutions though confirm accuracy before printing. However with digitization and proliferation of social media, there are hardly any safe guards. The ease of creating an account and the pseudo-anonymity of social media makes it easy for lots of people to engage in this.

Fake news will never be ended but each of us should have the responsibility of fact checking before sharing any fake content. It is easy to verify facts even through a simple google check. Social Media platforms should make it possible for users to quickly indicate whether content is fake or not similar to the concept of 'likes'. A robust Social media PR mechanism should be in place to react to any fake news affecting a government institution or an organisation. These are some of the ideas I could share to control fake news.

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

For extreme forms of content such as terrorism, I do agree. On fake news, my opinion is to let the users identify this, get marked as fake and for everyone to move on.

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

Same as above. Social Media platforms should make it possible for users to quickly indicate whether content is fake or not similar to the concept of 'likes'. A robust Social media PR mechanism should be in place to tackle fake news affecting a government institution or an organisation.

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

I do believe the citizens are ready, however, more awareness is needed. Blind trust could mean laxity by government and her agencies in establishing the right controls. Citizens need to understand what to look out for in terms of data privacy and demand for such if the standards don't match up. For example, your address and ID should not be shared with any external parties without consent of the owner. Do citizens know this?

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

Breach in data privacy as mentioned above.

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

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

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

- Have a broad Cyber Security Strategy
- Assign the rightful ownership and accountability
- Assess your organisation and mitigate the risks both from legal and technical side.
- Continuous User Awareness including simulated phishing attacks. I cannot emphasize this enough. It starts with the user.
- Have an IT DRP and BCP in place and routinely test these so that in the event of an attack, you are aware of what to do.

**Do you think organisations are spending enough money on combating cyber-crime?**

Organisations are beginning to wake up to the reality of Cybercrime. This trend needs to be upped to match with the rapid evolution of the nature of cyber security threats. Cybercrime is not only growing rapidly, it is also becoming organized, sophisticated, well-funded, and focused on profit making attacks. Although cybersecurity budgets are growing, it will be a challenge to keep up with the growth of cybercrime.

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

Ensuring you have a Cyber Security Strategy and assigning the right ownership and accountabilities.

This makes it easier to apportion budgets where needed.

Remember it is not an IT department accountability. It could be the responsibility of IT to execute the approved technical plans but the overall accountability lies within the business leadership. The business needs to understand the growing cybersecurity threats to their information security and operational technology. Security professionals need to present the real risks to their organisation and the potential consequences and financial impacts if appropriate security controls are not implemented.

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

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

I would differ on this with the majority.

The nature of Cyber Security threat is a global one; the assets targeted that are of the highest risk are global in nature hence I would not encourage an African centric solution to drive this on a separate path and re-invent the wheel but rather a consolidated effort. Cyber Security attacks are evolving fast and collaboration with all players.

The real focus in Africa should be on legal and regulatory fronts. Putting in place laws, policies, regulations that help drive the National Cyber Security awareness, prevention and control. It should be mandatory for example for organisations to report a significant breach and for institutions to enforce data privacy. Also, heavy punishment for those caught in the act of Cyber-attacks should be inflicted to discourage the vice. Bi lateral agreements should be in place to ensure even those remotely culpable are brought to book.

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

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

Implementing a robust Cyber Security Strategy with clearly defined vision, goals and objectives both at the national and organisational level.

To those African countries that have done so, enforcing what is on paper and that will need ensuring the agencies responsible are well skilled and funded to handle the increasing threat.

For enterprises, continuously assessing the environment for additional threats and fine tuning internal plans to adopt to those threats. As mentioned earlier, this could extend to the manufacturing sites. Lastly, it all begins with the individual person. Keep them informed!

