



S E R I A N U

KENYA

CYBER SECURITY
REPORT

2016





Achieving Cyber Security Resilience:

Enhancing Visibility and Increasing Awareness

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

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



Contents

- 06 About the Report
- 07 Acknowledgement
- 08 Foreword
- 10 Executive Summary
- 13 Top 5 Priorities for 2017
- 15 Kenya Cyber Intelligence Report
- 21 2016 Kenya Cyber Security Survey
- 32 Risk Ranking by Sector
- 36 Top Cyber Security Issues in 2016
- 38 Top Trends Influencing Cybersecurity in Kenya
- 42 The Serianu Cybersecurity Framework
- 49 References

About the Report

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

Data Collection and Analysis

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

The sensors are non-intrusive network monitoring devices that perform the function of monitoring an organisation's network for malware and cyber threat activities such as brute-force attacks against the organisation's servers. In an effort to enrich the data we are collecting, we have partnered with The HoneyNet Project™ and other global cyber intelligence partners to receive regular feeds on malicious activity within the country. Through such collaborative efforts we are able to anticipate, detect and identify new and emerging threats using our intelligent analysis-engine. The analysis-engine assists in identifying new patterns and trends in cyber threat sphere that are unique to Kenya.

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

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

Acknowledgement

Authors

Serianu Ltd

Brencil Kaimba

Kevin Kimani

Martin Mwangi

Barbara Munyendo

Faith Mueni

Daniel Ndegwa

Stephen Wanjuki

Nabihah Rishad

Samuel Keige

Jeff Karanja

Hilary Soita

USIU Africa

Paula Musuva-Kigen

Secauose Onyibe

Polly Mugure

Kenneth Mbae

Newton Karumba

Andrew Ngari

Edward Owino

Others

Paladion Team

Contributors

Francis Wangusi

Director General, Communications Authority of Kenya

Paula Musuva-Kigen

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

Joseph Mathenge

CISO Airtel Africa

Rajat Mohanty

Chairman and CEO, Paladion Networks

Juliet W. Maina

Associate - Telecommunications, Media and Technology; Tripleoklaw Advocates

Brencil Kaimba

Risk & Compliance Consultant, Serianu Limited

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

Design, layout and production: Tonn Kriation

Copyright © Serianu Limited, 2016

All rights reserved

For more information contact:

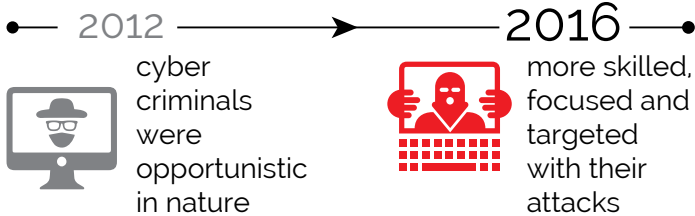
Serianu Limited, Turnkey House, 14 Chalbi Drive, Lavington

Tel: +254 20 240 9294, **Cell:** +254 702 847 570

Email: info@serianu.com | **Website:** www.serianu.com

Foreword

In 2012, we embarked on a journey to demystify the state of cyber security in Africa. **In four (4) years we have witnessed technology and cyber security landscapes change rapidly. Then, cyber criminals were opportunistic in nature but over time have become more skilled, focused and targeted with their attacks.**



The top methods used by cyber criminals in the **past 4 years** were **ransomware and database transaction manipulation**. In comparison to **2016, the top causes of compromise were malware and social engineering**.

Technology has also changed and we are seeing increased use of Optical Fiber Technology, introduction of 4G network capabilities and numerous companies are now offering Cloud computing services.

As more businesses digitize their business processes and move to the internet, their exposure to cyber-attacks also increases. This new operational environment **requires**

William Makatiani

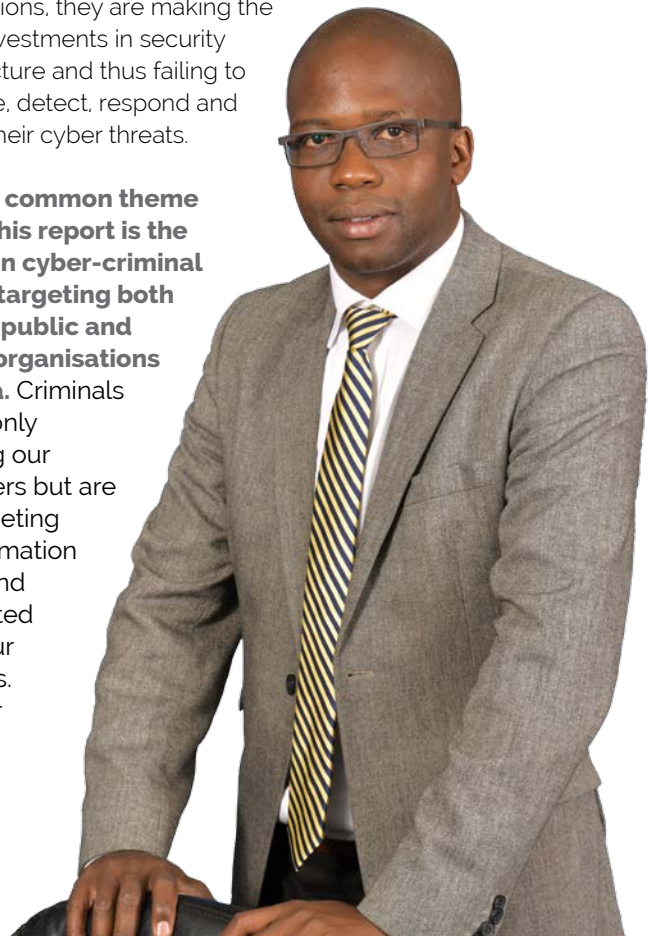
CEO, Serianu Ltd

organisations to build capabilities around anticipating, detecting, responding and containing (ADRC) cyber-attacks.

Unfortunately, most businesses in Kenya are not investing in these capabilities.

As such, a typical SME in Kenya will have at least one or two systems fully exposed on the internet. Such systems will have default passwords and unpatched software. In addition, the internal teams are unaware of these vulnerabilities. Due to the lack of visibility among Kenyan organisations, they are making the wrong investments in security infrastructure and thus failing to anticipate, detect, respond and contain their cyber threats.

The one common theme across this report is the growth in cyber-criminal activity targeting both specific public and private organisations in Kenya. Criminals are not only targeting our computers but are also targeting the information stored and transmitted within our networks. Whether



the source of an attack is an insider, a hacker or a terrorist, the consequences are often the same - loss of revenue, sensitive information, erosion of consumer and constituent confidence and interruption or denial of business operations.

One of the most critical challenges facing Kenyan organisations is the lack of awareness among technology users. Many of these users – mostly customers and employees – have little knowledge of the level of risk they are exposing themselves and their organisations to.

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

Serianu estimates the cost of cybercrime in Kenya to be USD 175 million in 2016, an increase from the USD 150 million reported in 2015.



Perhaps what was more alarming from our analysis was the disparity between the cost of cybercrime and budget allocation to technology products.

While there are high levels of investments in technology and automated processes in government services and the private sector, the study found that there was no matching investment in cyber threat prevention tools. 96% of the organisations surveyed spend less than USD 5,000 annually or none at all on cyber security related products. Consequently, majority of these organisations lack clear visibility on the cyber security issues they need to watch out for.

