SERIANU

Kenya

Cyber Security Report 2017

Demystifying Africa's Cyber Security Poverty Line

United States International University-Africa

ISACA

Trust in, and value from, information systems

LIQUID TELECOM

SERIANU CYBER-THREAT COMMAND CENTRE SC3 ANTICIPATE • DETECT • RESPOND • CONTAIN

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

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

For more information contact;

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

Content

Editor's Note and Acknowledgement

We are extremely pleased to publish the 5th edition of the Kenya Cyber Security Report. This report contains content from a variety of sources and covers highly critical topics in Cyber intelligence, Cyber security trends, industry risk ranking as well as home security.

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

Top Trends: We analysed incidents that occurred in 2017 and compiled a list of top trends that had a huge impact on the economic and social well-being of organisations and Kenyan 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 Kenyan 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 Kenyan organisations and in particular, to gain a better appreciation of the costs to the local economy. We provide an estimate of this cost, which includes direct damage plus post-attack disruption to the normal course of business.

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

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

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

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

Brencil Kaimba
Editor-in-chief

What can our readers look forward to in this report?

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

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

Appreciation

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

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

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

The Serianu CyberThreat Intelligence Team

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

Barbara Munyendo – Researcher, Cyber Intelligence

Kevin Kimani – Researcher, Anatomy of a Cyber Heist

George Kiio – Researcher, Home Security Researcher

Nabihah Rishad – Researcher, Risk Ranking and Survey Analysis

Morris Ndung'u – Data Analyst

Mark Muema – Data Analyst

Ayub Mwangi – Data Analyst

Margaret Ndung'u – Data Analyst

USIU Team

Raymond Musumba **Gaurav Bhatnagar**

Zamzam Hassan

Commentaries

Dr. Stanley Githinji

Information Security and Forensics, USIU-A

John Sergon

Ag. Chief Executive Officer, ICT Authority, Kenya

Joseph Mathenge

Chief Operations Officer, Serianu Ltd

Ben Roberts

Chief Technical Officer, Liquid Telecom Group

Martin Mirero

ICT Director, Huduma Center

Eric Mugo

Fraud Department, Safaricom Ltd

Faith Basiye

Head Forensic Services –KCB

James Nyakomita

CIO, APA Apollo Group

Steve Mambo

Cyber Insurance Consultant & Cyber Security Specialist

Sammy Nyambu

Head of ICT, Mwalimu National Sacco

Jeff Karanja

Information Security Consultant

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

PROJECT HONEY POT

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 Kenya.

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

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

Design, layout and production: Tonn Kriation

Disclaimer

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

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

For more information contact:

SERIANU

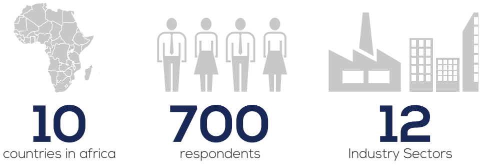
Serianu Limited:

info@serianu.com | www.serianu.com

Foreword

THE GLOBAL CYBER SECURITY LANDSCAPE IS EVOLVING AND BECOMING QUITE COMPLEX. THIS EVOLUTION IS LARGELY BEING DRIVEN BY THE RAPID CHANGE AND QUICK ADOPTION OF TECHNOLOGICAL INNOVATIONS ACROSS THE GLOBE. SINCE THE LAUNCH OF OUR INAUGURAL REPORT IN 2012, THE AFRICA CYBER SECURITY REPORT (ACSR) HAS FOCUSED ON DEMYSTIFYING 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.

Despite six years of research, we have not been able to answer 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 to be 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.



To answer this question, we surveyed over 700 business professionals from various business settings in 10 countries across Africa. We then cross-examined their annual expenditure on Cyber security. The findings from this survey shockingly suggest that a majority of 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 the **"Security Poverty Line"** or below. 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, 2017), 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 majority of the Cyber security professionals in Africa were contracted by established organisations. At the height of the crisis, the small talent pool of Cyber security professionals were snapped up by huge multi-nationals that offered better incentives. This left the vulnerable SME sector completely at the mercy of Cyber criminals. Considering the skills/technical resource challenge in the continent, who was taking care of the SMEs?

SMEs in Africa are facing a number of challenges including the prohibitive cost of Cyber security solutions and services, limited budgets, lack of skilled personnel. With these challenges, it is become expensive 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 KENYA.

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?

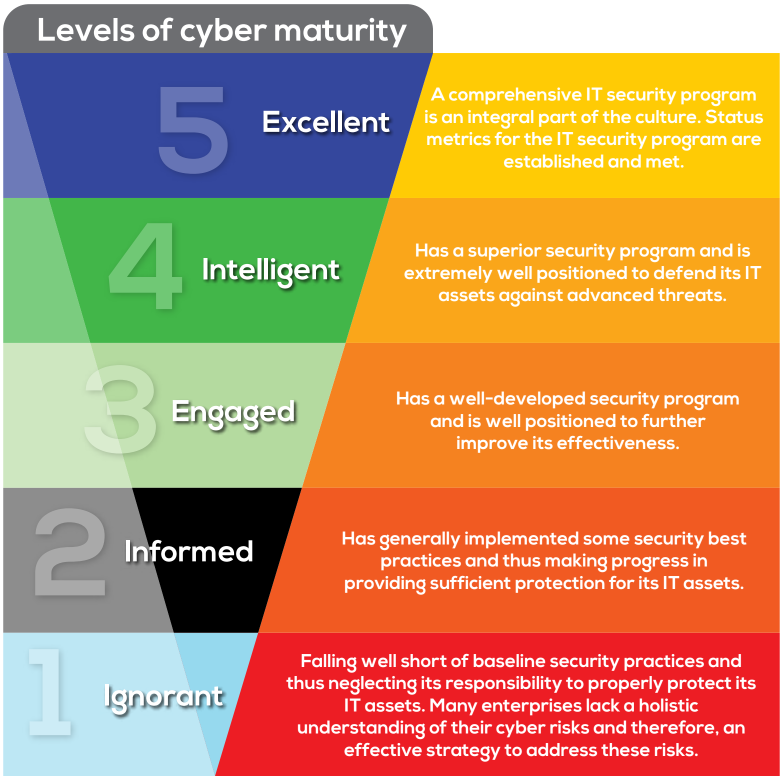
Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

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 Kenya.

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

Firms rated their own capabilities by responding to 24 questions that covered the five 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.



Levels of cyber maturity

5 Excellent: A comprehensive IT security program is an integral part of the culture. Status metrics for the IT security program are established and met.

4 Intelligent: Has a superior security program and is extremely well positioned to defend its IT assets against advanced threats.

3 Engaged: Has a well-developed security program and is well positioned to further improve its effectiveness.

2 Informed: Has generally implemented some security best practices and thus making progress in providing sufficient protection for its IT assets.

1 Ignorant: Falling well short of baseline security practices and thus neglecting its responsibility to properly protect its IT assets. Many enterprises lack a holistic understanding of their cyber risks and therefore, an effective strategy to address these risks.

What is the impact of operating below the poverty line?

The overall survey results found about 90% of respondents in Kenya 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
- remendously 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 is 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, its 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.

What can our readers look forward to in this report?

This report gives insightful analysis of Cyber security threats, trends and issues in Kenya. The report sections are well researched to cater to the needs of all organisational staff from the board to the general staff. The anatomy of a Cyber-heist is a section that was researched with security implementers and forensic investigators in mind while the top priorities section caters for boards and Executives within the organisations. We have also highlighted other social issues such as home security that plays an important role away from the corporate standpoint.

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 Kenyan organisations are operating below the security poverty line significantly exposing themselves to Cyber security risks

Cost of cyber-attacks $210M annually

FAKE NEWS

Fake News has hit Kenya'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 Kenya

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

96% Cyber security incidents either go unreported or unsolved

Dr. Stanley Githinji

Information Security and Forensics

USIU-A

There is a huge skill gap in Cyber security, what are academic institutions currently doing to close this gap?

The huge skill gap in cyber security in Africa is as a result of having academic programs that are not addressing industry's needs. Although more students are choosing to pursue STEM degrees, many of these programs have a retention problem. There are very few universities that are offering standalone degrees in cyber security at undergraduate and graduate level. Universities are currently providing cyber security certifications in partnership with certification bodies. The partnership ensure that the student in academic institutions get hands-on experience in cyber security. Going forward academic institutions may want to develop their own hands-on training programs that are more relevant to industry's needs.

In the previous year, what were the key Cyber security challenges faced in the academic sector?

Cyber-attacks are diversifying, putting businesses at increasing risk hence the need to have reliable mechanism to prevent the attacks. In 2017, multiple ransomware attacks such as the Wannacry and cryptoworm affected many insitutions. While cyber threats and risks are unique to each industry, higher education is currently one of the top five sectors facing high numbers of cyber attacks. New attack surface as a result of BYOD and IoT have greatly contributed to DDOS targeting institution infrastructure and enabling insider fraud. There is need to for institution to have a holistic solution to cyber-security strategy implementation.

In your opinion, are universities in the country adequately investing in Cyber security training programs?.

Very few Universities are currently offering programs in cyber security, majority of universities offers cyber security specialization within a larger program, such as computer science, Information Technology, Software Engineering and Telecommunication. The name of the degree program is not as important as its contents, there is need to review the ratio and distribution of core courses to address cyber security needs. Universities should also invest in industry-standard equipment's and laboratories with forensic software's, network security software for Intrusion detection and prevention, penetration testing software's, and auditing software's.

In the past year, what were some of the key Cyber security programs that students were interested in pursuing?

The shortage of cyber security talent means that pursuing a degree within the field can be a highly rewarding career. There is high demand in programs offering Information Security and forensics courses. Majority of students are also interested in taking certification courses such as Ethical Hacking, CISA, CISM, Digital Forensics and CCNA. Am happy to mention that USIU-A is in the process of launching a master's degree in Information Security.

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

African universities should first starts with hiring qualified cyber security faculty. Very few universities are investing in R&D as well developing hubs for innovation for cyber security solutions and programs. The universities should also focus on partnering with private entities and offer cyber security services There is need of having more stakeholder's forums where students can show case their research works to potential clients, I find it to be exciting when the work the student is received well by stakeholders.

What are your expectations for the year 2018 with regards to Cyber Security within the Academic sector?

The importance of cyber security in the year 2018 and in the future is unquestionable. I expect to see more stakeholder's involvement in R & D, the Future of Cyber security depends on collaboration between industry, academia and government without compromising academic fundamentals.

Given the cyber security regulations and laws that have been effected, Universities should use the opportunity to develop programs that are addressing global needs in cyber security and to recognize that technologies such as machine learning, deep learning, and artificial intelligence will be cornerstones of tomorrow's cyber defenses.

Top Trends

Fake News: Vulnerability of truth

It is often said that a lie can travel half way around the world while the truth is still putting on its shoes.

In 2017 our media platforms were overwhelmed by rogue politicians, disinformation, misinformation and outrageous claims. From videos of post-election violence to news about politicians who have defected 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 true information from false information.

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

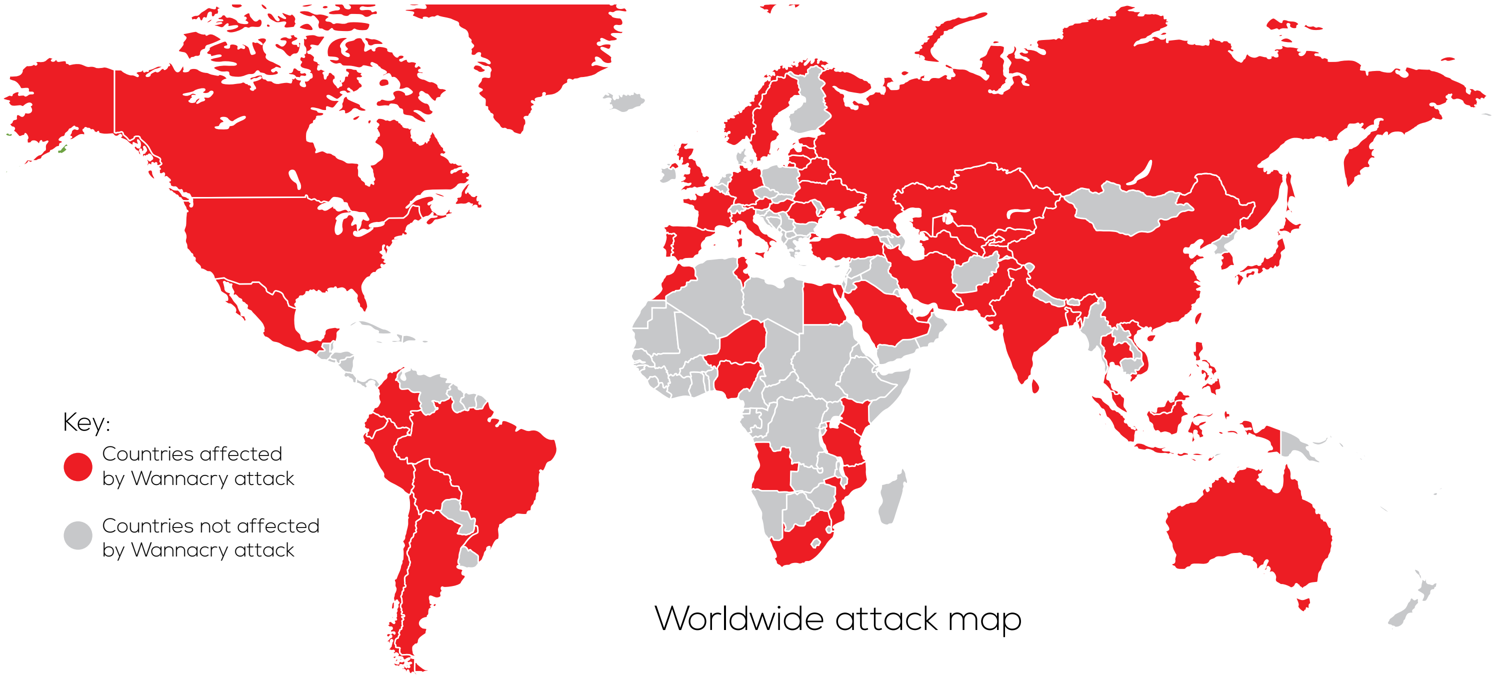
Insider Threat: The enemy within

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

Top insider threats:

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

Ransomware: I don't WannaCry


Key:
● Countries affected by Wannacry attack
● Countries not affected by Wannacry attack

Worldwide attack map

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

The level of sophistication in distribution methods and attack vectors have expanded and it is no longer enough to just rely on signatures and antiviruses, because, unfortunately, the data also shows no one is immune. The Polymorphic technique with minor changes leads to unknown malware and greater obfuscation. For example, there is a PowerPoint malware that spreads by simply hovering a mouse pointer over a tainted PowerPoint slide, WannaCry which spread itself within corporate networks without user interaction, by exploiting known vulnerabilities in Microsoft Windows.

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 anonymous 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. Although this game was banned in Kenya, one teenager fell victim to it.