# Anatomy of a Cyber Heist

**INDICATORS OF COMPROMISE**

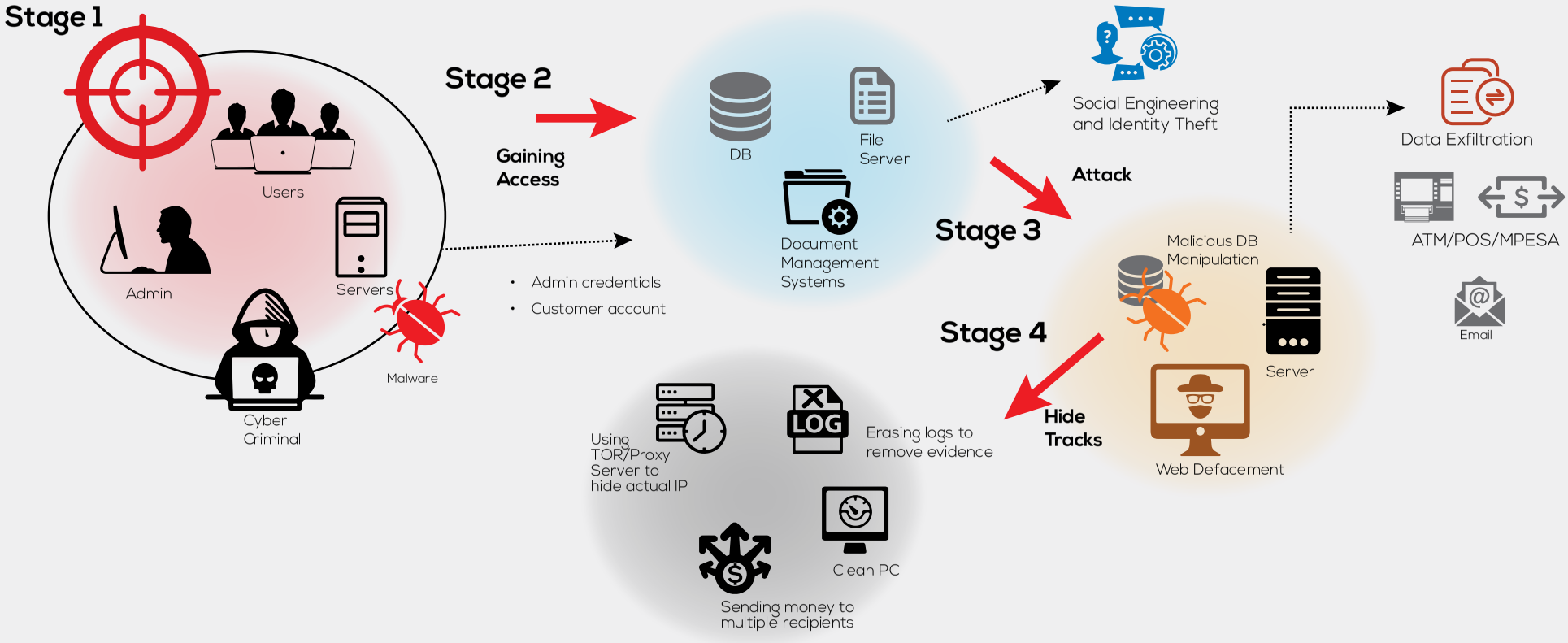
| | | | | |
|---|---|---|---|---|
| **MULTIPLICITY** | • Scanning from external IP | • Traffic to core VLAN from extenal IP | • Dormant account activity | • Logs deleted |
| **VELOCITY** | • Bruteforce attempts | • Multiple posting on DB | • Bulk transaction processing | • System unavailable |
| **VOLUME**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

**KEY SYSTEMS**

Firewall · Antivirus · DNS · DHCP · Active Directory

**ATTACK STAGES**

RECONNAISSANCE → GAINING ACCESS → ATTACK → HIDE TRACKS





# Home Security

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

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

## IP Cameras/Nannny Cams

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

## Smart Homes

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

## Home Routers

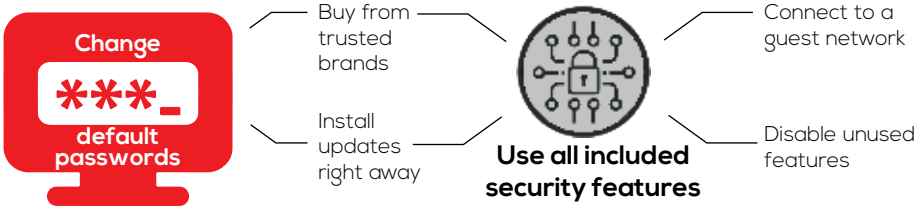
When buying a home router, no consideration is put on the security of these devices. Recent research has shown that your home routers can be used by malicious outsiders to launch attacks against websites belonging to other organisationss without your direct involvement.