96% of organisations spent less than **\$5,000** annually or none at all on cyber security related products



It is however notable that challenges faced by Kenyan and indeed African organisations in general are unique with budgetary constraints being a top challenge. With the inadequate budget for ICT, it's become expensive for small and medium sized companies to adopt complex cyber security frameworks. Therefore, in order to assist SMEs especially to identify and prioritize specific risks and steps that can be taken to address these risks in a cost effective manner, we developed the Serianu Cyber Security Framework. We have shared this simplified cyber security framework to this effect.

We are very excited about this year's report and we hope it will provide you with new insights on the ever-changing cyber security landscape.

Executive Summary






In recent years, the technology landscape in Kenya has seen tremendous growth. From strategic options to creation of new opportunities for innovation in products and services, technology is now incorporated in many if not all aspects of business. Mobile and Internet usage has also seen a continued increase especially within the local SMEs. However, as more

businesses digitize their business processes and move to the internet, the potential attack vectors for these organisations expand.

The Kenya Cyber security report is part of the Africa cyber security report 2016. In this report we sought to understand the current top threats, risks and levels of awareness in Kenya.

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.

Breakdown of key statistics for In-Scope countries:

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

*Certified Professionals is limited to the following certifications: CISA, CISM, GIAC, SANS, CISSP, CEH, ISO 27001 and PCI DSS QA

*Economic and internet usage data extracted from respective country Internet regulator reports and World Bank site.

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



Highlights of the Report

- ◆ **The estimated cost of cyber-crime in Kenya has soared to \$175 million.** This cost continues to grow as many organisations automate their processes. This is particularly so for banking and other financial services sectors where the introduction of mobile and e-services has introduced new weaknesses that have allowed loss of money through these channels.
- ◆ **Mobile money in Kenya has experienced numerous attacks through social engineering, use of malware and account personifications.** As one of the alternative channels for most banks, hackers are now exploiting the weak security controls around the mobile money platform to steal millions.
- ◆ **Malware targeting critical mobile and internet banking infrastructure are on the rise.** The results of our internal traffic analysis revealed that there are numerous forms of malware on internal systems which include: trojans such as Dridex and Zeus malware. Attackers are using these malware to compromise and access sensitive information on the network. Unfortunately, statistics still remain vague as organisations are reluctant to reveal the extent to which they have been targeted by attackers.
- ◆ **Insider threat is still the largest contributor of direct losses in cybercrime in Kenya.** Insider threats refer to fraud involving information or employee abuse of IT systems and information.
- ◆ **E-commerce platforms hit with more online scams, ATM card skimming and Identity Theft** as integrations with Electronic Payments and financial institutions increase. At the same time, electronic banking and cashless initiatives have been introduced into the country. This has resulted in unintended consequences ranging from online scams, ATM card skimming and identity theft.
- ◆ **Increase in IoT threats** - due to their insecure implementation and configuration, these Internet-connected embedded devices, including CCTVs and nanny cams, Smart TVs, DVRs, Smart routers and printers, are routinely hacked and used as weapons in cyber-attacks.
- ◆ **Technical training of employees is insufficient. The increase in the number of home grown cyber criminals in Kenya** is not because attackers are more talented, it's because they are more creative, patient, single minded and they explore limitless pathways. Kenyan organisations are not leveraging their own creative, curious analysts. Out technical teams are not empowered with tools

...at a glance



- ◆ Numerous attacks on mobile money through social engineering, use of malware and account personifications.
- ◆ The largest contributor of direct losses in cybercrime in Kenya is insider threat.
- ◆ E-Commerce Platforms hit with more Online Scams, ATM Card Skimming and Identity Theft.
- ◆ Low levels of security awareness.
- ◆ Malware targeting critical mobile and internet banking infrastructure are on the rise.
- ◆ Insider threat is still the largest contributor of direct losses in cybercrime.
- ◆ Technical training of employees is insufficient.
- ◆ Lack of practical regulatory guidance from industry regulators and government.
- ◆ Only 3% of reported cyber-crimes are successfully prosecuted.

and education to enable them explore the why?

◆ **Low levels of security awareness.**

Most organisations don't budget for awareness and training programs for their staff. This has been proven by the numerous breaches we have seen in the period under review alone attributed to compromised employees. Most trainings are conducted after a security incident has occurred.

◆ **Security professionals are struggling to demonstrate business value to senior management** because they are providing very technical operational metrics whereas business managers are looking for more business-oriented metrics.

◆ **Lack of practical regulatory guidance from industry regulators and government**

leads to poorly implemented and unenforceable security controls since they are not local focused and instead are copied and pasted regulations.

◆ **Only 3% of reported cyber-crimes are successfully prosecuted.** Inadequate training and awareness amongst the law enforcement and judiciary fraternity make prosecution of these cases impossible.

Way forward

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



Top 5 priorities for 2017



The challenges faced by Kenya and in essence African countries present great business opportunities for entrepreneurs, researchers and vendors. In order for us to stay ahead of the threat curve, we need to continually invest in research, build local cyber threat management infrastructure and enhance our ability to anticipate, detect, respond and contain information security threats. In our current state, we are unable to build these capabilities. Kenyan entrepreneurs need to step up, work together to build and provide information security services that address these challenges. Kenyan entrepreneurs and researchers should leverage their local presence and understanding of the environment to provide a clear indication of the security problems on the ground. This local presence combined with partnerships with global players will provide globally tested solutions and approaches to address identified security problems.

Awareness and Training

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

Continuous Monitoring and Log Analysis

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



Vulnerability and Patch Management

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

Continuous Risk Assessment and Treatment

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

Managed Services and Independent Reviews

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

Kenya Cyber Intelligence Report

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



For the purposes of this report, we inspected network traffic inside a representative of Kenyan Organisations, reviewed contents of online network monitoring sites such as Project honeypot 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 country.

External Cyber Threat Landscape.