The Cyber Crime Law is timely because, it provides a framework for identifying these cases and prosecuting them. The law now stipulates that harassing and stalking someone on Facebook or Twitter can earn you a 10-year prison sentence or a Sh20 million fine or both.

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

The cost of Cybercrime grew by approximately 20% but the skill gap is widening. No one knows what they're doing, majority of IT and security staff are downloading templates from the internet and applying these in their organisations. From our analysis, a key contributor to this is that organisations tend to look for people with traditional technology credentials such as IT and Computer Science. But when you look at the matter, we need Technology Analysts, Cyber Risk Engineers, Data Analysts and Risk Experts most of which does not necessarily warrant a technology course. Majority of organisations encourage their IT teams to take up courses that do not 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.

Joseph Mathenge

Chief Operation Officer

Serianu Limited

Approach in Raising Cyber Security Poverty

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

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

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

Ability to Identify threats.

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

Actively protect information assets.

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

Ability to detect cyber incident.

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

Understand how to respond and contain cyber event.

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

Have resilience and ability to recover from cyber event

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

In reading through this one may ask what tools are available to measure each of the above areas. There are several resources available to help assess these areas. Beginning with perhaps the simplest and least expensive is a self-assessment using template or questionnaire downloaded from resources such as NIST or the SANS Institute. An organization without internal resources with expertise in technology or cyber security might struggle working through the terminologies found in such templates. However they innately understand their operating environment and have the best knowledge in identifying impact a threat may have on the business. The next level would be engaging an external third party to conduct an assessment. Most organizations contract external parties to conduct a Vulnerability assessment and Penetration test (VAPT). These assessments, while are good and indicative of vulnerable areas may not fully explore all the areas required to ensure Cyber Security basic needs are met. Additionally the output tends to be technical in nature showing systems and vulnerabilities in terms of lack of patching or misconfiguration of systems. It is imperative that the output is contextualized in terms of business critical process to help create and implement and effective remediation plan.

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

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

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

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

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

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. For example

Wannacry exploited a vulnerability resulting from not applying a patch and for most cases, inadequate privilege account monitoring and 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 within 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 of 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. These schemes rely on a constant flow of new investments to continue to provide returns to older investors. When this flow runs out, the scheme falls apart. In recent times, we have seen these schemes evolve to now include crypto currencies.

System Integrity: Eroding Public Trust

Government systems have become a target for hackers seeking to make news or disrupt service delivery. From electoral systems to the 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.

Kenya's TOP 10 priorities for 2018

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

Kenya's TOP 10 priorities for 2018
1
2
3
4
5
6
7
8
9
10

1. **Database Security:** Secure the vault
2. **Privileged User Management:** Who has access to the crown jewels
3. **Patch Management:** To patch or not to patch
4. **Unstructured Data Management:** There is no one size fits all
5. **Endpoint Security:** Cyber security front-line
6. **Employee Security Awareness:** Ignorance is not Bliss
7. **Vendor/Third Party Security:** Bring Your Own Vulnerability
8. **The Board's Changing Role:** Security begins at the top
9. **Security Architecture/ Engineer skill set:** Widen your employee gaze
10. **Continuous Monitoring:** Askari Vigilance

1 **Database Security:** Secure the vault

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 **Endpoint Security:** Cyber security front-line

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 **Continuous Monitoring:** 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 is necessary that these organisations look for alternate solutions and practices including managed services and day long monitoring.

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 organization 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.

Cyber Intelligence Statistics, Analysis, & Trends

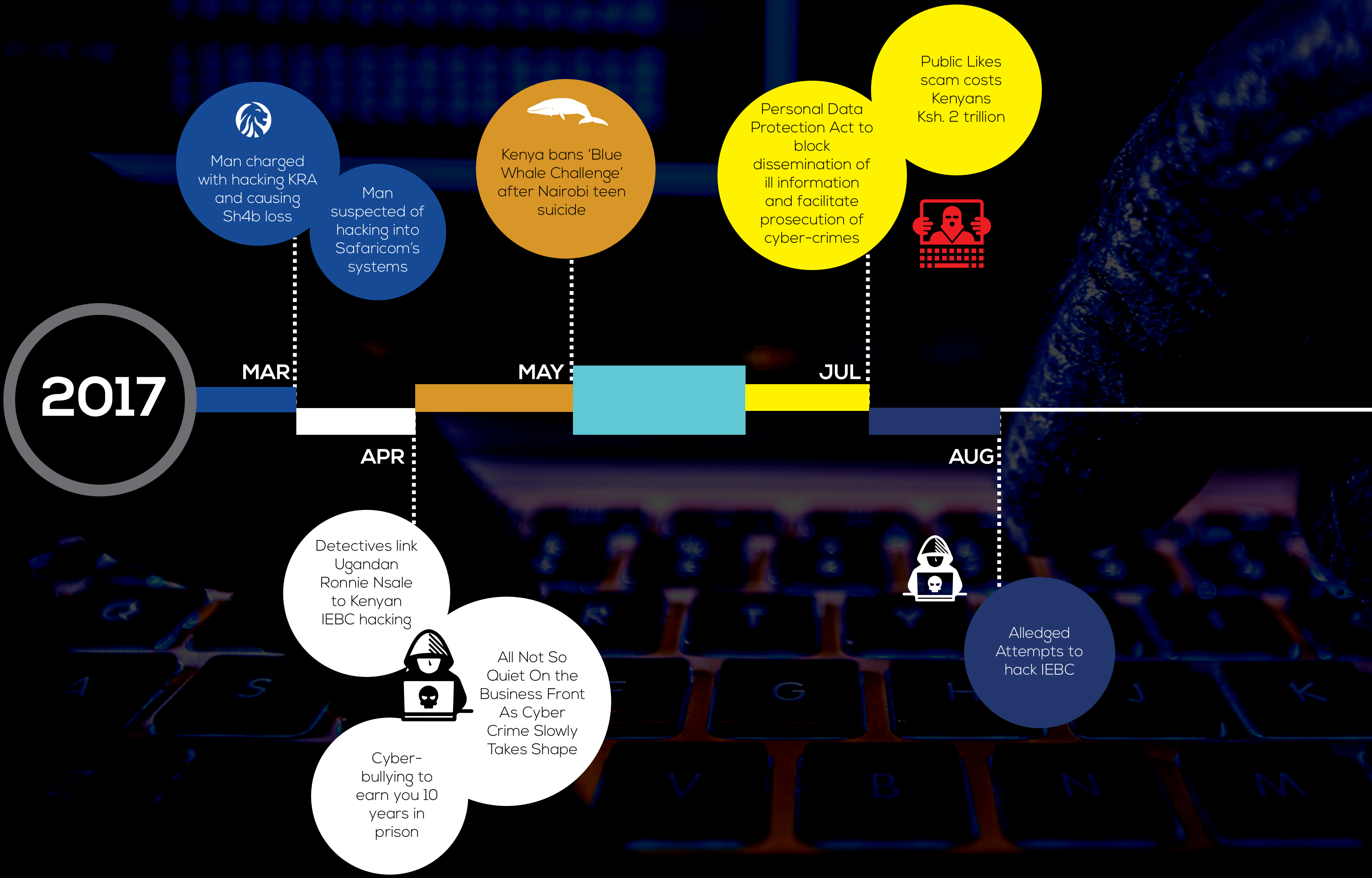
FOR THE PURPOSES OF THIS REPORT, WE INSPECTED NETWORK TRAFFIC INSIDE A REPRESENTATIVE OF KENYAN ORGANISATIONS, REVIEWED CONTENTS OF ONLINE NETWORK MONITORING SITES SUCH AS PROJECT HONEYNET AND REVIEWED INFORMATION FROM SEVERAL SENSORS DEPLOYED IN KENYA. THE SENSORS PERFORM THE FUNCTION OF MONITORING 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

MAR

Man charged with hacking KRA and causing Sh4b loss

Man suspected of hacking into Safaricom's systems

APR

Detectives link Ugandan Ronnie Nsale to Kenyan IEBC hacking

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

Cyber-bullying to earn you 10 years in prison

MAY

Kenya bans 'Blue Whale Challenge' after Nairobi teen suicide

JUL

Personal Data Protection Act to block dissemination of ill information and facilitate prosecution of cyber-crimes

Public Likes scam costs Kenyans Ksh. 2 trillion

AUG

Alledged Attempts to hack IEBC

Eric Mugo

Fraud Department

Safaricom Ltd

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

We have seen a lot of issues since all banks are connected to us. So many banks have approached us to help investigate their fraud. We have seen a lot of Cybercrime in the financial industry, where huge amounts are involved and the money moves very fast without a paper trail. We have noticed most of these crimes are insider enabled, Cyber criminals target to use specific employees within the organisations. It is no longer random these are now becoming organized crimes.

The new trend we are seeing is to move money through PesaLink into other banks as opposed to sending it out to accounts of the same bank. Trailing the money becomes very difficult for the involved victims.

There has been the issue of evidence where the judiciary or police expect hard evidence while many at times the evidence is abstract for example logs.

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

Yes. Lack of accountability is the issue. Tracking the source of the news is also very hard and the effort, time and resources needed is too great, so many times organizations just leave the issue.

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

Ideally the person posting the information, because take for example following up on anonymous person is quite difficult. We can't put it on institutions.

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

Yes. It is one of their mandates as consumer protection, however, how practical is it? Given the fact that most of these platform are not locally based. Controlling these platforms is very difficult.

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

Above the line user awareness is important however organisations do not do it often, probably because they don't want to implicate themselves or because the awareness doesn't seem to raise profits. There's also another issue in awareness where you have to consider how much information to give out.

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?

Yes definitely. These services must go online and must be availed to all in a convenient way. The challenge is, risk is always left behind by the organizations. So now these services end up being misused for as some services output personal data on a simple query eg. sending an ID number. There must be mitigations put in place.

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?

Exposure of confidential information. As a result of the exposure fraud is bound to happen especially to do with identity fraud.

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

We faced attempts like other organisations from phishing emails to specific attempted attacks to services. We have not had major incidents.

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

This can be done through the strategic level: have conversations in boards and government institutions. Invest in the necessary technology to prevent this incidences. These conversations need to happen to enable investing in Cyber security.

Universities also need to be research driven, and update courses to actually what is needed in the market. The academia has a role to play in this too.

Forums are also needed to prevent similar attacks happening. Exchange of information is important for organisations in the same industry.

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

No. Some organisations have had to hire information security professionals just because the CBK mandated. Thus in such cases even convincing the board is a hard task.

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

Awareness of business leadership. Because what is important is; customer experience, reputation and the money bottom-line.

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?

Creating an enabling environment for people to go into these innovations. Academia, private sector and government need to partner in order to encourage the innovation.

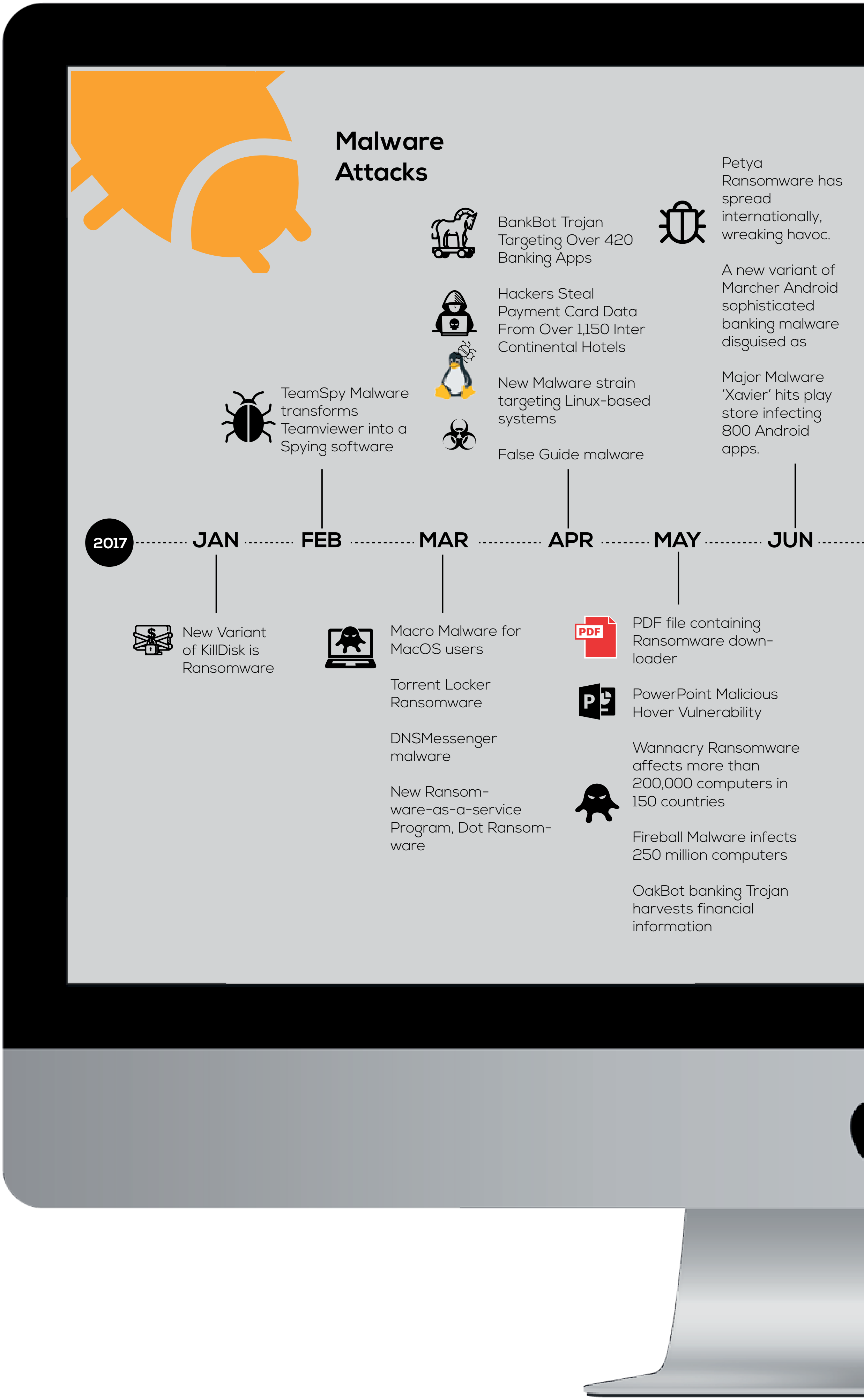
What role can the private sector and consumers of imported Cyber security products play to ensure we can encourage local players to start developing African grown Cyber security products or solutions or even services?

There is a large opportunity here as the fraud we experience here is very different from what the west experiences take for example fraud on mobile money is bigger here than anywhere else. That is an opportunity for us to develop solutions that work for us.

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

Prioties would be remote access and key loggers. Number two would be identity theft. We are trying to mitigate this on our level through 2 factor authentication. Organisations need to take care of basics such as patching. Basic awareness, educating users and employees. Building whistle blowing systems; where employees approached by outsider fraudsters need to report to prevent the fraudsters from approaching another naive employee.