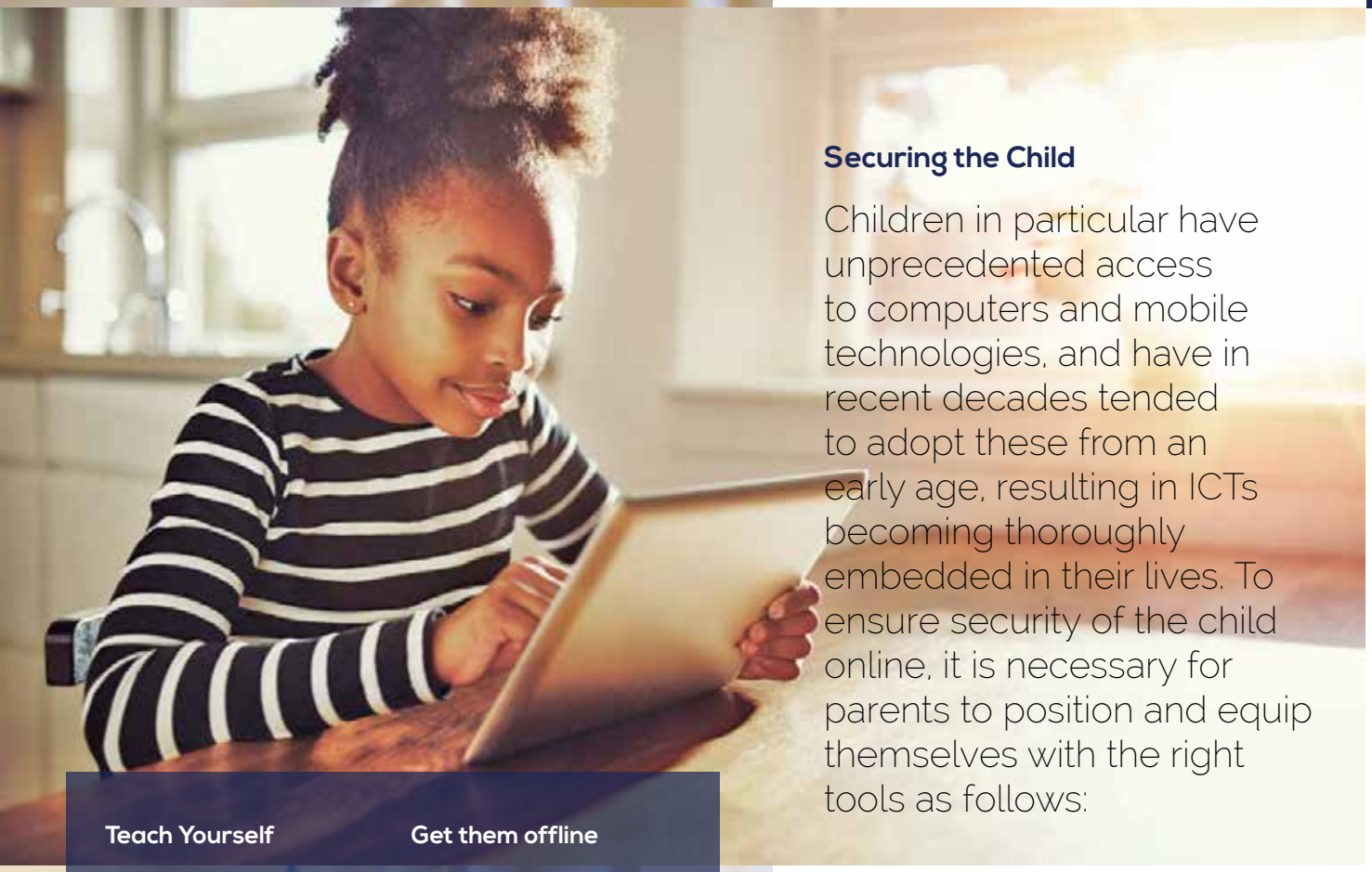
As a home owner, you run the risk of being blocked by certain sites, your internet speed may be slow due to the excessive bandwith utilization and you will incur higher costs.