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



Project HoneyPot Intelligence Analysis

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

IP Statistics

Most Malicious Local IPs

The IP Address

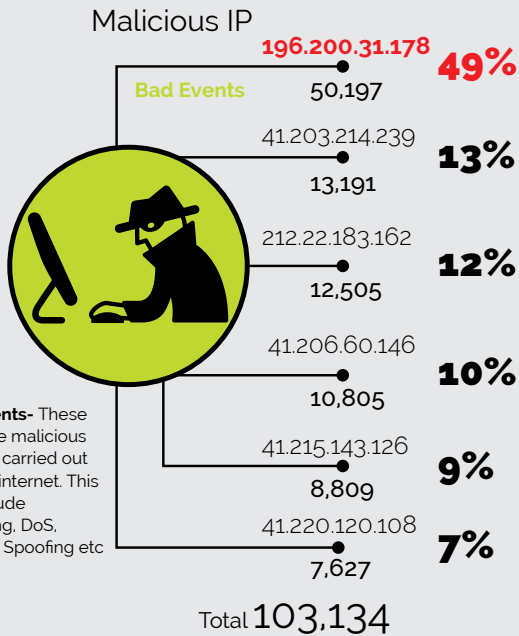
a. 196.200.31.178

was found to be the

top IP address with
the highest number of bad events

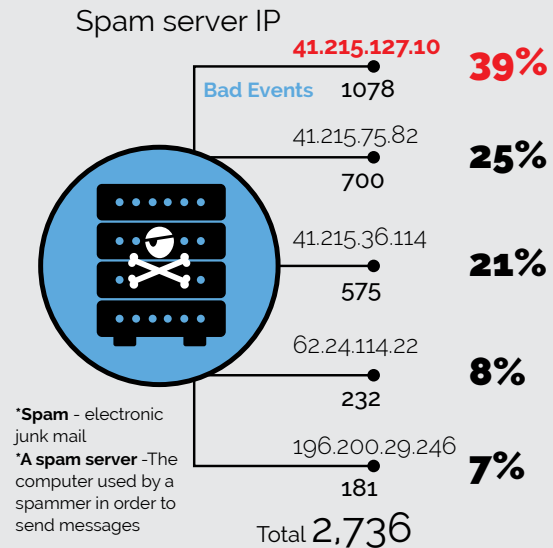


Most Malicious Local IPs



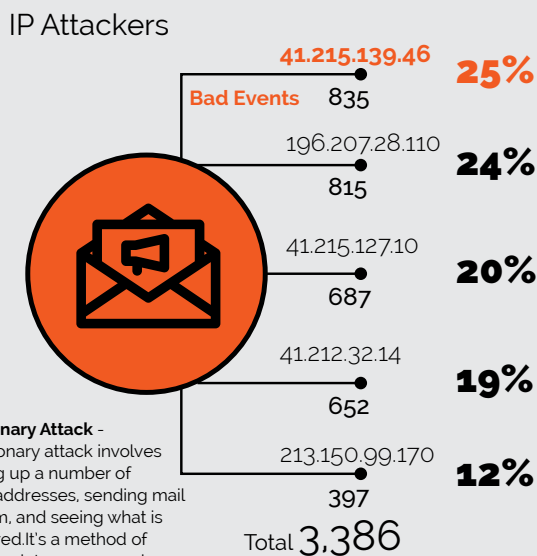
*Bad Events- These are all the malicious activities carried out over the internet. This may include spamming, DoS, Phishing, Spoofing etc

Top Spam Servers-Email



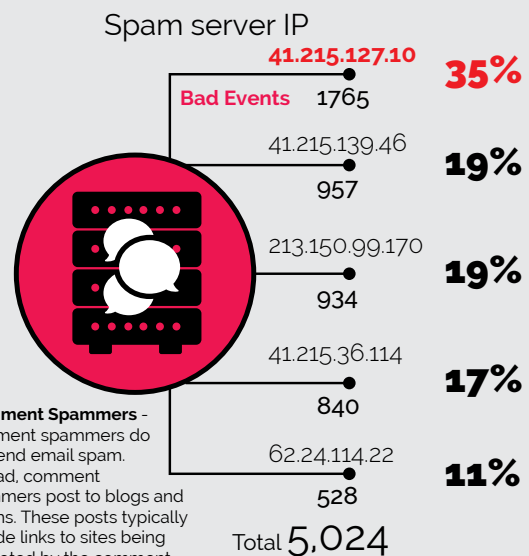
*Spam - electronic junk mail
*A spam server -The computer used by a spammer in order to send messages

Dictionary Attackers



*Dictionary Attack - A dictionary attack involves making up a number of email addresses, sending mail to them, and seeing what is delivered. It's a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A **dictionary attack** can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

Top Comment Spammers



*Comment Spammers - Comment spammers do not send email spam. Instead, comment spammers post to blogs and forums. These posts typically include links to sites being promoted by the comment spammer. The purpose of these links is both to drive traffic from humans clicking on the links, as well as to increase search engine rankings which are sometimes based on the number of links to a page.

Port Scan Analysis

a.) Top Vulnerable Ports

Port 80 had the highest percentage of online services hosted on it at 23%. Running applications on this port comprises of routers, web servers, applications and web portal management systems which make them vulnerable to attack.

b.) Most vulnerable Routers

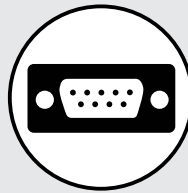
MikroTik and Cisco routers are the most vulnerable enterprise routers at 66% and 16% respectively.

c.) Top Vulnerable Web Servers

Apache HTTPD was the most vulnerable web server at 12% followed by IIS Server at 6%.

d.) Most Vulnerable Applications

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



Port 80

23%

Ports 443, 8080,
3306, 3389, 22, 23
21, 445, 139

9%

**Most
Vulnerable
Port**



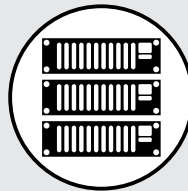
MikroTik

66%

Microsoft IIS

16%

**Most
Vulnerable
Enterprise
Routers**



Apache HTTPD

12%

Mic IIS Server

6%

**Most
Vulnerable
Web
Server**



Microsoft Outlook
Web App

**Most
Vulnerable
Application**

Internal Cyber Threat Landscape

This section summarizes local intelligence obtained on the following areas: **Top device vulnerability categories, Top malicious signatures and Top local attackers.**

Top Vulnerability Listings

- 1. Use of obsolete systems and applications** – Obsolete operating systems and applications are those that are no longer supported by the vendor and thus no security patches are released for such. We observed that majority of organisations still run on such legacy systems among them windows XP and windows server 2003.
- 2. Use of clear text and insecure protocols** e.g. SNMP V1/V2, FTP, Telnet – These are communication standards that do not encrypt data in transit. If exploited, such protocols could compromise the confidentiality of the data in transit.
- 3. Web server misconfiguration** – Majority of the deployed web servers are running on default configurations while others leak web server information through their error handling mechanisms.
- 4. Use of default credentials** – Default credentials and configurations still remain one of the highest risks in organisations due to the lack of secure device configuration procedures during the on-boarding of such devices.

Vulnerability Categories


This section summarizes the top vulnerability categories identified: missing patches, clear text protocols, obsolete systems, system misconfiguration and weak password.

Missing patches remain as the highest category at **94%** for **critical and severe risk ratings** followed by insecure protocols at 81%.

	Clear text/ insecure protocol	Missing Patches	System Miscon- figuration	Weak password / insecure access
Critical	14%	27%	3%	25%
Severe	67%	67%	44%	27%
Moderate	19%	6%	53%	48%

System Misconfiguration

This is a representation of top commonly identified system misconfiguration.




Vulnerability

- IP Source Routing Enabled **36%**
- Invalid CIFS Logins Permitted **29%**
- SSH server supports SSH protocol v1 clients **23%**
- SMTP unauthenticated 3rd-party mail relay **8%**
- IPMI 2.0 Cipher Type Zero Authentication Bypass Vulnerability **4%**

Weak/Poor Authentication Protocols


Majority of devices have the 'public' and 'private' SNMP community strings configured allowing attackers to perform reconnaissance activity against such devices and also update existing device configurations.



- SNMP **60%**
- FTP **35%**
- Cisco IOS **5%**


Clear Text and Insecure Protocols

These are communication standards that do not encrypt data in transit or can be easily exploited by attackers.



- SNMP credentials transmitted in clear text **73%**
- Anonymous FTP Writeable Directories **7%**
- VNC remote control service installed **11%**
- 'rsh' Remote Shell Service Enabled **9%**

Top Malicious Signatures



- ET MALWARE Double User-Agent (User-Agent User-Agent) **49%**
- ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03 **22%**
- ET DOS MC-SQLR Response Inbound Possible DDoS Target **5%**
- ET TROJAN DNS Reply Sinkhole - Anubis - 195.22.26.192/26 **19%**
- ET TROJAN DNS Reply for unallocated address space - Potentially Malicious 1.1.1.0/24 **13%**
- ET MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake **2%**
- ET MALWARE User-Agent (Internet Explorer) **5%**
- ET DOS DNS Amplification Attack Inbound **5%**



Francis Wangusi

Director General, Communications Authority of Kenya

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

Yes

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

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

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

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

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

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

In your opinion, what drives criminals to commit cybercrime?