Collaboration! Information is in silos and not being shared between organizations. Sharing information is key in helping to mitigate Cybercrime. We are now dealing with organized crime and we are unorganized hence we are being hit!



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 Ransomware-as-a-service Program, Dot Ransomware

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 downloader

PowerPoint Malicious Hover Vulnerability

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

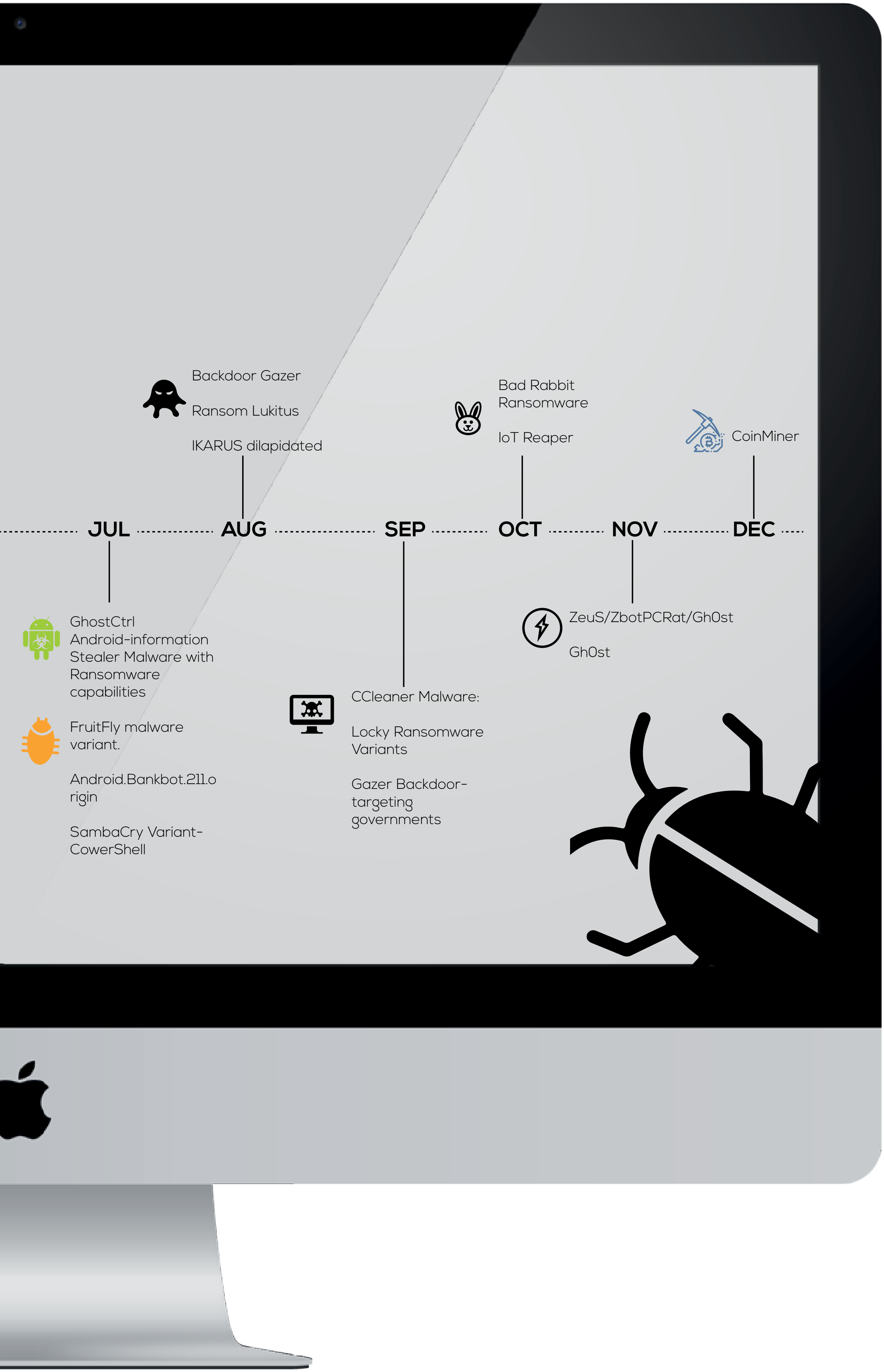
Fireball Malware infects 250 million computers

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

GhostCtrl Android-information Stealer Malware with Ransomware capabilities

FruitFly malware variant.

Android.Bankbot.211.origin

SambaCry Variant-CowerShell

CCleaner Malware:

Locky Ransomware Variants

Gazer Backdoor-targeting governments

ZeuS/ZbotPCRat/Gh0st

Gh0st

Ben Roberts

Chief Technical Officer
Liquid Telecom Group

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

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

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

Yes.

If yes, who should be responsible for controlling the creation and distribution of fake news (government, end users, Telcos/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 is 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 is probably fake news, and don't forward fake news.

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

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

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

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

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

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

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

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

Do you think organisations are spending enough money on combating 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.

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

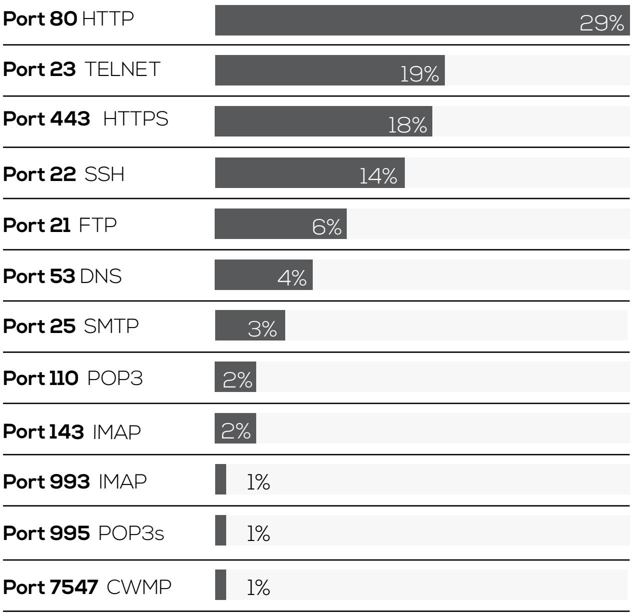
Open Ports

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.

65,535
TCP ports

65,535
UDP ports

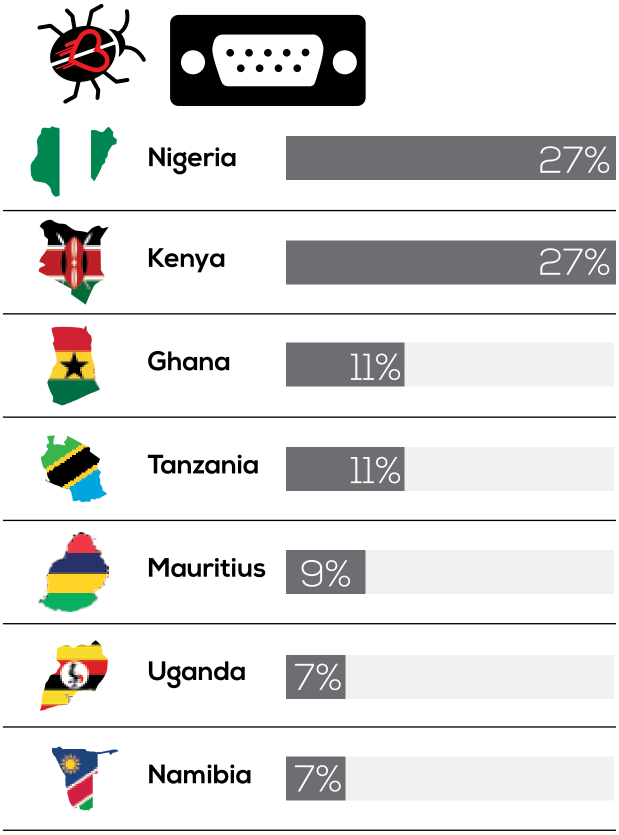
Top Open Ports



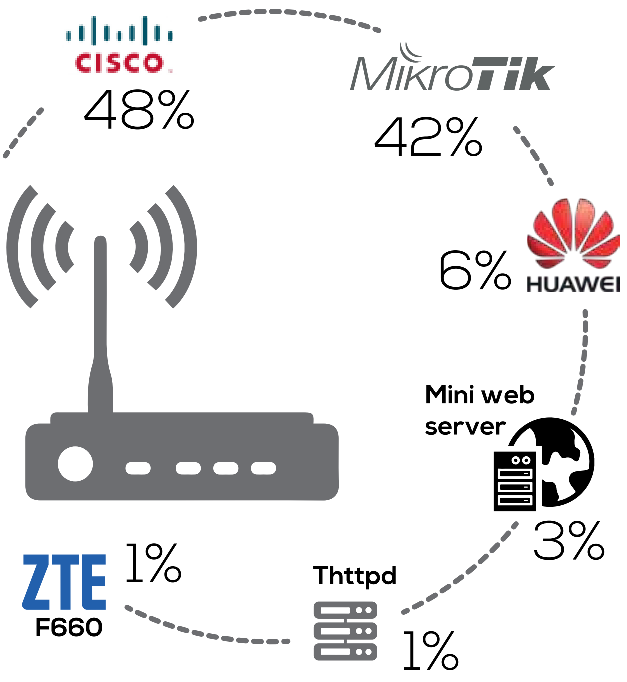
- TCP port 80, 8080 and 443 support web transmissions via HTTP and HTTPS respectively. HTTP transmits unencrypted data while HTTPS transmits encrypted data. Ports 25 and 143 also transmit unencrypted data therefore requiring the enforcement of encryption. These ports are commonly targeted as a means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

b) Heartbleed Vulnerability

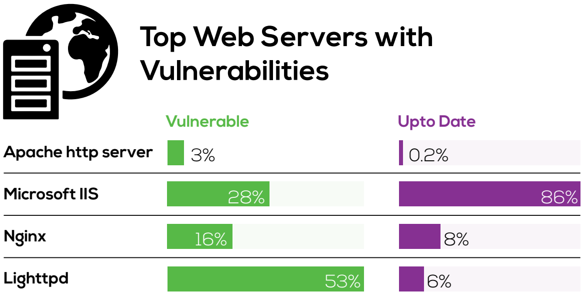
The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information such as user names and passwords, instant messages, emails and business critical documents and communication protected that under normal conditions, is encrypted by the SSL/TLS encryption. As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been released and now it has to be deployed.



Top Routers



Top Web Servers with Vulnerabilities



Apache is the most commonly used web server. Key vulnerabilities associated with web servers include remote code execution, SQL injection, format string vulnerabilities, cross site scripting (XSS). Majority of these are as a result of not applying patches. There is need for constantly upgrading to the updated web server patches.

Top Spam Servers

Spam Servers IPs

41.215.20.74	60%
196.200.29.246	8%
196.207.24.202	7%
41.215.59.246	6%
41.222.14.89	5%
196.200.16.23	4%
41.215.68.2	3%
41.212.55.179	2%
62.24.108.239	2%
196.202.202.197	2%

*Spam - Electronic junk mail

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

Top Dictionary Attackers

Dictionary Attacker IPs

41.215.20.74	36%
196.200.29.246	20%
196.207.24.202	18%
41.215.59.246	18%
41.222.14.89	7%
196.200.16.23	4%
41.215.68.2	3%
41.215.68.2	3%
41.222.14.89	7%
196.200.16.23	4%
41.215.68.2	3%

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

Dictionary attackers typically send to common usernames

Faith Basiye

Head Forensic Services

Kenya Commercial Bank

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

“For this industry the impact is majorly from the “”enemy within””. Most attacks are moving towards manipulating technology with the help of insiders.

It is also more of a generation issue; the current generation coming into the job market is very restless and looking for instant gratification, success and fast money so when they face reality and get frustrated they end up collaborating with fraudsters to commit Cybercrime.”

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

Yes, it places a huge reputational risk on organisations. For example just a tweet alone, as small as an “ ATM not working” has a great impact on an organisation. News on social media is especially unverified but has the capability of spreading very fast potentially capable of killing a small business. We are aware that it is potentially damaging.

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

In this era suppressing social media is very difficult.

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

They could, but at the moment this responsibility primarily lies with the institution to manage communication with their customers; how we respond to customers and incidences matters. These platforms are in a different business which is becomes hard for them to majorly control information in a way that works for all institutions.

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

User awareness is necessary. Depending on the damage being caused, in the near future we expect to see law suits against slanders without facts. Educating internal staff on better communication online especially to customers, they need to be aware that what you share can be shared/ retweet a thousand times going to millions.

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 right place to utilize and consume these services. The country is in a good place technologically, however data privacy is a big risk area. It is just a matter of time before something happens. There are many questions around it, for example; who holds e-government data? Is the data safe? In that regard, identity fraud is very easy. Cloning and running another “e-citizen portal is something that can easily happen; case in point the Tanzania incident.

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?

Data security is a big risk, identity fraud, data corruption, creation of e-citizen clones. Our data is out there and our citizenry is too trusting; for example when IEBC was recruiting clerks a lot of personal data eg. Bank account details was shared even before being employed.

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

No. We are aware it is a big concern and we are not sleeping on Cyber security. We are putting the necessary measures.

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

They have started. The government has just put up a Cyber security task force under the Ministry of ICT. Within the organization, we are not sparing any coins: spare a coin and see how many more you lose. There is now a positive change in budgeting for Cyber security matters. It was hard to convince boards to invest in Cyber security until incidences occur and they see the need to invest more in Cyber security.

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

Awareness is key, as most boards are not aware of the severity of not budgeting for Cyber security.

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

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

We need to invest more in Cyber security Research and Development. At least we have had some hubs coming up encouraging innovation within the younger generation, hoping that progresses.

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?

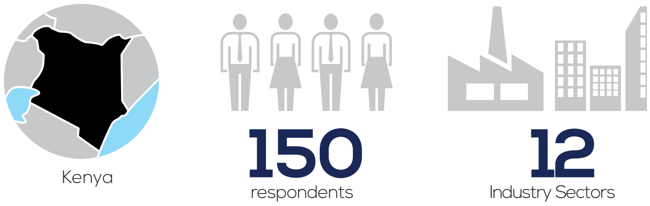
By sponsoring these initiatives and providing more opportunities for them, coming up with custom products for them such as loans and grants.

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

Key loggers is big, malware, and look out for unauthorized remote access. Policies like BYOG can compromise organisations when malware is introduced into an organisation through employee gadgets. Man in the middle attacks and "data kidnapping" are also things to watch out for.

We can't ignore technology, understand the risks it poses. Information is key, guard it from a personal, organizational and national level. Security is everyone's business.