## Security Begins at Home

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

Security Tips





## Securing the Child

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

### Teach Yourself

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

### Check Privacy Settings

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

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

### Get them offline

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

### Cyber Bullying

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

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

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

### Parents can

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

**Dr. Peter Tobin**

Privacy and Compliance Expert

BDO IT Consulting Ltd

Mauritius

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

## Historical context for the GDPR

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

## African personal data privacy and protection developments

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

## So what is the European Union GDPR?


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

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

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

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

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

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

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

### Key changes in the GDPR

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

### Beyond the vanilla GDPR

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

### So how is your compliance status?

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

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

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

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

# Africa Cyber Security Framework

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

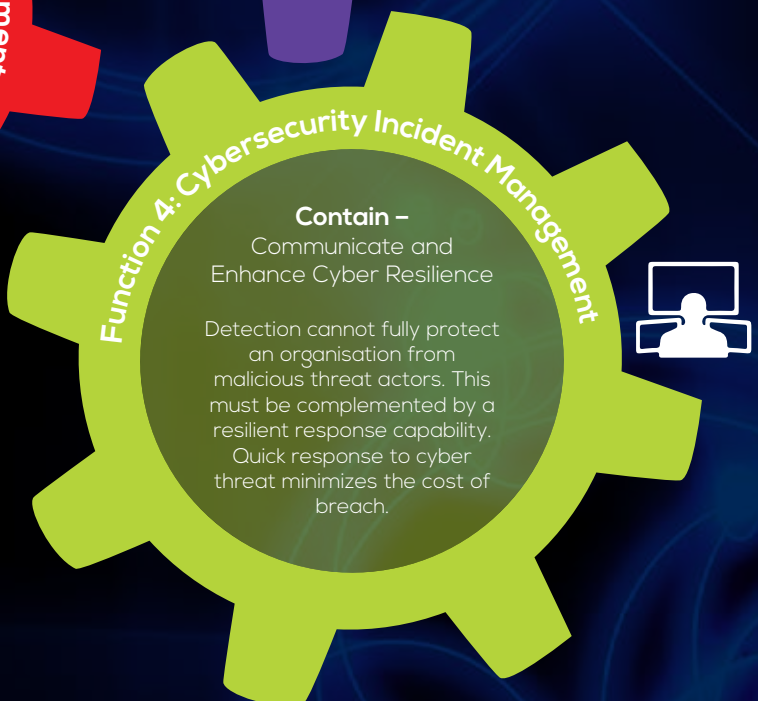
With the increasing business requirements of the 21st century businesses and the inadequate budget allocated to IT, it has become expensive especially for small and medium sized companies to adopt complex and international cyber security frameworks. As such, cybercrime prevention is often neglected within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