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

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

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

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

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

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

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

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

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

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

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

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

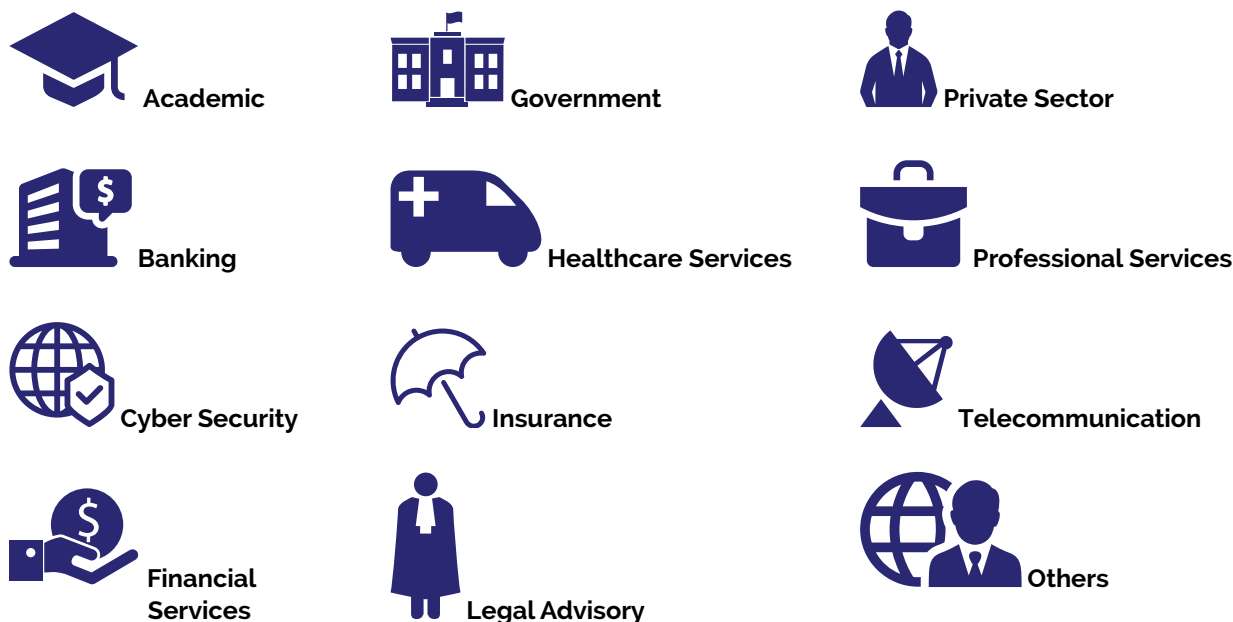
2016 Kenya Cyber Security Survey

The goal of the Kenya 2016 report is 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 local organisations and the most prominent threats that they face.



About the Survey

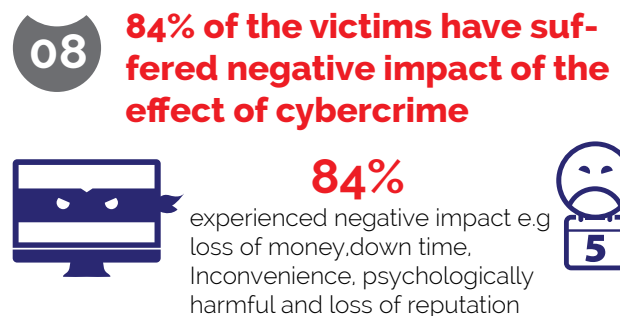
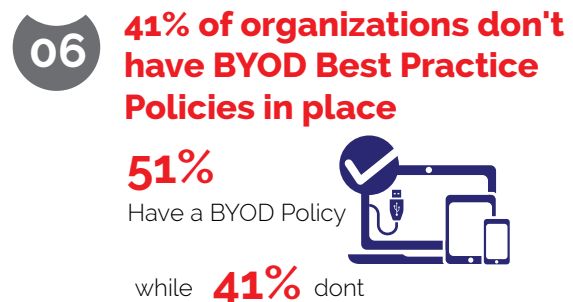
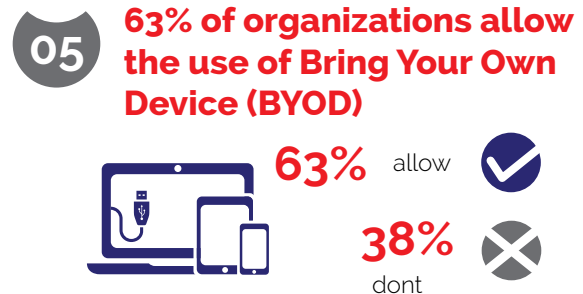
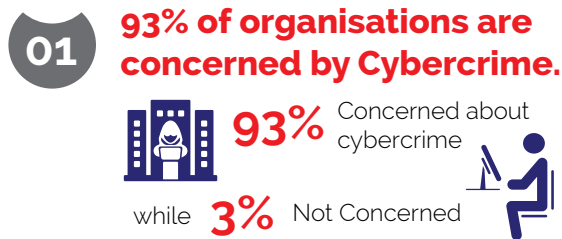
This report was prepared based on data collected from a survey of over 150 respondents across organisations in Kenya and they included companies from the following sectors:



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



Summary of findings

According to the survey findings, **98.8% of respondents have a general understanding of what cybercrime is.** With the many advances in information technology and the transition of social and economic interactions from the physical world to cyberspace, it's expected that majority of individuals have a general idea of what cybercrime is.



09 **88% of Cybercrime cases go unreported to the police.**

88% did not report cases of cybercrime to the police

13 **95% of organisations apply system testing techniques?**

95% apply system testing techniques like penetration testing, vulnerability testing and audits.



10 **96% of organizations spend less than \$5,000 annually on Cyber security products.**



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



14 **Majority of organisations have sensitive data in their Databases.**

38% Databases contain the most critical information

followed by Emails at **20%**

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


9% outsourced to either an ISP or Managed Services providers while

83% manage cyber security internally or don't have any management system in place.



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

- 21%** Better education of users of the Internet
- 20%** Better encryption & improved privacy
- 18%** Improve our understanding of society and the cyber community
- 16%** Improved technology for our networks and operating systems
- 14%** Better laws and regulations



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

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

38% have defined security frameworks based on these standards.





Analysis

According to the survey findings, majority of respondents have a general understanding of what cybercrime is. With the many advances in information technology and the transition of social and economic interactions from the physical world to cyberspace, it's expected that majority of individuals have a general idea of what cybercrime is. Concerns around cybercrime are also very high.

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

With the increase in use of BYOD and businesses looking to save money by not having to equip and maintain an increasingly mobile

workforce with the expensive devices they need to do their jobs, it was found that more than half of the organisations represented in the survey have adopted BYOD. However, even with these developments, more than 41% did not have any internal device usage policy or BYOD policy to govern the usage of these BYODs.

When it comes to managing cyber security, the largest percentage of the respondents (67.1%) manage their security In-house, 9.8% have an in-house CERT, 6.3% have outsourced to an independent specialist or organisation while 8.4% don't know how their cyber security is managed. Even with these, it should be noted that, even though majority of the companies are managing their cyber security in-house, more often than not these individuals are overloaded with other tasks within the organisation and/or lack the necessary skill set to handle cyber incidents. This was highlighted by the survey results whereby only 37.8% of the respondents had Information Security Management certifications while 44.8% of the respondents did not have any information security management certifications. 16.8% did not even know if anyone in their organisation had such certifications.