2017 Kenya Cyber Security Survey



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

About the Survey

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

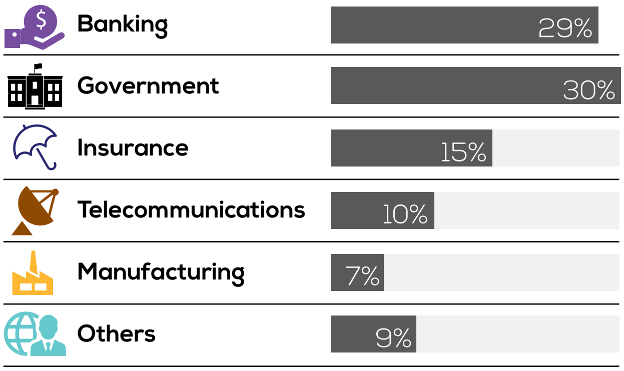
- Academic
- Banking
- Financial Services
- Government
- Healthcare Services
- Insurance
- Legal Advisory
- Professional Services
- Telecommunications
- Others

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

Summary of Findings

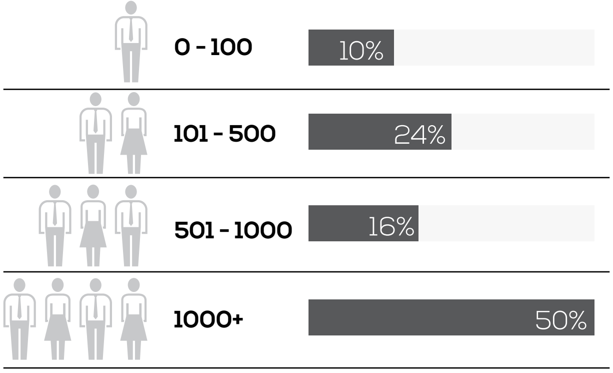
According to the survey findings, 99.4% of respondents have a general understanding of what Cybercrime is. With the many advances in information technology and the transition of social and economic interactions from the physical world to Cyberspace, it is expected that majority of individuals have a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

Majority of the respondents were from the banking industry



10% of the respondents are organisations with 100 and below employees

50% of the respondents are employees of organisations with 1000+ employees. These were mostly from the Banking and Government sectors.



62% of the organisations allow the use of IoTs

Organisations that allow/utilize Cloud Services or IoTs Tech **53%**

48% lack policies to govern the usage o Cloud Services or IoTs Tech

Security concerns are evolving with the rapidly changing nature of CyberThreat and it is paramount that organisations which have adopted cloud and IoT implement policies and procedures to govern the adoption, maintenance and retirement of these technologies.

58% of respondents are concerned about Cybercrime in their organisations

58% extremely concerned about cybercrime in their organisation

72% have experienced Cybercrime in their organisation

72% have experienced cyber crime in their organisation

while

28% have not experienced Cyber-crime

From our analysis, this can be attributed to two main issues:

- Increasing Internet penetration in Kenya at 85% and rising.

- Majority of people do not understand what qualifies as Cyber-crime. A case in point is when a lady saw a skull and bones complete with a voice laughing after her phone was hacked and she quickly threw the phone in the nearby bonfire. As such, a huge percentage of people lack the ability to recognize a Cyber-attack when it occurs.

90% have been impacted by Cybercrime

85% **of the respondents have had an Impact of Cyber crime**

System Downtime	25%
Money Lost	22%
No effect	15%
Inconvenience	15%
Reputation damage	12%
Psychological	10%

Majority of attacks in Kenya are motivated by financial gain – suggesting reasons why financial institutions, telcos, fin-tech companies, micro-lending institutions, Saccos and organisations that deal with transaction processing are primary targets for the Cyber-attacks.

Only 28% reported Cybercrime to the authorities

28% **Reported cyber crime to the authorities**

Did not report to the police	72%
Reported to the police with no further action	6%
Reported to the police, who contacted me /organisation but no further action	6%
Reported to the police, who followed it up to successful prosecution	11%
Reported to the police, who followed it up but no successful prosecution	5%

55% spend less than US $5000 annually for Cyber security

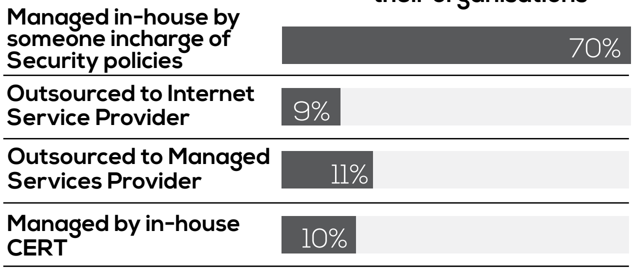
43% **spend less < US $5000 on cyber security**

Dont know their organisation's cyber security expenditure	43%
Spend US $ 1 - 1000	22%
Spend US $ 1001 - 5000	17%
Spend US $ 5001 - 10000	10%
Spend US $ 10000+	7%

Majority of organisations which spend $ 10,000 USD or more came from the banking and financial sectors. This is not surprising since these industries are the most targeted in Cyber attacks.

28% of the organisations outsource their entire security functions

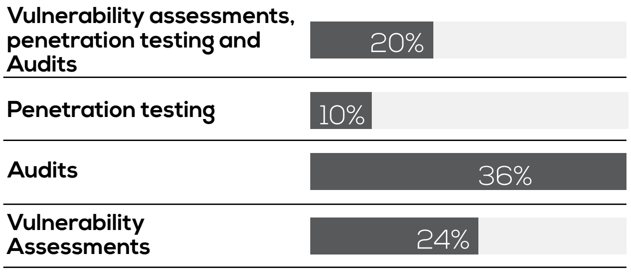
20% of the respondents outsource the entire security function for their organisations



Telcos and large sized banks are key players who have in-house capabilities to manage Cyber security. A critical trait however, noted with in-house managed Cyber security is that, usually the system administrators double up as the personnel in charge of security. As a result, majority of these set-ups lack sufficient skillsets, time and resources to fully manage this role.

80% ofthe organisations carry our security testing techniques in their organzations

80% of the respondents carry out security testing techniques in their organisation



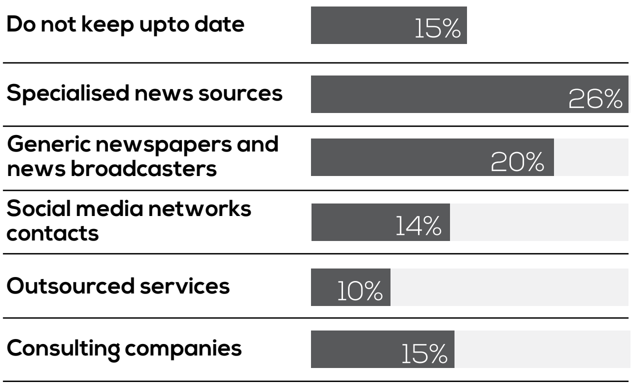
60% of the organisations regularly train their employees on Cyber security isssues

64% of the respondents are regularly trained

while 36% of organisations DO NOT regularly train their staff on cyber security.

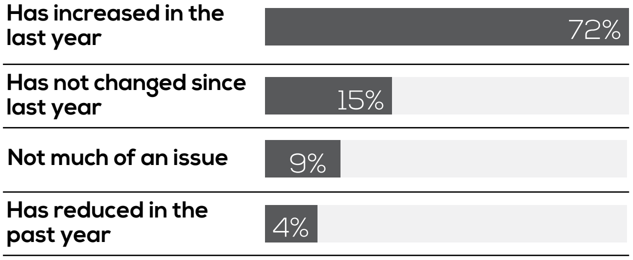
22% of the respondents do not keep upto date with Cyber security news

75% of the respondents keep upto date with cyber security news from various sources



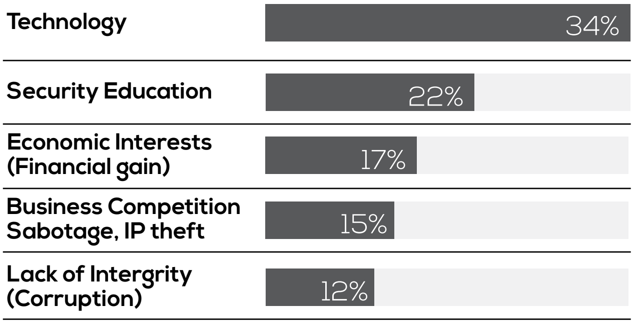
72% believe that Cyber crime has increased in Kenya

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



34% believe that Cyber crime is rooted in technology

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

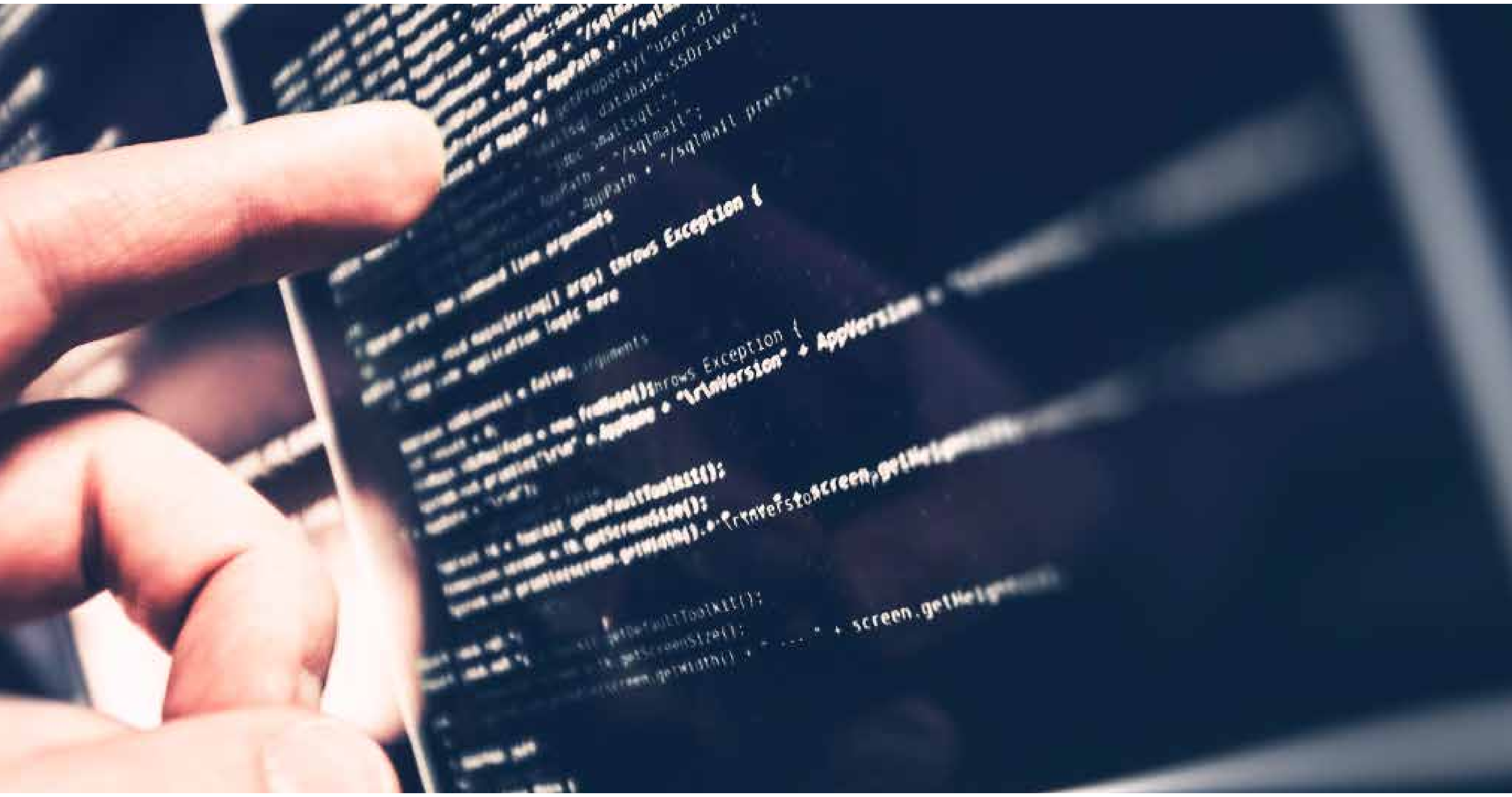


41% of organisations allow the use of BYOD

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

while

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



Sammy Nyambu

Head of ICT

Mwalimu National Sacco

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

Internal accomplices or collaboration in aiding cyber crime.

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

Yes. Growth of social media as a means of information dissemination as opposed to mainstream media has been a big contributor to fake news. Improved bandwidth coupled with smart devices makes it easy to access the internet/ social media; hence easy to share your story whether authentic or not.

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

Previously government agencies, mainstream media were the primary source of information to the vast majority- they then took full responsibility to the accuracy of information they disseminated; however that has since changed with growth of social media as a means/source of information as anyone with access to an online platform is able to tell his story. Government/related organs has a responsibility of coming up with legislation or guidelines aimed at curbing propagators of fake news; whereas end users also have a moral and ethical obligation in ensuring that any form of information disseminated is verifiable and factual

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

On the contrary. If agreed, end users originate content in the form of fake news and the same end users should create content to counter or debunk the fake news. In this way Google and Facebook and all related social sites are left to be what they are built to be – search engines or social networks.

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

Users should at all times verify the source and content of the story; in most cases fake news have no verifiable source.

At all times educate users to countercheck the story against stories posted on the otherwise reputable sites in order to ascertain the veracity of the story.

Users should be made aware that fake news is normally created to push traffic to a specific site; thus the more sensational the story, the higher chances it may be fake.

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 think the African citizenry is ready for e-services with the understanding that respective governments take it slightly further upon themselves to ensure that electricity, connectivity and cost of end user devices is not only affordable but accessible.

The onus to keep the e-service portals secure will rest with the hosting government agencies; where due care must be undertaken to ensure that the citizen data is secure and its privacy assured.

E-services in themselves will among other benefits enhance transparency and accountability thus reducing corruption tendencies, enhance service delivery and efficiency.

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?

Impersonation, being sure that whoever is transacting is actually the person. There needs to be an identification of the person behind the transaction. The challenge is data getting into the wrong hands. The benefits therein are however great.

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

No, however there were reported cases in the country.

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?

Since ransomware is all about encrypting user files and holding them "hostage", with the intention to demand that the user pays a fee to decrypt them and get them back;

educating users on the need to have regular data backup will limit its impact

educate users on the need to patch up or update software often

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

No

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

Increased regulation requirements around the information security domain that will compel organizations to spend in order to comply with regulation

More sensitization and education of Board Directors on information security; highlighting the risks and inherent business impact in the event of an attack

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/universities focus on to encourage innovation in the development of cyber security solutions?

Reevaluate the curriculum to introduce cyber security related courses at our institutions of higher learning.

Though government and private sector partnerships, provide for complementary scholarships for cyber security related courses, setting up of cyber security centric academies etc.

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 target should be around young graduates to enable them to bring out their innovation in cyber security.

Develop incubations for these ideas.

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

Ransomware

There's a trend of cryptocurrency, not sure whether these avenues will impact cyber security. We don't know what new challenges block chain will bring with the new embrace.

Insider threat is real and happening, key loggers and also remote access should be looked into.