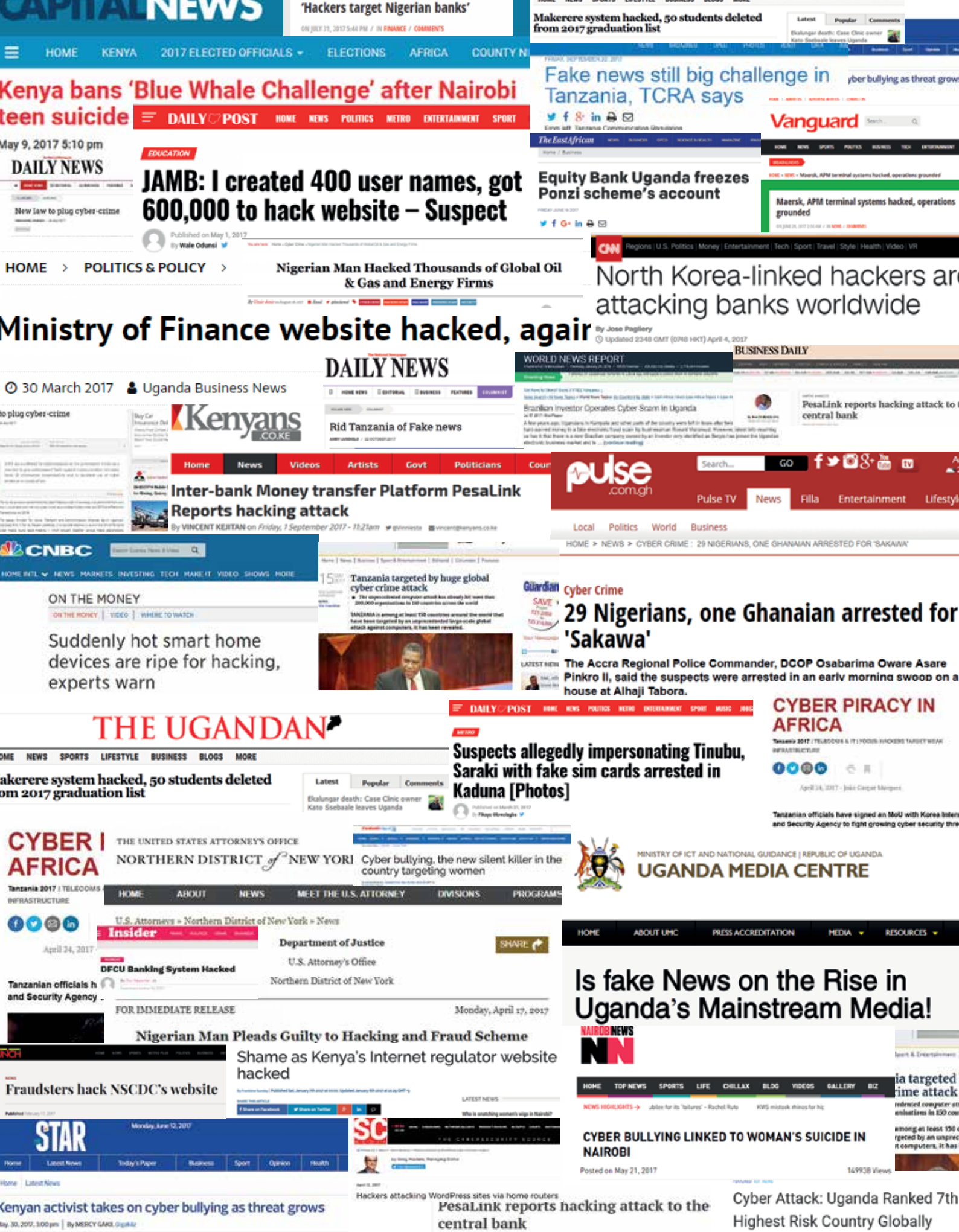
## Solution

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

# Functions of the Africa Cyber Security Framework




'Hackers target Nigerian banks'
Makerere system hacked, 50 students deleted from 2017 graduation list
Kenya bans 'Blue Whale Challenge' after Nairobi teen suicide
Fake news still big challenge in Tanzania, TCRA says
Vanguard
May 9, 2017 5:10 pm
DAILY NEWS
New law to plug cyber-crime
JAMB: I created 400 user names, got 600,000 to hack website – Suspect
Equity Bank Uganda freezes Ponzi scheme's account
Maersk, APM terminal systems hacked, operations grounded
HOME > POLITICS & POLICY >
Nigerian Man Hacked Thousands of Global Oil & Gas and Energy Firms
North Korea-linked hackers are attacking banks worldwide
Ministry of Finance website hacked, again
30 March 2017 Uganda Business News
DAILY NEWS
Rid Tanzania of Fake news
Kenyans.co.ke
Brazilian Investor Operates Cyber Scam In Uganda
PesaLink reports hacking attack to central bank
Inter-bank Money transfer Platform PesaLink Reports hacking attack
pulse.com.gh
CNBC
ON THE MONEY
Suddenly hot smart home devices are ripe for hacking, experts warn
Tanzania targeted by huge global cyber crime attack
Cyber Crime
29 Nigerians, one Ghanaian arrested for 'Sakawa'
The Accra Regional Police Commander, DCOP Osabarima Oware Asare Pinkro II, said the suspects were arrested in an early morning swoop on a house at Alhaji Tabora.
THE UGANDAN
Makerere system hacked, 50 students deleted from 2017 graduation list
Suspects allegedly impersonating Tinubu, Saraki with fake sim cards arrested in Kaduna [Photos]
CYBER PIRACY IN AFRICA
CYBER CRIME AFRICA
THE UNITED STATES ATTORNEY'S OFFICE
NORTHERN DISTRICT of NEW YORK
Cyber bullying, the new silent killer in the country targeting women
MINISTRY OF ICT AND NATIONAL GUIDANCE | REPUBLIC OF UGANDA
UGANDA MEDIA CENTRE
U.S. Attorneys » Northern District of New York » News
Department of Justice
U.S. Attorney's Office
Northern District of New York
DFCU Banking System Hacked
FOR IMMEDIATE RELEASE
Monday, April 17, 2017
Nigerian Man Pleads Guilty to Hacking and Fraud Scheme
Is fake News on the Rise in Uganda's Mainstream Media!
Fraudsters hack NSCDC's website
Shame as Kenya's Internet regulator website hacked
NAIROBI NEWS
CYBER BULLYING LINKED TO WOMAN'S SUICIDE IN NAIROBI
Posted on May 21, 2017
149938 Views
STAR
Monday, June 12, 2017
Kenyan activist takes on cyber bullying as threat grows
Hackers attacking WordPress sites via home routers
PesaLink reports hacking attack to the central bank
Cyber Attack: Uganda Ranked 7th Highest Risk Country Globally

**Fredrick M. Bobo**

IT Audit Manager

African Organisation of English-speaking Supreme Audit Institutions

South Africa

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

One of the major cyber issues related to leaking personal information of millions of people. This raises the question of whether there are adequate systems and laws to safeguard personal data.