Also critical was the security testing within organisations,

Highlights of Kenyan

Organisations:

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

Majority of the organisations spend

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

More than half of the organisations have allowed

! BYOD but **41%** don't have any BYOD policy

67% manage their security In-house, **10%** have an in-house CERT,

! **6%** have independent specialists while **8%** have no knowledge on how their cyber security is managed

...cont

38% had Information Security Management Certifications,

45% don't have

while **17%** had no knowledge of the existence of such certifications within their organisation.

55% carried out penetration and vulnerability testing,

40% carry out audits

while **4.6%** have no knowledge of any testing techniques

71% have been affected by cybercrime in one way or another

91% cyber security incidences go unreported or unsolved

55.2% of the respondents carry out system testing in terms penetration testing and vulnerability testing, 40.2% carry out audits while 4.6% do not know what security testing techniques have been implemented in their organisations. All these testing techniques are not independent and in fact work best when they are applied concurrently.

With the increased rate of Cybercrime in Kenya, most of the respondents (70.6%) have experienced cybercrime in one way or another. Out of these, 34% was through work while 66% at personal capacity. This highlights the importance of incorporating cyber security awareness and vigilance in the work areas as it's the most targeted environment.

There are low levels of awareness within the country hence it is no surprise that when it comes to reporting of cybercrime to the police, 97.1% of the cyber security incidents either go unreported or unsolved. Only 2.9% of the reported cases were followed through to a successful prosecution.

External Infrastructure Vulnerabilities identified during the survey include unnecessary services enabled; including content management and remote administration, misconfigured SSL certificates and encryption settings. With these vulnerabilities an unauthorized user or attacker can gain access to business critical systems.

The results of our internal traffic analysis revealed that there are numerous forms of malware on systems and these include; trojans such as Dridex and Zeus malware.



Rajat Mohanty

Chairman and CEO, Paladion Networks



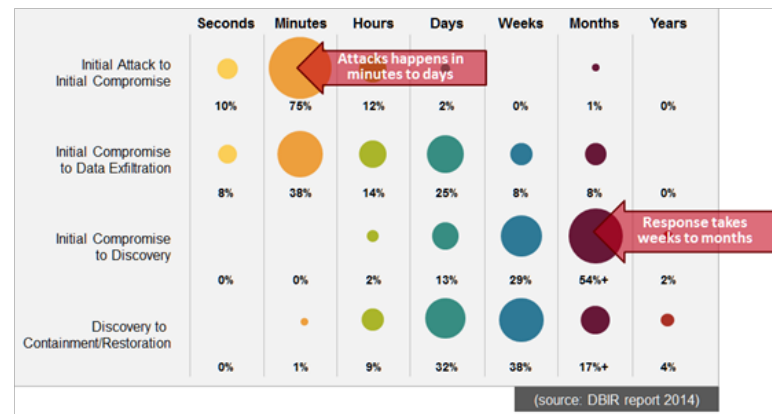
Cybersecurity Needs a New Paradigm - Speed!

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

these breaches are not detected till around 200 days by the organisations. As per Data Breach Investigation Report 2015, over 60% of the times such breaches are actually reported by external entities and not detected by organisations themselves.

Asymmetry in Cyber Security

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



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

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

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

State of Detection and Response

Modern attacks are sophisticated and long drawn. Advanced attackers enter into a network with initial attack and then navigate through the network over months to carry out their objective. The industry average shows that

Speed as the new Determinant of Success

Given that breaches are inevitable and organisations will have security incidents despite best effort, the focus should shift to how soon the breaches can be detected and how fast they can be responded. No organisations get impacted because they get breached, they get affected

and become news items only due to the long period of time that elapses from an attacker's first entry to the final detection and response. What security needs as a new paradigm is speed of operations: increasing the speed in discovery and response. With enough speed, every breach will be insignificant. As part of this paradigm, the questions that management should ask are- How fast can we detect attacks- Is it as fast as the attacks themselves? And how fast can we investigate, contain and eradicate attacks- Is it as fast as the attacker's movement within the network?

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

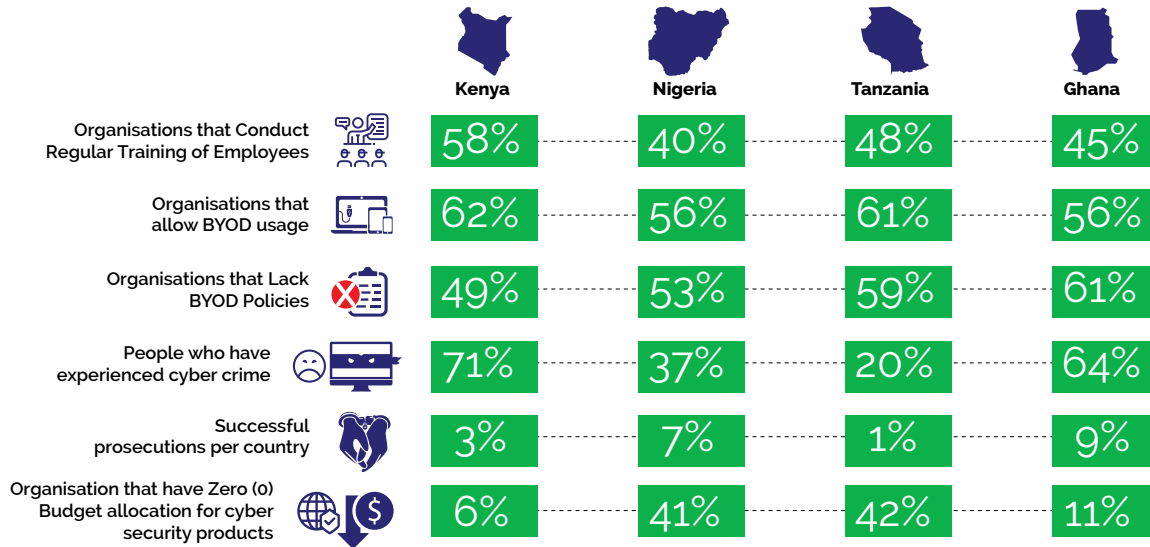
- 1. 360° Situational Awareness:** For fast discovery of attacks, the security operations should have full visibility into every asset, user activity, network traffic, system vulnerabilities and network topography at all times. Today, such visibility is limited to critical assets and users, which severely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