As much as there is a rush to adopt new technology, the risks should not be forgotten. Organisations leave themselves vulnerable when they skip the assessing the risks the new tech comes with.

Summarized Findings Report – What are Cybersecurity Gaps in Kenya?

*Reporting approach adopted from Cyberroad-project and survey

Theme	Scenario	Consequence(s)	Mitigation	Identified Gap(s)
Database Security	Limited visibility on activities on the databases.	**1. Fraudulent database postings!** **2. Loss of sensitive information!**	24/7 monitoring of activities within databases. Limit and monitor access to database. Audit and review privileged access to DB.	How can Kenyan 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 Kenyan organisations maintain a patch management program without exhausting resources?
	Employees are trained only after an incident.	**Employees fall victims of social engineering attacks!**	Regular employee training programs that have an effectiveness measuring metric.	How can organisations ensure employees understand the concepts taught during awareness workshops/ trainings?
Training and Awareness	IT Training is done on specific tools.	**IT teams lack the expertise for defensive and offensive security!**	Regular training on both defensive and offensive Cyber security concepts.	How can IT teams widen their gaze from being "tool analysts" to network engineers and architects?
	Board members lack Cyber security expertise and rely on standard audit reports to understand the security posture of organisations.	**Lack of visibility on actual Cyber security posture!** **No standard way of measuring progress and ROI on IT investments!**	Board training to involve reporting metrics for enhanced visibility that can provide a basis and guide on future decision making.	How can Board members shift from the traditional "oversight" role into the proactive Cyber security role?
Network Security Engineering	Limited expertise in the country on Security Architecture/ Engineering skill set.	**Networks are misconfigured to allow easy manipulation and system sabotage!**	Organisations to invest in or outsource security engineers/ architects for network design purposes.	Where can organisations get specialized training on security architecture/ Engineering?

Theme	Scenario	Consequence(s)	Mitigation	Identified Gap(s)
Insider Threats	Greedy and Disgruntled employees are being recruited by cartels to launch attacks	**Compromise of administrator accounts** **Privilege escalation** **Malicious transaction posting** **Data exfiltration** **Sabotage of critical systems**	Audit and monitor activities of privileged accounts Segregation of duties Develop a user access matrix	How can Kenyan 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 Kenyan 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		Telecommunications		Other Industries	
YEAR	’16	’17	’16	’17	’16	’17	’16	’17
Been victims of any cybercriminal activity in the last 5 years; Through work	59% ↑	55%	63% ↑	67%	67% ↓	65%	48% ↑	51%
Organisations spending below $1,000 USD annually on cyber security	33% ↓	30%	45%	45%	30% ↓	27%	48% ↑	50%
Organisations with Cyber Security managed In-house	63% ↓	55%	58%	58%	71%	71%	40% ↑	48%
Yearly training staff on Cyber Security risks	39% ↑	45%	45% ↑	47%	55% ↑	57%	38% ↓	33%
Organisations that allow Bring Your Own Devices (BYODs) usage	20% ↑	26%	60% ↑	61%	49% ↓	40%	60%	60%
Organisations who lack BYOD policy	30% ↑	35%	74%	74%	60% ↓	56%	57% ↓	55%
Organisations utilizing Cloud Services or Internet of Things Tech (Big Data Analytics)	*	46%	*	43%	*	40%	*	58%
Organisations which lack an IoT and Cloud Policy	*	35%	*	71%	*	54%	*	54%

* No statistical analysis done in 2016 on this section.

STEVE MAMBO

Cyber Insurance Consultant & Cyber Security Specialist

Cyber Risk Insurance Satisfying Africa Cyber Security Poverty Line

Cyber Risk or Cyber Liability Insurance is an insurance product designed to cover businesses against all related damage to, or loss of information from, IT systems and related infrastructure. The cover enables organizations mitigate financial risk exposure by offsetting costs involved with recovery, investigation after a Cyber incident. Cyber attacks lead to both direct and indirect costs. Direct costs relate to cost of recovery i.e. Restore data/systems, lost productivity, ransom payments, regulator penalty, forensic charges etc while indirect cost could arise as a result of customer whose data is compromised taking a legal action against the organization. In addition there are other intangible costs e.g. reputation damage that arise from the security breach.

Should African organizations invest in a Cyber Insurance cover?

Cyber threats are inevitable and will likely occur at some point despite all the best efforts at Cyber Risk Management. Cyber Security is not just an issue of protecting from the known but more on the need to prepare for the inevitable.

Dynamic nature of Cyber threats – Cyber threat landscape is expanding, getting more vicious and leading to catastrophic effects to organizations. Cybercrime-as-a-service aggravates the threat to organizations as the number of attacks is also on the rise. The high probability of a Cyber attack or data breach to an organization makes it more expensive to defend.

Cost of Cyber Crime – Cyber crime cost has been on the rise as the threats get more sophisticated. Wannacry Ransomware in 2017 lead to a loss of approx $ 4 billion with over 97 countries affected, in Kenya over 19 organization were impacted as per report by CA. Insider threat highly contribute to loss in Cyber crime, the insider knows the "crown jewels" and leak data or compromise systems and processes for their own advantage.

Increased expectations from regulators and government – Government and industry regulators have formulated policies and laws to address Cyber risks. The regulators expect organizations to have in place Cyber security governance and risk management frameworks that mitigate Cyber risks but also build trust and confidence in the relevant industry. Kenya, Tanzania, Zimbabwe, Ethiopia, Rwanda, Nigeria, Egypt and Morocco are some of the nations at the forefront on enacting Cyber related laws.

Cyber Security is now a boardroom agenda – The board members as part of their fiduciary duties are requires them to monitor and address corporate risk – including Cyber risks. In today environment, where Cyber security is no longer just an IT issue, the board is expected to provide a strategic direction in relation to Cyber risks. Cyber security has become a governance issue for the boards who are increasingly seeking Cyber insurance as a financial instrument for transferring the risk.

Cyber Insurance is catalyst for 'better' security – The due diligence undertaken as part of underwriting a Cyber insurance cover may help improve organization security posture. The underwriting process involves quantifying the organizations Cyber risks which entails reviewing Cyber risk frameworks, policies, defense measures as well as promoting a Cyber security culture within the organization. It is during this process the organization can identify weakness that can be acted upon to reduce their Cyber risk exposure. As the risk exposure is reduced the organization benefits by paying a lower premium for insurance cover.

How do you arrive at the value of Cyber risks?

Cyber risk quantification is the process of evaluating the Cyber risks using modeling techniques to accurately represent an organizations financial exposure. One of the prominent models used to value Cyber risk is VaR (Value at Risk) which has been widely used in the financial service industry.

Cyber VaR calculates the exposure of key assets and liabilities to the variations of Cyber environment in which an organizations computing infrastructure is operated. The model incorporates organizations financial posture, threat scenario and Cyber security defense posture. Cyber VaR model estimates the likely loss an organization might experience from Cyber attacks over a given period of time. i.e, "Given a successful Cyber attack, a company will lose not more than X amount of money over a period of time with 99% accuracy". Cyber VaR model greatest benefit is that it both quantifies risk and expresses it in financial terms that can be understood by boards and executive suite. The Cyber VaR concept can help with critical decisions, such as defining Cyber risk appetite, assessing the optimal allocation of Cyber risk management resources and determining risk transfer mechanism to be adopted.

Does Cyber insurance replace Cyber security?

Cyber insurance can't prevent Cyber attacks however it will keep your organization on a stable financial footing should Cyber attack occur. Just like having a fire insurance policy doesn't prevent the risk of a fire but it comes in handy to compensate for the loss from the fire. Cyber Insurance is a component within Cyber risk management (Risk transfer) and doesn't remove the responsibility of trying to defend organization from Cyber attacks. Making Cyber security investment still makes sense and is beneficial to the organization as they can negotiate for lower premiums. The Cyber security investment will be an indicator of measures taken to mitigate Cyber risks which reduces VaR. Cyber insurance compliments risk management by protecting the organization from financial exposure that emanates from Cyber risks.

How does the Computer & Cyber Crime bill and CBK Cyber Security Guidance note related to Cyber Insurance?

Kenya is in the process of enacting Cyber crime laws under the Computer & Cyber Crime bill 2016. The bill defines offences by a corporate body and further passes the liability to the corporate body where crime is committed by the body or employees of the corporate. Organizations will need to factor Cyber litigation costs and investigation costs for Cyber crimes alleged to have been committed by the organization or its principal officer of the organization. Third party Cyber insurance policies cater for litigation support as well penalty settlement which as per the bill shouldn't exceed fifty million shillings.

The CBK Cyber risk guidance note outlines the minimum requirements that institutions shall build upon in the development and implementation of strategies, policies, procedures and related activities at mitigating Cyber risk. The note further issues responsibilities to several stakeholders in the banks starting with the board, senior managers and CISO. A Cyber insurance cover enables the bank define its risk appetite as part of Cyber risk quantification as well offer strategic direction of Cyber security preparedness. By taking up a cover the bank is able to demonstrate that it has taken the level best risk mitigation controls and where there exists a residual risk, the bank has transferred that risk through a Cyber insurance cover.

Cyber insurance may be that magic pill that is needed to absorb the financial losses from Cyber attacks. It neither replaces Cyber security but rather compliment Cyber risk mitigation strategies adopted by organizations more so provides cushion against financial exposure to the organization.

R
T
Y
U
S
F
G
H
J
V
B
N

Cost of Cyber Crime

Analysis – 2017

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

From our research and analysis, we estimate that Cyber-attacks cost Kenya businesses around $210 million a year, which includes direct damage plus post-attack disruption to the normal course of business.

Kenya

Cost of cyber-attacks

$210m annually

Methodology

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

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

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

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

A significant proportion of this cost comes from the insider threat, which we estimate at $6.3M per annum. In all probability, and in line with our worst-case scenarios, the real impact of Cyber crime is likely to be much greater. As for measuring costs, this report decomposes the cost based on these 4 categories:

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

$210m annually

Type & Cost of Cyber Crime in Kenya

Insider Threat	30%	$63M
Attacks on Computer Systems (Unauthorized Access and Malware)	20%	$42M
Social Engineering and Identity Theft	15%	$21M
Email Spam & Phishing	12%	$32M
Data Exfiltration	10%	$25M
Online Fraud Scams	8%	$17M
Ransomware	5%	$11M

TOTAL $210M

Cost of cyber crime Industry/Sector Analysis in Kenya

Banking & Financial Services	33%	$70M
Government	24%	$50M
E-Commerce	7%	$15M
Mobile based transactions/ e-commerce/e-payment	12%	$25M
Telecommunications	14%	$30M
Other Sectors/ Industries	10%	$20M

TOTAL $210M

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 Kenyan 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

Mobile money in Kenya is considered a key transaction channel, with a record of $27 Billion mobile money transfers in one year! With that growth comes a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks and risky consumer behavior. We have seen numerous counts of breaches as a result of insecure configurations, use of malware infected phones and reverse engineering of the mobile code. Whether or not an institution uses a proprietary or third-party mobile banking application, the risk posed by these systems are still inherent.

FInancial Services

In 2017, the number of successful attacks launched against financial services doubled. Saccos, Cooperatives and microfinance institutions have seen rapid growth in Kenya however, these institutions have not prioritized Cyber security. This has made them a popular target for opportunistic Cybercriminals. Larger institutions have invested more in Cyber security in comparison to smaller institutions hence making the smaller fish 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 ALL INDUSTRIES, CYBER SECURITY COMES ALONG AS PART OF THE PACKAGE. IN KENYA, 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 Services

Mobile money in Kenya is considered a key transaction channel, with a record of $27 Billion mobile money transfers in one year! With that growth comes a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks and risky consumer behavior. We have seen numerous counts of breaches as a result of insecure configurations, use of malware infected phones and reverse engineering of the mobile code. Whether or not an institution uses a proprietary or third-party mobile banking application, the risk posed by these systems are still inherent.

Hospitality & Retail

The hospitality industry is primarily public-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.

Martin Mirero

ICT Director,

Huduma Center

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

Wannacry without a doubt was one of the biggest things we saw. It was the first issue that fully awakened the reality of the cyber security eco system.

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

Yes, especially through social media. We have seen the effects around us. We have seen clones of government websites come up and being used to propagate fake news.

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

All stakeholders although the government needs some legislation around this, we are abit behind on this, a lot needs to be done. The users also need to be educated on their part. As for Telcos/ISPs, this weighs in on net neutrality, I believe information should be available to all, things like censoring or blocking information should go through a legal process otherwise I would be very weary of that as it highly likely to be misused.

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

No. We should just use the already existing mechanisms of regulating fake news such reporting or lodging complaints. These mechanisms should be strengthened.

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?

Yes, they are very much ready to consume these services. There has been overwhelming support. On the issues of privacy, security and fraud, citizens are blissfully ignorant, they are not aware of the risks around this. They trust the government is keeping their data safe. It is a function of citizenry awareness, users need to be taught how to differentiate clone sites from the original sites.

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?

Identity fraud. There is not a proper mechanism to always authenticate that the person is the actual person.

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

No. We have our perimeter covered. We were aware of the Wannacry attacks we are also aware that some of the institutions were affected that may have not disclosed.

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

We have got to partner with industry leaders like Serianu, it is very key as they have wider and better view of the cyber security environment. Organisations also need to strategize on a cyber security roadmap.

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

Not nearly. A lot of investment needs to be done here as well as policy creating and developing skills within the organisations as well in skills, technology.

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

Drive awareness/sensitization.

Benchmarking in other countries or organizations and compare where we are with organisations in the same industry.

Sharing of incidences in a trusted framework.

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?

We need to start somewhere, we probably need to white label some open source solutions that fit into our needs and nature of incidences.

Encouraging the collaboration of academia and the private sector.

Support from the government into initiatives already in progress.

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?

Work is for the local players to build something. We need to build compelling products that run against the already existing international ones. Association with Private sector with the help of regulators to makes sure certain percentages are of local purchases.

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

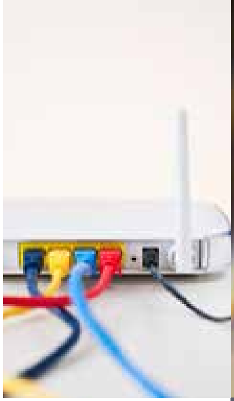
Ransomware on a bigger scale.

Breaking into cryptocurrencies using quantum computing.

Artificial Intelligence progression is very amusing and these agents probably could be capable of creating their own malwares or computations.

Spying is on the rise, case in point the African Union incident, as a continent we are a bit too trusting.

Reiterate the issue of sensitizing and awareness on cyber security.



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

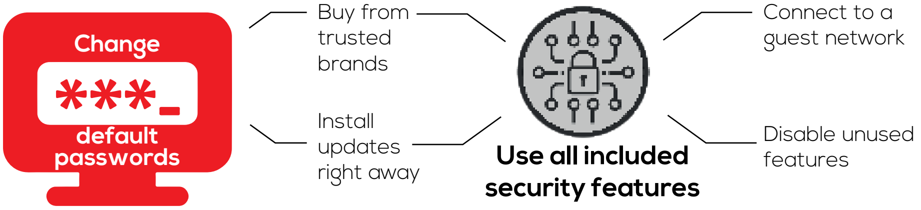
IoT is changing our traditional approach to how we live and interract with our homes. A number of houses, apartments and estates in Kampala have CCTV surveillance, Smart TVs, DVRs and connected thermostats that you can monitor and handle from any part of the world. These gadgets add convenience like 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.