WannaCry ransomware was another top issue in the year. Luckily my organisation or myself were not hit by it but numerous organisations in South Africa were hit.

From an overall perspective, the top cyber security issue anywhere probably remains human gullibility. Very few attacks are based on technological weakness but social engineering. What is needed, is education, training and awareness of cyber security.

**Do you think fake news is a major problem in Your Country/Africa?**

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

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

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

Certainly, fake news is a problem everywhere. What even makes it worse is that corrected positions are never publicized as much as the fake news. What is required, is for people to understand that news is not beyond reasonable doubt just because it is online.

Fake news really is something that does not have an immediate solution.

With the advent of social media and increased internet penetration year on year I only see fake news increasing.

Any entity should be free to create and distribute news, but not fake news. Regulators should not force influential platforms only, but all platforms to remove fake news. But to do that, the regulators must first define what fake news is in their jurisdictions, according to their laws.

We need the main stream media houses and journalists to rise to the occasion and be a true north when it comes to news reporting. It is disheartening when fake news is disseminated by an established news house.

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

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

I believe the citizenry is ready to consume these systems owing to the efficiency brought about by them. Additionally, I think going that direction is inevitable. What I think needs to be importantly worked on is matching legal frameworks and fundamentals to support e-service provision. These fundamentals include such things as internet access, computing devices etc.

The threat of privacy security and fraud will always be there, and the level will differ on the platform as well as services provided, e.g. e-voting with our current African politics will be a serious challenge. The right thing to do is implement it properly and ensuring feasibility before the projects are implemented.

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

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

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

Not affected by it

A good way that we can limit impact is going back to basics, awareness and training. This is so often underrated but very cardinal in limiting ransomware cases. As ransomware is based on cryptography algorithms, stopping it in advance like a basic virus is not possible.