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

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

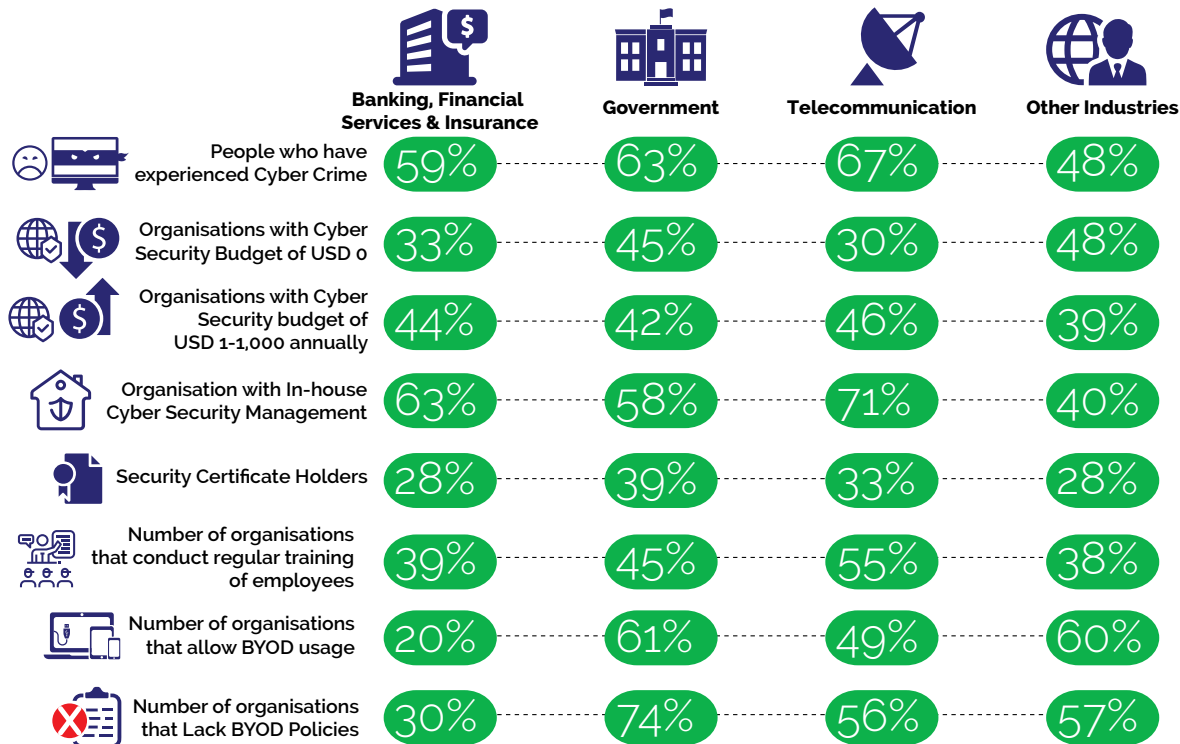
Inter Country Analysis

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



Industry Analysis







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






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

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

Achieving Cyber Security Resilience

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



Paula Musuva-Kigen

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



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

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

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

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

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

- (i) perceive what the key cyber security events are
- (ii) comprehend what these events are indicative of
- (ii) projecting into the future the impact of these events and their implications to our current organisational setting.

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

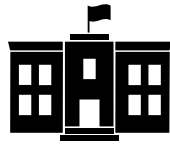


Risk Ranking by Sector



1. Banking

The motives for data breaches are increasingly financial. This obviously makes banks more of a target than ever. 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 are often the same. It is paramount that local banks invest in mechanisms to Anticipate, Detect, Recover and Contain cybercrime.



2. Government

The government has been a prime target for cyber-attacks. This is attributed mainly to the huge volumes of critical confidential social and economic information. In the month of April, the Ministry of Foreign Affairs suffered a cyberattack in which a trove of data amounting to 1 Terabyte was stolen and leaked to the dark web, which included confidential and non-confidential email conversations, security related information, trade agreements and letters on the Sudan's security situation in the form of PDF or Docs. We have also witnessed various web defacement for different government officials. The Immigration and Registration of persons, the National Environment Trust Fund and the Integrated Financial Management Information System (IFMIS) were reported to be compromised.

There is need for the government to formulate policies and laws around cybercrime and also increase collaboration with the private sector in fighting this vice.



3. Financial Services

Sacco's, cooperatives and microfinance institutions are rapidly growing in Kenya. However, these organisations are so focused on customer satisfaction and reducing costs that they tend to neglect investment in cybercrime prevention. This has made them a popular target for cybercriminals.



Mobile Money

Kenya continues to lead in mobile money usage across Africa and in many parts of the world, 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, risky consumer behavior. Whether or not an institution uses proprietary or third party mobile applications, the risks posed by these systems are still inherent.



4. Betting Sites

The betting and gambling sites in Kenya increased rampantly from the year 2013 when the first online sports betting company was registered. As of today, there are myriads of online casinos, poker sites, sports betting sites, lotto and bingo sites registered in the country by the Betting Control and Licensing Board (BCLB). In addition, there are 10 operators that run sports betting using mobile operators, integrating with SMS and other services on mobile platforms.

The approximated revenue for the leading betting site in Kenya is approximately 4.2 Billion per annum, which is predicted to increase to 5.1 billion in the next three years. As this craze engulfs fans and gamblers, it opens new attack channels for hackers who are obviously motivated by the economic returns.

Our research showed that most of these sites lack proper cybersecurity controls in their infrastructure, with most of them using unencrypted HTTP to capture user credentials and information during registration and for transactions.



5. E-commerce

Penetration of e-retailers including online shopping malls such as Jumia and E-Bay, OLX, Rupu, Kili mall, Real estate market places; buyrentkenya.com among others has increased significantly. More companies in the different sectors of their economy are taking their marketing and distribution of goods to online sites as well. This growth, paired with the services of 24/7 delivery companies like G4S, DHL and Postal Corporation of Kenya's EMS has increased confidence in online shopping. Due to this change, an increase in the number of online scams, fraudulent transactions and breach of customers' personal information have been noted. Merchants need to be aware of the risks electronic transactions carry, and work towards securing the systems to the highest standards.



6. Hospitality & Retail

The hospitality industry is primarily client facing and as such deals with a great deal of sensitive customer information. Processes ranging from reservation details, payment, travel, personal information are now automated and we are seeing introduction of services such as digital conference facilities, smart room keys and mobile applications which enable the client to perform a wide range of otherwise manual processes. However, information security aspects tend 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.



Joseph Mathenge

CISO Airtel Africa



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

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

While the private sector appears to lead in the charge of addressing cyber security threats, not nearly enough is being done. Not unlike global trends, private sector in Africa in most instances invest in security controls after falling victim to cyber-crimes. Taking the example of Heartland Payment systems that were victims of a credit data loss back in mid-2000, the company's CEO reported in quadrupling their spending in system security controls solutions. The major force driving the growth of the African market is expected to be the increasing focus on government regulations and compliance requirements. Regions that will probably lead in this (South Africa, Nigeria and Kenya) have had several laws enacted in the recent past requiring private sectors to do more in protecting the data they collect, process and store. Again there are simply not enough laws, regulations and stiff consequences put in place to improve cyber security. While the Telecommunications industry in Africa doesn't necessarily have laws or frameworks written for them, they are a big target for cyber-attacks because they communicate and store large amounts of

sensitive data. This very nature makes them subject to a wide range of the clauses included in many of laws by the nature of their industry. According to findings from The Global State of Information Security Survey 2015, many telecommunications companies are not doing enough to address cyber threats. The survey lists statistics showing that the number of security incidents detected by telecommunications companies dropped by almost 20% in 2014, however this drop doesn't indicate a reduction in intrusion but rather an increase in sophistication of attack vectors that make detection very difficult.