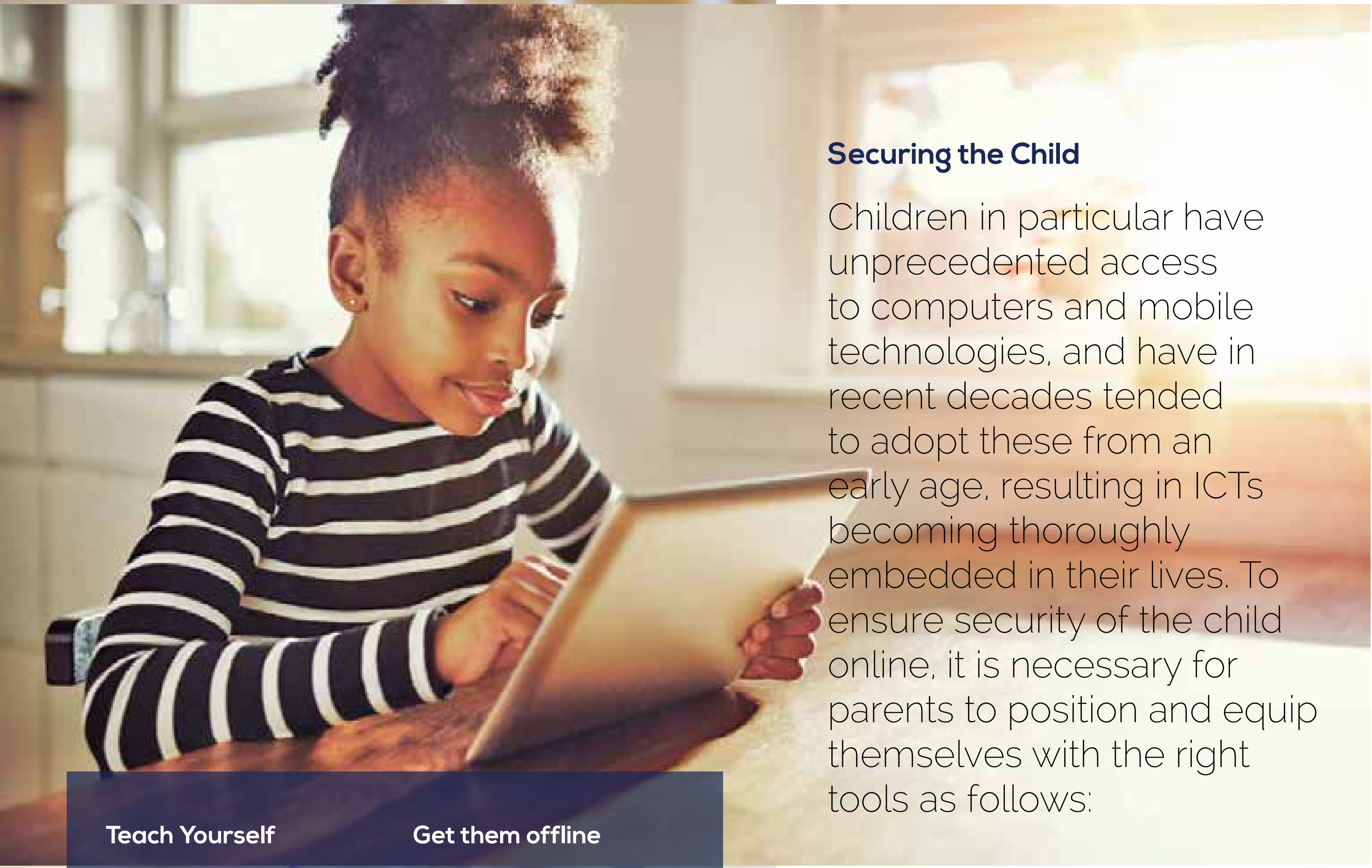
As a home owner, you run the risk of being blocked by certain sites, your internet speed may be slow due to the excessive bandwith utilization and you will incur higher costs.

Security Tips



Security Begins at Home

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



Securing the Child

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

Teach Yourself

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

Check Privacy Settings

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

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

Get them offline

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

Cyber Bullying

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

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

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

Parents can

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

Kenneth Ogwang

CIO

East African Breweries Ltd

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
VELOCITY
VOLUME
LIMITS

- Scanning from external IP
- Bruteforce attempts
- Excessive DNS queries
- IP conflicts

- Traffic to core VLAN from extenal IP
- Multiple posting on DB
- Remote Access tool detected
- Auditry disabled

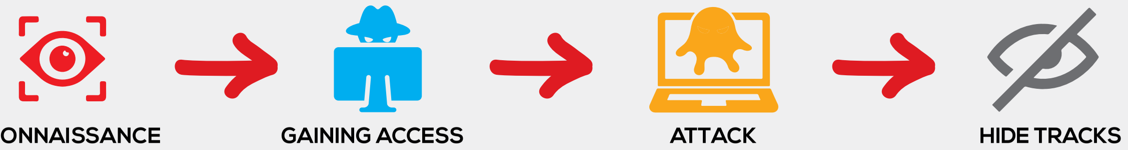
- Dormant account activity
- Bulk transaction processing
- Transaction over limit

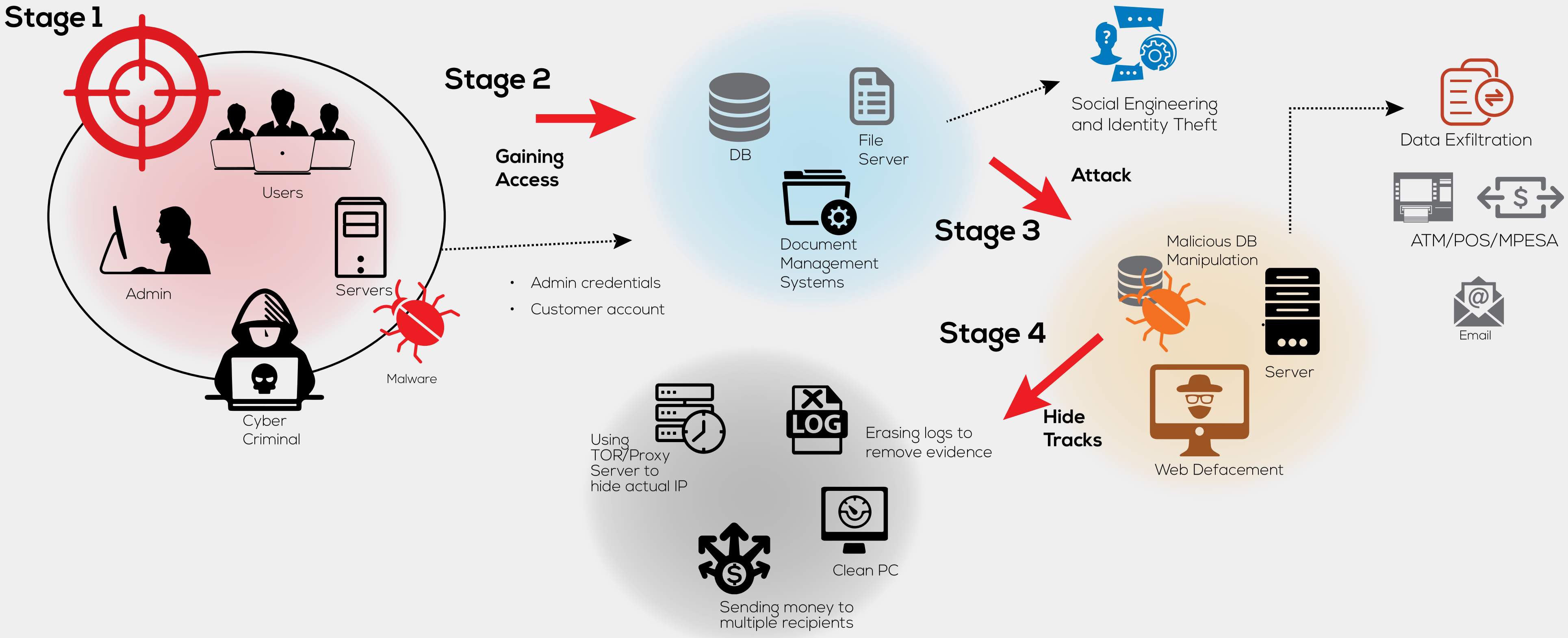
- Logs deleted
- System unavailable
- AV disabled

KEY SYSTEMS

Firewall
Antivirus
DNS
DHCP
AD
Active Directory

ATTACK STAGES





JAMES NYAKOMITTA

CIO, APA Apollo Group

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

Africa remains an exciting market for business growth as seen in the prior years and Cyber security plays a very critical role in securing the future of the continent. 2018 a very important year for Kenya in addressing some of the major Cyber security challenges experienced in 2017. Governments and institutions have to make additional investments in security, which must be done in parallel with the growth in GDP. The country has made great efforts in cross-industry discussions on Cybersecurity and passed into law, the "Computer and Cybercrimes Act, 2017, which will play a key role in assisting law enforcement agencies to firmly deal with offences relating to computer systems and Cybercrimes including timely and effective detection, investigation and prosecution of offenders. The Act also makes provisions for facilitating international co-operation in dealing with Cybercrime matters. Continued efforts must be made to update these laws and educate citizens and policy makers on critical Cyber issues.

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

The year 2017 will be remembered for some big moments in the world of Cybersecurity. Threats and attacks kept coming in like "rapid-fire" through ransomware, distributed denial of service (DDoS) attacks, phishing attacks, the Internet of Things, social engineering, among others. On May 12, 2017 for example, the world was stunned by an unprecedented global Wanacry ransomware attack that infected more than 200,000 computers in 150-plus countries. The attack severely impacted the UK's National Health Service operations, as well as FedEx, Spanish Telefonica, French Renault factories, a Chinese energy company and the Russian Interior Ministry. The malware, spread rapidly among connected networks because it acted as a worm that self-propagated via the EternalBlue exploit. Examples of other top Cyber security issues experienced in 2017 include: NotPetya, BadRabit, IoT Botnets, Broadpwn, BlueBorne, KRACK, and many more. Moving forward, information security professionals across the globe, will have to think like hackers in order to stay ahead of the challenge.

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

Yes. This is a major problem in Kenya, and specifically with regard to social media, which has continued to be the dominant source of fake news and has significantly amplified the impact of this vice over the past decade. WhatsApp, for example, continues to play a key role in mass distribution of these stories. Besides being more pervasive than any social network in Kenya, Whatsapp is fast, simple, and much more intimate compared to Facebook or Twitter. These factors rapidly increase a fake news story's persuasive power. In many ways, Whatsapp, may be the biggest problem that Kenyans have when it comes to fake news.

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

Everyone has a responsibility to combat the scourge of fake news. This, in my view ranges from supporting investigative journalism, reducing financial incentives for fake news, and improving digital literacy among the general public. While it is important for news organizations and content distribution platforms to call out fake news and disinformation without legitimizing them, it is increasingly becoming critical for social media platforms to put in place automatic hoax detection systems powered by specialized algorithms to detect and minimize the spread of fake news.

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

There is no doubt influential platforms like Facebook, WhatsApp, Google, Twitter, among others have have become a key conduit of false narratives. However, I do not advocate for an overly restrictive regulation of Internet platforms in an open society like Kenya, as this can set a dangerous precedence which can encourage regulators and government agencies to continue and/or expand censorship. Instead, the companies should double their efforts in detecting and minimizing the spread of fake news. Most fake news posted on Facebook, for example, are financially motivated, aiming for clicks that lead users to websites containing mostly ads. Facebook has made tremendous progress though in preventing the spread of false news, by demoting the posts thereby cutting their traffic by more than 80 percent. This destroys the economic incentives spammers and troll farms have to generate these articles in the first place. Repeat offenders posting false news should have their advertising rights removed, their distribution reduced, and their opportunities to monetize restricted.

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

Awareness campaigns and educational programs are key. Ahead of the 2017 elections in Kenya for example, Facebook rolled out an educational tool that would help its users spot and limit the spread of fake news stories on its platform, just a few days before the hotly-contested general election. Facebook, together with its WhatsApp platform, placed adverts in some of the country's national newspapers and radio stations giving consumers tips on how to spot false stories. Most importantly, these influential platforms should put new initiatives to understand how users decide whether or not, information is accurate based on the news source

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 ultimate goal of government driven e-services is to offer increased portfolio of public services to citizens in an efficient and cost effective manner. This would in turn save money and time as well as facilitate better communication between governments, citizens and businesses. Additionally, e-services create social benefits for the citizens of a country. For countries that have a widely dispersed population, government driven e-services allows citizens situated in remote areas to have access to same services that citizens within major cities would enjoy. African citizenry however are not fully ready to consume and utilize these services, main reason being that a huge majority of the population are still computer illiterate. Full implementation of government driven e-services can therefore make life very difficult for this class of citizens particularly if alternative previous ways of accessing government services are withdrawn.

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?

First and foremost, it is important to understand that digitization results in ease of access of data, which is largely a "double-edged sword". The government sometimes can pass legislations undesirable to citizens without adequate information of the citizens, and then go on to use the easily-accessible data for its purpose. Secondly, adoption of e-governments can lead to privacy issues. There is a risk of private data of citizens getting stolen as well as the possibility of rogue government employees misusing private data, which can easily lead to fraud. Encryption and security therefore become very important. There are no specific incidents I can site in Kenya, however, the impact of these risks can be very high, hence the need for proper legislation for data governance around e-services.

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

2017 was particularly a difficult year. We had cases of attempted attacks through emails with attachments and links to dangerous sites. However, we assessed all vulnerabilities that could potentially be exploited by this threat and revamped our security controls so as to mitigate any associated risks.

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

We responded by implementing "layered security" for our infrastructure as well providing continuous security awareness training to all staff.

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

Ransomware is a multi-million-dollar crime operation that strikes everyone from financial institutions to hospitals to government departments to online stores; name them. It is such a profitable scheme that experts say traditional Cyber thieves are abandoning their old ways of making money (stealing credit card numbers and bank account credentials) in favor of ransomware. It is true there is shortage of skilled resources in Africa. However, the following simple initiatives can help limit the impact of ransomware cases:

i. Ensure antivirus is installed and up to date across all endpoints within the business. Keep in mind, antivirus software are based on signatures so new variants may and will slip through the cracks, but this could easily be a first line of defense.

ii. Establishing continuous security awareness campaigns that stress the avoidance of clicking on links and attachments in email. Ask yourself these questions when receiving an email message with a link or an attached file: 1) Do you know the sender? 2) Do you really need to open that file or go to that link? Phishing is a common entrance vector for ransomware and because most end users never think twice, it is extremely successful.

iii. Backup the data. There are a lot of options here, from backing up to cloud providers to local storage devices or even network attached drives, but each comes with a certain level of risk. It is important to detatch the external storage device once a backup is taken so that if ransomware does infect the computer, it won't be able to infect the backup

iv. Patching commonly exploited third party software such as Java, Flash, Adobe and majority of other applications will undoubtedly prevent many of these types of attacks from even being successful in the first place.

v. Limit the ability of employees who do not need the authority to install software and limit access of employees to only that data to which they need access

vi. Got an infection? Disconnect: In case of an infection, the administrators should not only disconnect infected systems from the corporate network, but they should also disable Wi-Fi and Bluetooth on machines to prevent the malware from spreading to other machines via those methods.