**Do you think organisations are spending enough money on combating cyber-crime?**

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

Working in a public space across Africa, it is clear the public sector is not treating Cyber crime with the seriousness it deserves. We have seen a few countries change legislation and put in structures, but I think most governments are waiting to be hit hard before they put in mitigating measures.

One way we can encourage appropriate spending on cyber security issues is to increase awareness. There is currently very little focus on cyber security in governments of Africa. We lack proper public statistics on cybercrimes and losses. I suspect a good number may be going unnoticed and it pains me to think of how much money our poor governments may have lost.

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

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

I am biased to think that a lot of work needs to be done on cyber security in public sector

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

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

- Legislative reform
- Structures & processes to combat cyber crimes

# Appendix

## List of Remote Access Tools for Database

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

## Remote Access tools for Endpoints

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

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

## List of Open Source Tools

Vulnerability Scanners

1. OpenVAS

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

2. Retina CS Community

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

3. Microsoft Baseline Security Analyzer (MBSA)

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

4. Nexpose Community Edition

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

5. SecureCheq

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

6. Qualys FreeScan

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

# References


## Top Issues

https://securityintelligence.com/the-enemy-within-identifying-insider-threats-in-your-organisation/

https://portland-communications.com/pdf/The-Reality-of-Fake-News-in-Kenya.pdf

The Computer and Cybercrimes Bill, 2017 - Kenya Law

http://www.ke-cirt.go.ke

CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015 ...

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

339_The Cybercrimes Acts, 2015-1

## Attacks

https://www.standardmedia.co.ke/business/article/2000228978/shame-as-kenya-s-internet-regulator-website-hacked

https://www.standardmedia.co.ke/business/article/2001249724/how-kenyans-were-lured-into-sh2-trillion-public-likes-scam

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

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

## Cyber Intelligence

https://www.google.com/search?q=heartbleed+vulnerability&oq=heartbleed+vulnerability&aqs=chrome..69i57j0l5.6115j0j9&sourceid=chrome&ie=UTF-8

https://www.projecthoneypot.org/list_of_ips.php?t=h

SERIANU

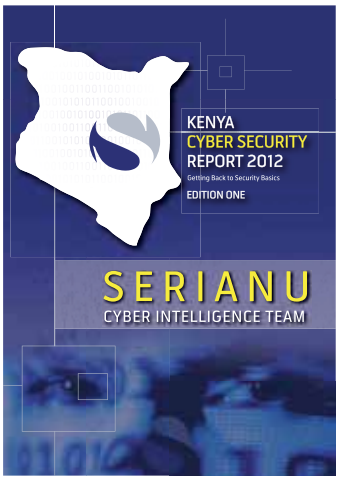
# Cyber Immersion

Hands on Cyber Security Training for Professionals

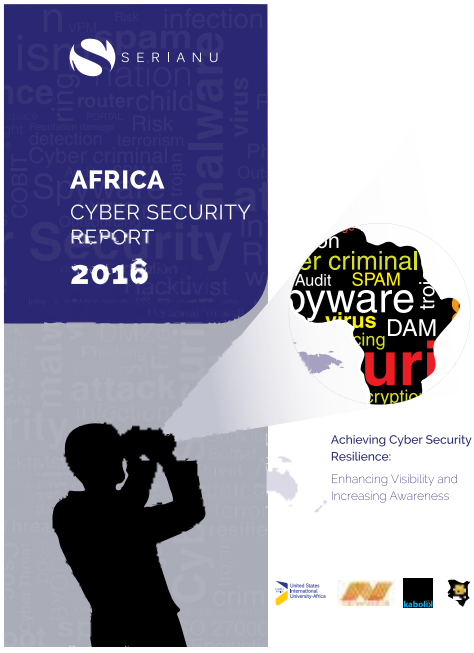
Africa Cyber Immersion Centre
acic
Engage | Educate | Empower

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

info@serianu.com | www.serianu.com






SERIANU United States International University-Africa ISACA DataposIT DEMADIUR kabolix Botswana LIQUID TELECOM