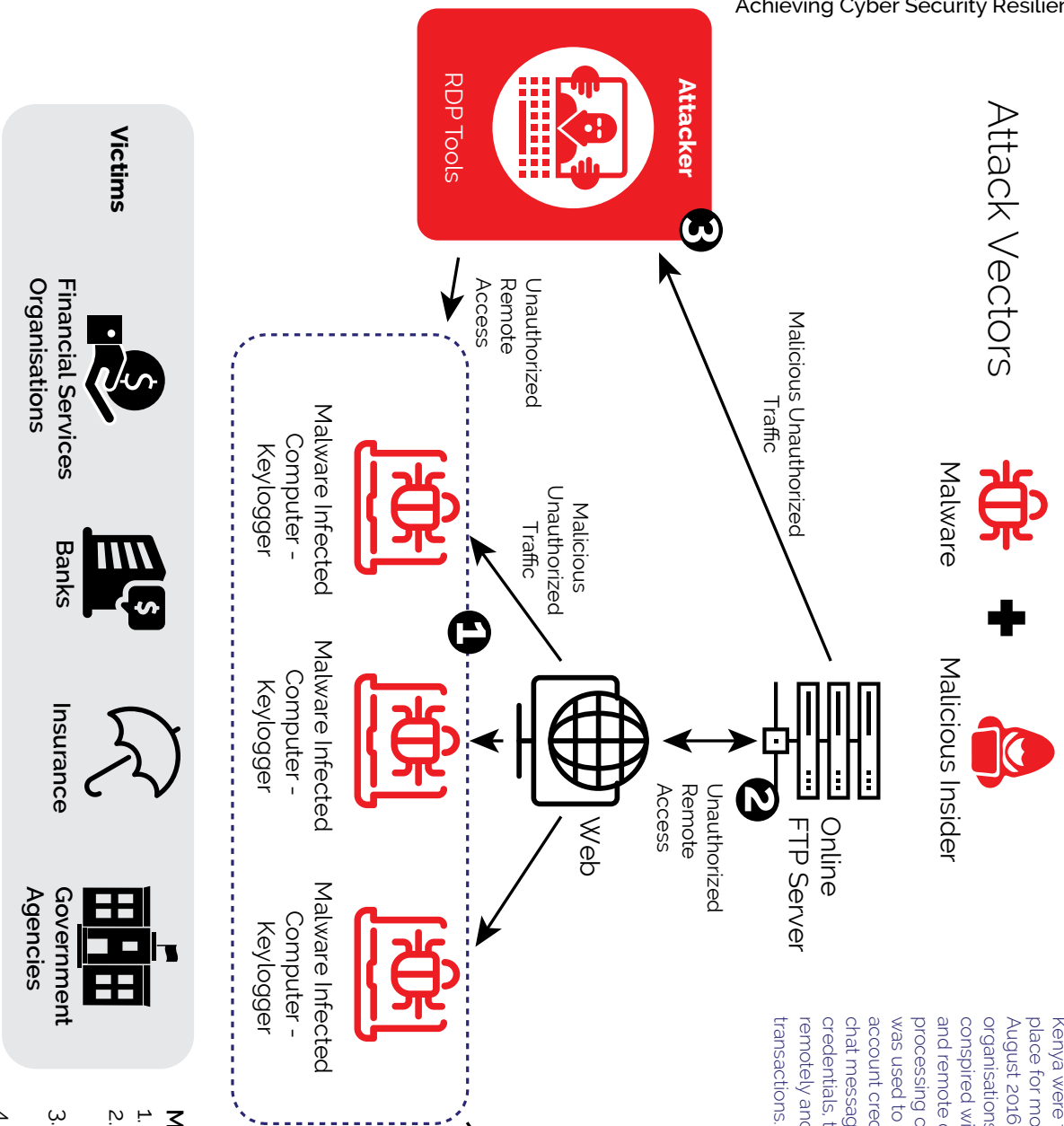
Addressing cyber security in Africa particularly in the Telco sectors would entail a replay of number of fundamentals successfully carried out in other fields globally.

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

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

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

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



Anatomy of a Cyber Heist

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

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



Top Cyber Security Issues in 2016



5

Identity Theft

Identity theft involves the offender getting hold of the victim's personal information and using it to their advantage. The motive behind this is usually for financial gain. There is a lot of personal information that is held online and in the event a cybercriminal is able to access this information they can use it to commit fraud. Cases of attackers using victims' personal information to set up new accounts have been noted. An increase in account take overs where the victims' accounts are compromised and are used for unauthorized transactions have also been noted in the year 2016.



1

Insider Threat

The enemy within is still alive and kicking. Our research indicates that over 80% of system related fraud and theft in 2016 was perpetrated by employees and other insiders. We are coming across numerous cases of privileged access and attacking systems for a variety of reasons including disgruntlement, revenge and financial gain. This year alone, 50% of the direct costs of cybercrime is attributed to insider threats. Organisations cutting across both the government and private sector have lost billions of shillings due to fraudulent activities orchestrated by its employees



2

Attacks on Computer Systems –Trojans and Malware

The various endpoints on a network such as mobile devices, laptops, desktop PCs and servers are often a target for most attackers. The results of our internal traffic analysis revealed that there are numerous forms of malware on systems, these include; trojans such as Dridex and Zeus malware. Most of these go undetected on these systems. From our analysis of the cost of cybercrime, attacks on computer systems contributed 22% of all direct costs and 29% of indirect costs of cybercrime.

Mobile Banking

Individuals who have subscribed to mobile banking services risk exposure to cyber related criminal activities. Currently, there is a gap in security controls put in place for mobile money services. The number of institutions using mobile money and have adequately implemented security controls are minimal within the country. The major issues we found were unauthorised third parties gaining access to online bank accounts, login details 'sniffed' (stolen) over insecure WiFi networks and rogue hotspots, unencrypted traffic and reverse engineering. Malware infected phones are also one of the reasons that has led to compromise in mobile banking platforms.



4



3

E-payments and e-commerce fraud

In recent years, we have seen an influx of new ways for consumers and businesses to pay for expenses. As electronic payment trends continue to gain traction, one of the old payment staples – the paper check – is quickly diminishing. However, as businesses move to electronic payment processes, security concerns surrounding these systems are not always addressed. Hacking, Viruses, Identity theft and Password compromise as just a few of the ways attackers are now using to compromise these payment channels. There has been a notable increase in the use of stolen debit or credit cards. Exposing credit card details is enough to facilitate fraudsters to make online purchases using stolen information.



Poor Identity and Access management

Uncontrolled identities and access controls are exposing organisations. Identity and access management processes and technologies are not well adopted in most local organisations. These lead to unauthorised and inappropriate access to highly sensitive information.



6

Cyberstalking / Social media abuse / Web defacement

Cyberstalking involves using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person. Social media abuse in Kenya includes instances where social media has been used to say or spread hate speech. This year, the official twitter account of KDF Spokesman Major Emmanuel Chirchir was hacked and used to send abusive information. Because of the low awareness levels in Kenya, most individuals don't recognise this vice or what to do when attacked in this way and end up suffering in silence.



7

Security Awareness Training - Ignorance is not bliss

People, process and technology. The people aspect (company's staff) is the weakest link when it comes to IT security. Despite the heavy investment your business may have made into IT security technology, none of these systems are completely full-proof. Criminals and scammers are placing more focus on the elements of your business that you have less direct control over—your employees. Without training, most users in Kenya don't have the skills and knowledge they need to adequately protect the organisation's infrastructure and information from cyber-attacks.



8

Continuous Monitoring and Response

Almost all organisations are not prepared for cyber threats. In our survey, we noted that majority of the organisations are ill prepared to monitor and respond to cyber-attacks. 90% of Kenyan organisations have no real-time insight on cyber risks, lacking the agility, budget and skills to combat rising cybercrime. Majority of these organisations are unable to detect cyber-attacks using existing systems and processes.



10

Data Exfiltration

Many organisation have moved to electronic data storage in order to improve efficiency and service delivery. However, these organisations have failed to implement proper security controls and technology in order to safeguard confidential information. This has led to large amounts of organisation data being stolen by both employees and external attackers.



9



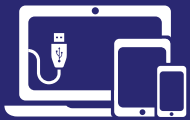


Top Trends Influencing Cybersecurity in Kenya



Mobile and Internet Usage and Costs

The number of mobile and internet users has rapidly increased this year. This is mostly due to the reduction in cost of these services making it affordable to more. Internet Service Providers (ISPs) are continuously expanding their network coverage areas and constantly keeping competitive prices making internet access cheaper across the continent hence enabling more people to obtain the service. Having an increased number of Internet users means that we now have more people exposed to cyber-attacks.