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

Historically, the lack of an adequate budget has been a key challenge in addressing Cyber security issues in organizations. CISOs, CIOs and other security executives have struggled for years to get their budget requests approved, so they can put at least satisfactory safeguards in place. As a result of the growth of infosec industry, which, naturally, correlates to the development of IT industry as a whole; this situation has changed significantly in the past years and organizations, both private and government are investing much more money in Cyber security, both in terms of technology and human capital. However, despite the fact that Cyber security spending is going up, Cybercrime is not slowing down at all.

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

Investing more money in security technology is not the only thing that organizations need. Effective spending has to be based on a clear understanding of what security priorities the company has. The organization has to focus on the right things such as automating patching, ensuring adequate traffic filtering layers, implementing layered security or defense in-depth, focus on employee education, as well as dedicating more resources to proactive protection other than simple reactions to ongoing Cyber threats.

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?

This remains a critical gap in Africa. National governments and Universities must make investment in training and education to improve understanding of Cyber security as well as focus initiatives focused developing Cyber security solutions within Africa. Many investigators, for example continue to only use open source tools that make it incredibly difficult to investigate advanced Cyber crime cases.

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?

Today, companies are more informed security buyers, looking for efficient and effective investments rather than mere silver bullets. Cyber security has evolved into a central board topic and a core business concern, and the private sector and consumers of imported Cyber security products in Africa must play a key role in supporting local players to start developing African grown Cyber security solutions and services.

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

What's HOT is likely getting HOTTER in 2018. More sophisticated hacker tricks, phishing attempts, data breaches, new forms of malware, more expensive ransoms, Internet of Things (IoT) device problems, AI and machine learning gone astray (as a Cyberweapon), cryptocurrency problems, cloud computing breaches and plenty more of everything we already saw in 2017. These are going to dominate the Cyber security space in 2018. Digital extortion for example, will be at the core of most Cyber criminals' business model and will propel them into other schemes that will get their hands on potentially hefty payouts. Global losses from business email compromise scams will probably increase and threat actors will ride on machine learning and blockchain technologies to expand their evasion techniques. Gartner predicts that by 2022, half of all security budgets for IoT will go to fault remediation, recalls, and safety failures, rather than to protection. Most organizations especially in Africa don't have budgets for IoT security now, but this will be important moving forward..

Jeff Karanja

Information Security Consultant

Ransomware: A Growing Threat

One of the most debilitating attack vectors we are experiencing today via ransomware. This, coupled with the fact that malware authors are opting to use custom-written libraries and methods instead of reusing off-the-shelf packages, presents a very formidable challenge to individuals, security researchers, and organisations at large.

Anatomy of a Ransomware Attack

1. The malware author generates an encryption key pair and incorporates the public key in the malware's code.
2. The malware is deployed using any number of delivery strategies, e.g. targeted spear phishing, spam e-mail, Trojan download, malicious URL, e-mail attachment.
3. Once the malware is on the system, it starts by generating a random symmetric key and encrypts the victim's data using that key.
4. The public key, inserted into malware by threat actor, is then used to encrypt the symmetric key that was generated in Step 3.
5. The malware proceeds to lock the screen and puts up on the screen a ransom note with instructions on how to pay the ransom, including a deadline countdown timer.
6. The victim sends a unique, asymmetric ciphertext (generated by the malware) and proof of payment to the attacker.
7. The attacker receives payment and proceeds to decrypt the asymmetric ciphertext using their private key.
8. The attacker sends a unique symmetric key to the victim that will be used to decrypt the encrypted data so the user can gain back access to their data. This last step is not guaranteed.

Organisational Challenges

Organisations across the board are facing strenuous challenges as they strive to enhance their security posture. Below are the top challenges we have observed since our last report:

- Budget allocation – One of the primary prohibitive obstacles to developing and sustaining a robust Cybersecurity ecosystem.
- Low Cybersecurity Maturity Posture – Lack of skilled professionals to develop, spearhead and implement customized Cybersecurity roadmaps for their organisations.
- Network Architecture – Poor and inconsistent network design without proper segmentation or access control.
- Cloud Deployment – Lack of awareness when it comes to service provider security control implementation. Hire a competent firm to perform a SAS 70 Audit and request for a Type II Service Auditor's Report beforehand.

Counter measures

1. Implement security awareness training for the entire organisation.
2. Implement patching policies and supporting infrastructure to test and deploy patches within your organisation.
3. Employ Anti-virus/Anti-malware solutions that carry out heuristic analysis and rootkit detection to tackle evasion techniques such as the use of oligomorphic, polymorphic, and metamorphic engines

4. Actively monitor privileged account usage on your network to identify outliers and anomalous activity on your network.
5. Implement strict access controls on sensitive resources in your network.
6. Implement e-mail filters to block spam, phishing and spoofed e-mails. Employ technologies such as SPF, DKIM and DMARC collectively to complement existing e-mail security controls.
7. Stay informed
8. Ensure your organisation has a business continuity plan and an IT disaster recovery plan.
9. Implement Application Whitelisting
10. Implement a SIEM or open-source solution with similar reporting capability (e.g. OSSEC)
11. If a host on your network has been infected, immediately disconnect it from the network (physically) to prevent further spreading before malware removal.
12. In case of ransomware infection, do not pay the ransom. Restore from backups. There is no guarantee you will get your data back. Paying the ransom only achieves to guarantee a successful POC (Proof of Concept) extortion exercise for the threat actor.

History of Ransomware

1989 – **AIDS Trojan:** Distributed via 20,000 infected diskettes.

2006 – **Archievus:** Use of RSA encryption to encrypt files.

2011 – **Unnamed Trojan:** mainstream anonymous payment services.

2012 – **Reveton:** the rise of "police-based" ransomware .

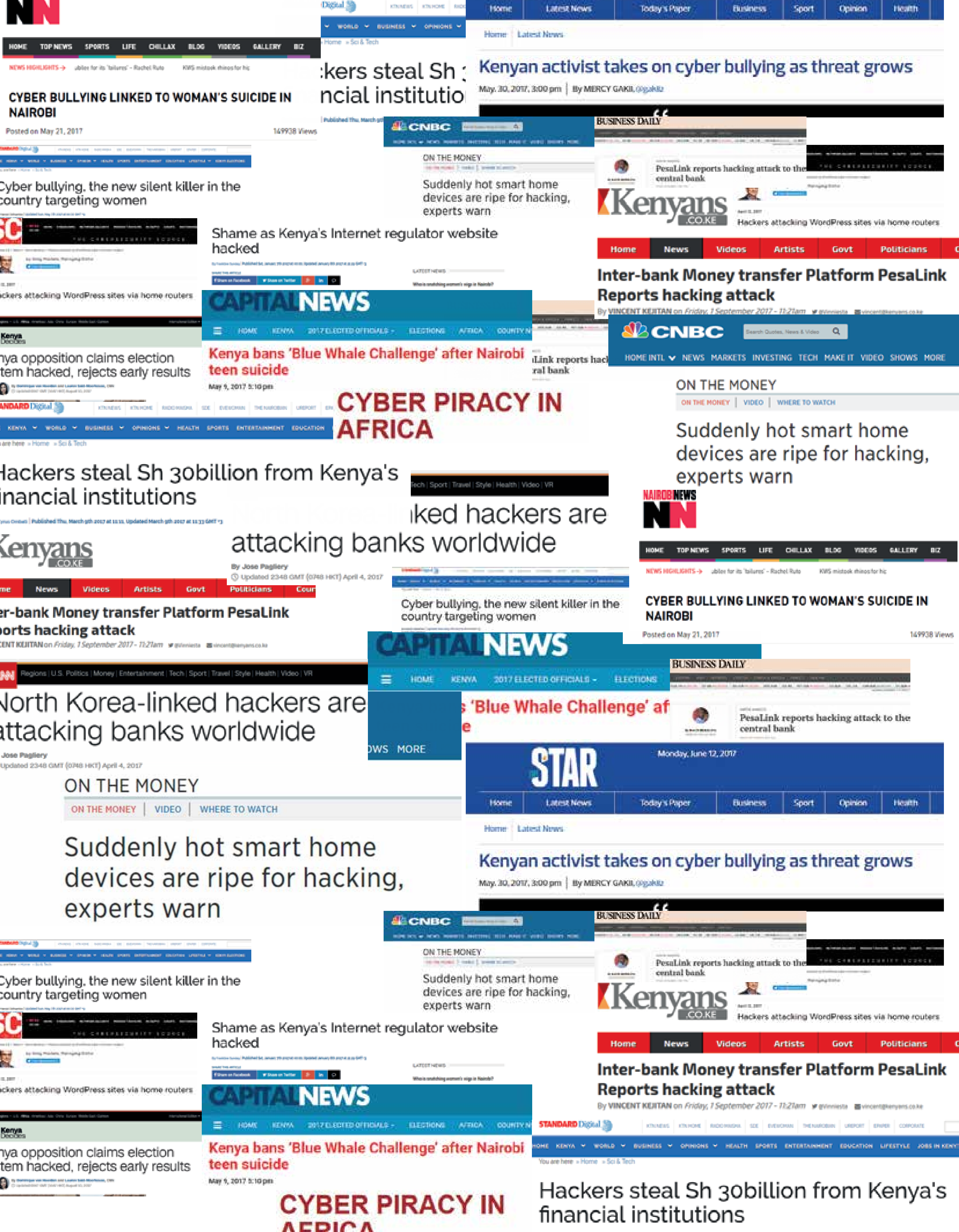
2013 – **Cryptolocker:** uses e-mail as primary attack vector.
2013 – **Locker:** Extorted $150 ransom, payable via Perfect Money or QIWI Visa Virtual Card number.
2013 – **CryptorBit:** corrupts the first 1,024 bytes of data on any file. Leverages Tor and Bitcoin for anonymity and payment.

2014 – **CBT-Locker** (Curve-Tor-Bitcoin Locker): communicates with C2 server directly via Tor.
2014 – **SynoLocker:** Attacked Synology NAS devices by encrypting files individually.
2014 – **Simplocker:** first mobile ransomware that actually encrypted files (images, documents, and video) using AES encryption.
2014 – **Cryptodefense:** Uses Tor and Bitcoin for anonymity. Uses Windows built-in encryption CryptoAPIs using 2048-bit RSA encryption.
2014 – **CryptoWall:** Exploited Java vulnerability. Also delivered via exploit kits such as Angler.
2014 – **Cryptoblocked:** only encrypts files less than 100MB. Skips Windows or Program Files folders on C: drive and uses AES encryption.
2014 – **OphionLocker:** Uses ECC (Elliptical Curve Cryptography) encryption.
2014 – **Sypeng:** One of the first Android-based ransomware delivered via fake Adobe Flash updates in SMS messages.
2014 – **Koler:** Considered the first "Lockerworm" as it contained self-propagating techniques within the code.

2015 – **Pclock**: Encrypts files within a user's profile. Deletes and disables volume shadow copies.
2015 – **TeslaCrypt:** CryptoWall variant that targets popular video game files
2015 – **LowLevel04**: Spreads via brute force attacks on hosts with Remote Desktop or Terminal Services. Encrypts files using AES encryption; encrypts key using RSA encryption
2015 – **Chimera:** the hackers threaten to publish the victim's encrypted files on the internet if the victim does not pay.

2016 – **Ransom32:** First ransomware written in JavaScript for cross-platform capability on Linux, Mac OSX, and Windows.
2016 – **7ev3n:** Payment demand was one of the highest (13 Bitcoin) and was specifically developed with capabilities to ensure there was no possible way of recovering encrypted files.
2016 – **L0cky:** Aggressively spread via spear phishing campaigns and leveraging the Dridex infrastructure.
2016 – **SamSam/SAMAS:** The threat actors specifically distributed it to vulnerable JBoss servers after vulnerability assessment using JexBoss tool.
2016 – **KeRanger:** First official Mac OSX-based ransomware. Delivered via a Transmission BitTorrent client and signed with a MAC development certificate, effectively bypassing Apple's GateKeeper security software.
2016 – **Petya:** Delivered via DropBox and overwrote the MBR (Master Boot Record). Used a fake CHKDSK prompt while encrypting the drive.
2016 – **Maktub:** Used a Crypter. Performed offline encryption using Windows CryptoAPI.
2016 – **Jigsaw:** Threatened to delete a file every 60 minutes if the $150 ransom was not paid.
2016 – **CryptXXX:** Spread via multiple exploit kits, primarily Angler. Includes ability to monitor mouse activity, Anti-Sandbox detection, custom C2 communication protocols, and payment through Tor.
2016 – **Zcryptor:** One of the first "CryptoWorms", primarily spread through spam email.
2016 – **Cerber:** Leverages Ransomware-as-a-Service (RaaS) model whereby malware author nets 40% of paid ransom and affiliates keep 60% via Bitcoin and Tor. Uses RC4 and RSA algorithms for encryption.
2016 – **Petya:** Infected Master Boot Record (MBR) used by NTFS file systems. Installs a payload that encrypts the file tables the next time the system is booted, essentially blocking the system from booting into Windows until the ransom is paid.

2017 – **WannaCry:** Rapidly spread through the internet by leveraging the EternalBlue exploit.
2017 – **NotPetya:** It erases the first sectors of a disk, and although it demands a ransom to be paid, victims have little to no chance of recovering their data even if the ransom is paid as the MBR is completely overwritten and not encrypted like Petya does.



HOME TOP NEWS SPORTS LIFE CHILLAX BLOG VIDEOS GALLERY BIZ

CYBER BULLYING LINKED TO WOMAN'S SUICIDE IN NAIROBI

Posted on May 21, 2017 149938 Views

:kers steal Sh 3
ncial institutio

Home Latest News Today's Paper Business Sport Opinion Health

Home | Latest News

Kenyan activist takes on cyber bullying as threat grows

May. 30, 2017, 3:00 pm | By MERCY GAKII @gakiiz

Cyber bullying, the new silent killer in the country targeting women

CNBC

ON THE MONEY

Suddenly hot smart home devices are ripe for hacking, experts warn

BUSINESS DAILY

PesaLink reports hacking attack to the central bank

Kenyans.CO.KE

Hackers attacking WordPress sites via home routers

Shame as Kenya's Internet regulator website hacked

Home News Videos Artists Govt Politicians

Inter-bank Money transfer Platform PesaLink Reports hacking attack

By VINCENT KEJITAN on Friday, 1 September 2017 - 11:21am

CAPITAL NEWS

HOME KENYA 2017 ELECTED OFFICIALS ELECTIONS AFRICA COUNTY N

Kenya bans 'Blue Whale Challenge' after Nairobi teen suicide

May 9, 2017 5:10 pm

nya opposition claims election
tem hacked, rejects early results

CYBER PIRACY IN AFRICA

STANDARD Digital

KENYA WORLD BUSINESS OPINIONS HEALTH SPORTS ENTERTAINMENT EDUCATION

Hackers steal Sh 30billion from Kenya's financial institutions

HOME INTL NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS MORE

ON THE MONEY | VIDEO | WHERE TO WATCH

Suddenly hot smart home devices are ripe for hacking, experts warn

NAIROBI NEWS

CYBER BULLYING LINKED TO WOMAN'S SUICIDE IN NAIROBI

Posted on May 21, 2017 149938 Views

Regions | U.S. Politics | Money | Entertainment | Tech | Sport | Travel | Style | Health | Video | VR

North Korea-linked hackers are attacking banks worldwide

By Jose Pagliery

Updated 2348 GMT (0748 HKT) April 4, 2017

STAR

Monday, June 12, 2017

Kenyan activist takes on cyber bullying as threat grows

May. 30, 2017, 3:00 pm | By MERCY GAKII @gakiiz

Suddenly hot smart home devices are ripe for hacking, experts warn

PesaLink reports hacking attack to the central bank

Cyber bullying, the new silent killer in the country targeting women

Hackers attacking WordPress sites via home routers

Shame as Kenya's Internet regulator website hacked

Inter-bank Money transfer Platform PesaLink Reports hacking attack

By VINCENT KEJITAN on Friday, 1 September 2017 - 11:21am

Kenya bans 'Blue Whale Challenge' after Nairobi teen suicide

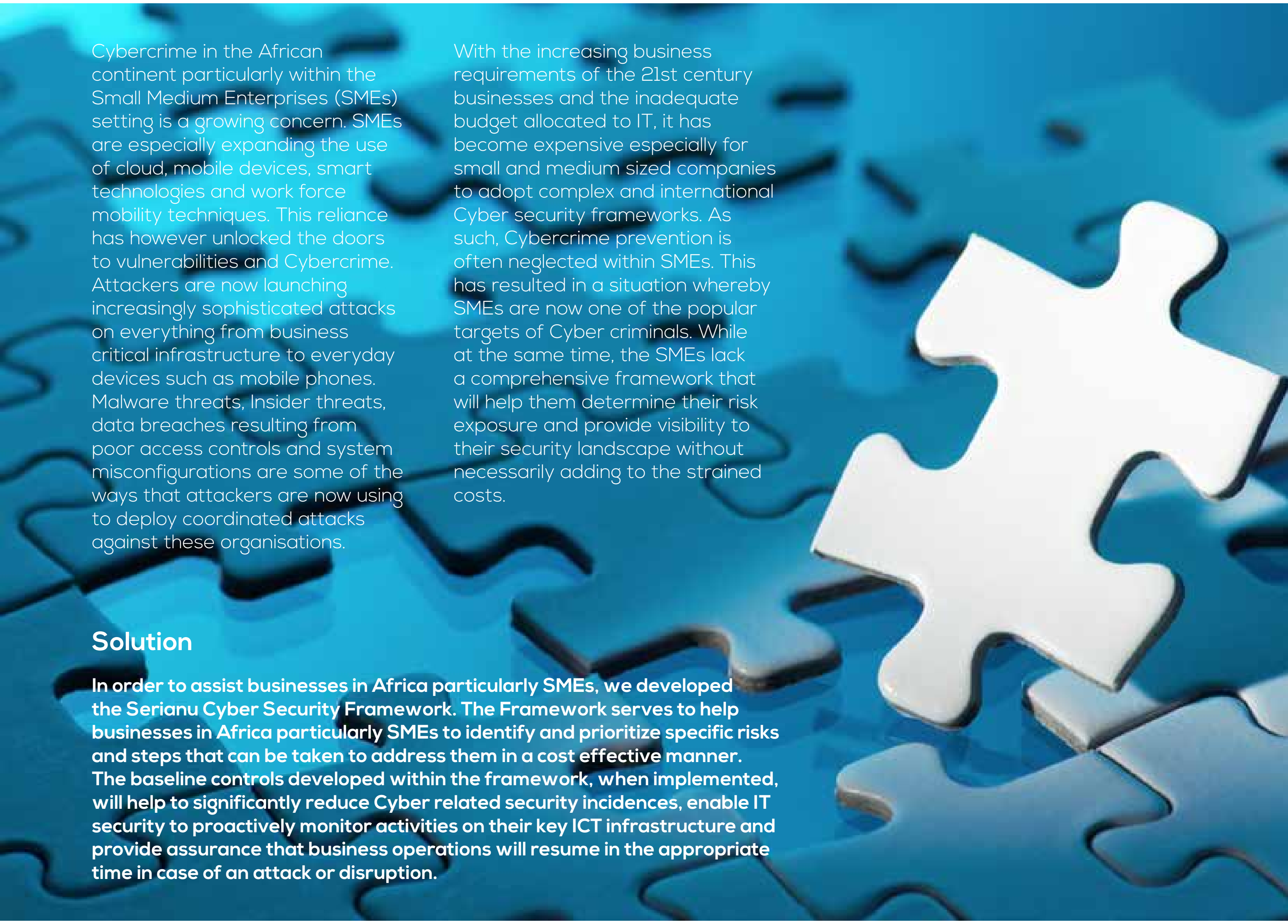
May 9, 2017 5:10 pm

nya opposition claims election
tem hacked, rejects early results

Hackers steal Sh 30billion from Kenya's financial institutions

CYBER PIRACY IN AFRICA

Africa Cyber Security Framework



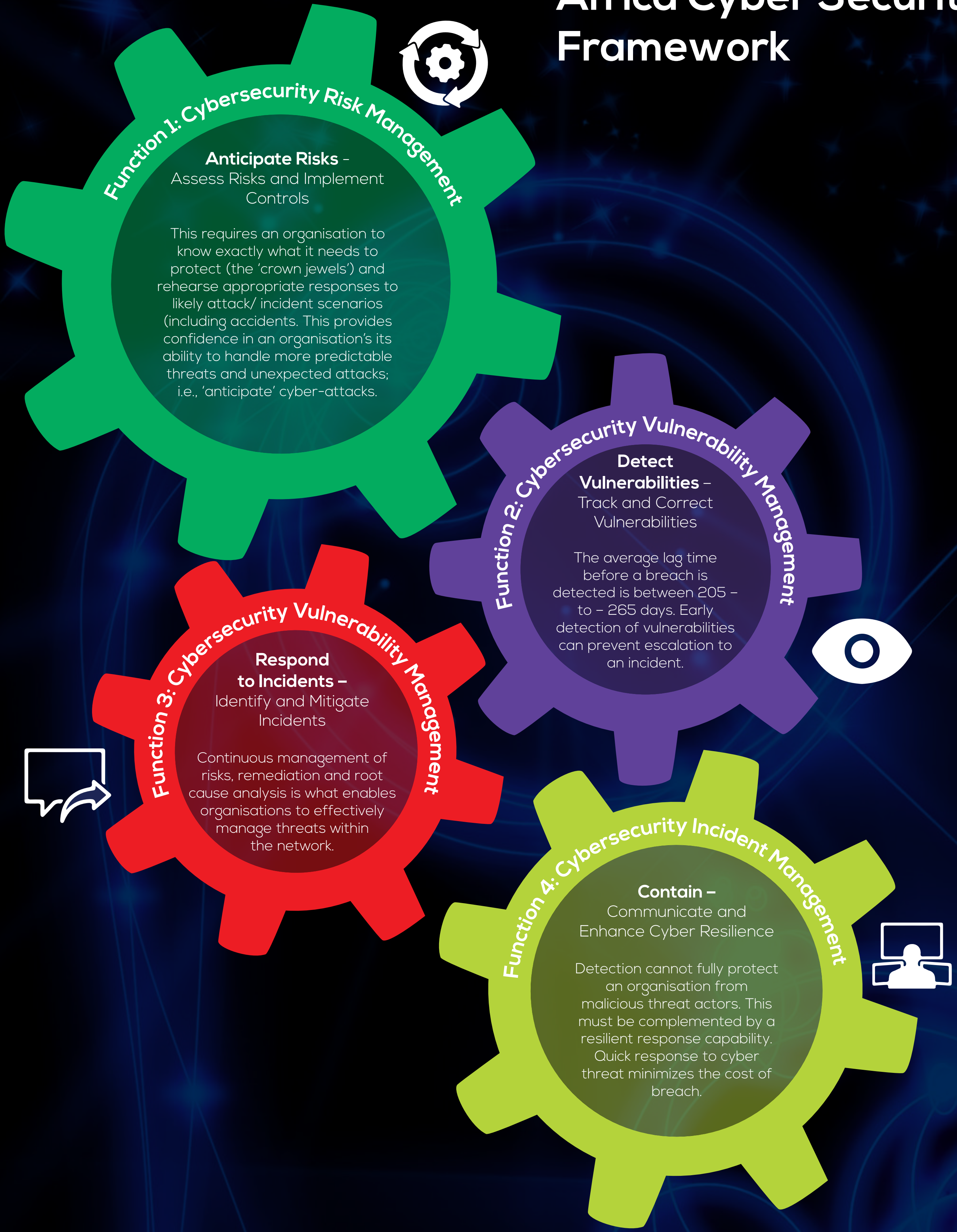
Cybercrime in the African continent particularly within the Small Medium Enterprises (SMEs) setting is a growing concern. SMEs are especially expanding the use of cloud, mobile devices, smart technologies and work force mobility techniques. This reliance has however unlocked the doors to vulnerabilities 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



Function 1: Cybersecurity Risk Management

Anticipate Risks – Assess Risks and Implement Controls

This requires an organisation to know exactly what it needs to protect (the 'crown jewels') and rehearse appropriate responses to likely attack/ incident scenarios (including accidents. This provides confidence in an organisation's its ability to handle more predictable threats and unexpected attacks; i.e., 'anticipate' cyber-attacks.

Function 2: Cybersecurity Vulnerability Management

Detect Vulnerabilities – Track and Correct Vulnerabilities

The average lag time before a breach is detected is between 205 – to – 265 days. Early detection of vulnerabilities can prevent escalation to an incident.

Function 3: Cybersecurity Vulnerability Management

Respond to Incidents – Identify and Mitigate Incidents

Continuous management of risks, remediation and root cause analysis is what enables organisations to effectively manage threats within the network.

Function 4: Cybersecurity Incident Management

Contain – Communicate and Enhance Cyber Resilience

Detection cannot fully protect an organisation from malicious threat actors. This must be complemented by a resilient response capability. Quick response to cyber threat minimizes the cost of breach.

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

Dr. Peter Tobin

Privacy and Compliance Expert

BDO IT Consulting Ltd

Mauritius

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!

Appendix

List of Remote Access Tools for Database

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

Remote Access tools for Endpoints

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

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

List of Open Source Tools

Vulnerability Scanners

1. OpenVAS

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

2. Retina CS Community

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

3. Microsoft Baseline Security Analyzer (MBSA)

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

4. Nexpose Community Edition

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

5. SecureCheq

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

6. Qualys FreeScan

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

References

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

Attacks

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

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

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

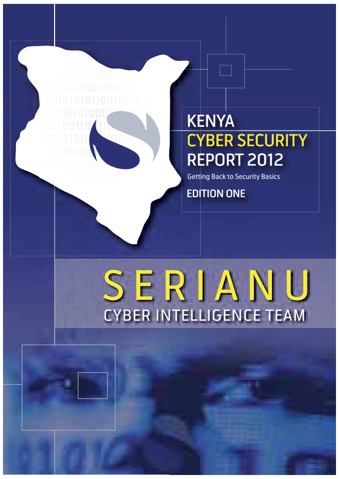
Cyber Immersion

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



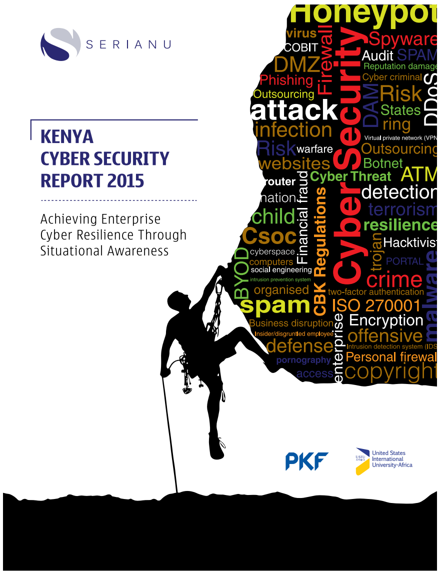
KENYA
CYBER SECURITY
REPORT 2012
Getting Back to Security Basics
EDITION ONE

SERIANU
CYBER INTELLIGENCE TEAM

KENYA
CYBER SECURITY
REPORT 2014

Rethinking Cyber Security –
"An Integrated Approach:
Processes, Intelligence and Monitoring."

Compiled and published by the Tespok iCSIRT in partnership with the Serianu Cyber Threat Intelligence Team and USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology.

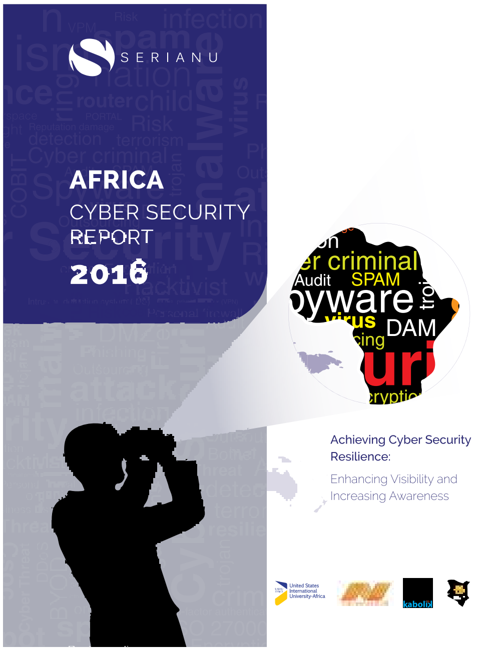


SERIANU

KENYA
CYBER SECURITY
REPORT 2015

Achieving Enterprise
Cyber Resilience Through
Situational Awareness

PKF
United States International University-Africa



SERIANU

AFRICA
CYBER SECURITY
REPORT
2016

Achieving Cyber Security Resilience:

Enhancing Visibility and Increasing Awareness

United States International University-Africa
kabolik

SERIANU

USIU AFRICA United States International University-Africa

ISACA®
Trust in, and value from, information systems

LIQUID TELECOM

SERIANU CYBER-THREAT COMMAND CENTRE SCC ANTICIPATE • DETECT • RESPOND • CONTAIN