BYOD

BYOD acceptance in Kenyan organisations has risen substantially. This is reflected by the 62.2% of respondents of the Kenya Cyber Security Report Survey 2016 who were allowed BYOD within their organisations. Despite the obvious cost benefits that this adoption presents, we have witnessed the number of incidents involving mobile devices grow. As such, ensuring the centralized management of these devices and keeping them secure needs to become an important need for businesses.



Cloud – Based Solutions

Companies are handing over part or the whole of their ICT function resulting in major cost saving and also allows businesses to focus on their core activities. Majority of Kenyan organisations have adopted cloud services such as Google apps, Microsoft office 365 Microsoft Azure, Amazon and Oracle cloud. This trend has given rise to two security issues; traditional security controls won't help protect business critical systems and companies are losing visibility of their security posture.



Outsourcing - Vendor Risk

There is a growing dependence on third parties by organisations in Kenya which has resulted in introduction of new attack vectors. Organisations are handing over a lot of the typical controls that you would expect to see internally to these third parties. And while the term "third-party" is often used in reference to big jobs - such as outsourced labor, data processing, or manufacturing - the associated risks can apply to every contractual relationship, no matter how small. Kenyan organisations are not adequately performing risk assessment on their service providers before or during their engagements. As a result, many breaches that occurred in the recent past involved a third party in one way or another. There has to be a robust and continuous review and evaluation process for these vendors. Organisations also need to establish comprehensive contract agreements and third-party risk management programs that include provisions for monitoring compliance and enforcing those contracts.



Industry Regulation

Several regulatory bodies within different industries have formulated rules and guidelines that seek to enhance confidentiality, integrity and availability of critical information. The Central Bank has prudential guidelines that include requirement to conduct regular risk assessment on critical information systems. As a country, we are also in the process of reviewing the proposed cyber bill before passing it to law. Even with these guides, most Kenyan companies still lack effective implementation mechanisms in place therefore they do not completely adhere to these set standards.



IoT

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



Cyber Insurance

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



Automation and Technology Adoption Rates

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



Terrorism & Radicalization, Cyber-activism

There is an increase in the number of terrorists and activists using the internet to spread their agenda, recruit new members and attack their targets. We have seen Al Shabaab and other terrorist organisations move to the internet. Extremist individual groups make use of cyber space to threaten citizens and groups across Kenya. Based on our research, we have noticed that most of these attackers design their attack to cause physical violence or extreme financial harm. We have seen that these attacks are mostly aimed at government and business related websites. Cyber terrorism is becoming both an internal and external security threat. It is therefore critical to have cyber security awareness training as there is an increase in the number of internet users.



Poverty rates- Unemployment rates

The high rate of unemployment in Kenyan countries has contributed greatly to the cybercrimes witnessed in 2016 within the region. The rate of poverty in the region has encouraged cases of rogue employees within organisations to find means to generate extra income, hence insider attacks. Unlike regions with low unemployment rates where sabotage and espionage are the main concern, Kenyan organisations are operating in environments with very high unemployment rates.



Juliet Maina

Associate - Tripleoklaw Advocates



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

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

Yes indeed cybersecurity is a major problem in Kenya. However, the greatest concern is the low levels of awareness. Given the levels of penetration in the country, and the robustness of the ICT industry, everyone is now easily at risk.

The problem of cybersecurity in Kenya is exacerbated by several things. For starters, we are extremely innovative as a nation and as such new technologies are constantly being created for our context. The uptake of technological advancements is always very high!! However, even as we leverage technologies to leapfrog and compete globally in various sectors, the awareness of the associated risks is quite low. This essentially means that Kenya is excellent breeding ground for cybercriminals both locally and internationally.

Additionally, the lack of a clear legal and regulatory framework allows the majority these crimes to go unprosecuted. There is little to no deterrence in this area as the current fines and liability for cyber related offences are not proportional to the crimes being perpetrated today.

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

From my perspective, the investments in cybersecurity are nowhere near the level of threat. As all organisations now leverage technologies to gain competitive advantage, they need to also consider the cyber risk element which they are currently not doing. Beyond financial services sector, the threat is not readily appreciated by other professionals.

In your opinion what drives criminals to commit cybercrime?

To some extent it may be the lack of deterrence in the country. From the legal and regulatory framework, to the law enforcement agencies and the judiciary, there is low awareness and capacity in arresting the issue of cybercrime. Criminals are more proactive whereas we are extremely reactive to cyber threats.

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

No I don't think they have done ENOUGH. Additionally, I feel that what has been done is not publicized enough to maximize the impact. Based on this I believe government could do more to support the private sector.

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

Yes. A few people I know have fallen victim to social engineering attacks.

Were these cases reported to government authorities and prosecuted?

The cases were reported but not prosecuted to completion.

From a Kenyan context, what would be the top priority to address cybercrime?

From a legal perspective, I believe adequate laws can set the tone for real change in the approach to cybercrime. Beyond that, we need plenty of awareness exercises to ensure that people are sensitized and are alive to the imminence of this threat.



Brencil Kaimba

Risk and Compliance Consultant, Serianu Limited



Building Resilience in The African Cybersecurity Ecosystem

Cybersecurity ecosystem refers to the deep interdependence of many players that interact for multiple purposes with information as the life blood. Resilience in the ecosystem requires changes to the infrastructure, architecture and operations for the different players within it. This will not only help to extend the focus beyond resistance to shocks but also support long-term thinking about new risks and opportunities.

The Need for an Ecosystem

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

1. **IT Staff:** The IT team needs to embrace best practice in the development lifecycle, threat modelling and system hardening. This will ensure that protection is provided in the various network levels in an organisation.
2. **Non-IT Staff:** Upholding the requirements of the Information Security policy and by so doing, promoting the security posture of the organisation.
3. **Organisations** – Organisations need to document information security policies with relevant controls that will guide the implementation and operation of information security.
4. **Supply Chain** – To ensure confidentiality of business critical information assets is maintained, third parties should incorporate information security controls during system development and service delivery. Vendors also need to provide vulnerability reporting platforms to their respective clients in order to ensure that critical vulnerabilities are reported and remediated on time.
5. **Government** – The government is mandated with formulating and implementing cyber laws and creation of nationwide CERTs for incidence response and forensic investigations. For international initiatives, government needs to establish platforms that promote healthy collaboration between countries.
6. **Professional Bodies** – Professional bodies need to encourage their members to participate in security awareness initiatives just as much as skill/ technical training.
7. **Judiciary and Law Enforcement** – These bodies lack the skills and technology needed to identify cyber crimes and perform forensic investigations that will lead to successful prosecutions of cybercrimes.
8. **Academia** – The academia forms the backbone of information security research. More academic institutions need to incorporate security awareness in their curriculum to promote further research on emerging cyber threats in Africa and develop innovation hubs for young talent in the area of cyber security.
9. **Cyber Security Firms** – Cyber security firms have the advantage of large attack-knowledge base. This puts them in a unique and important position of providing visibility into the cyberthreat landscape for the other players in the ecosystem.
10. **Media** – The media plays an important role of spreading awareness to information system users by publishing cyber security events and providing information security awareness tips.
11. **Insurance** – Insurance companies need to provide cyber insurance and perform disaster preparedness drills. This will ensure that business continuity is assured for the various players in the ecosystem.



Serianu Cybersecurity Framework

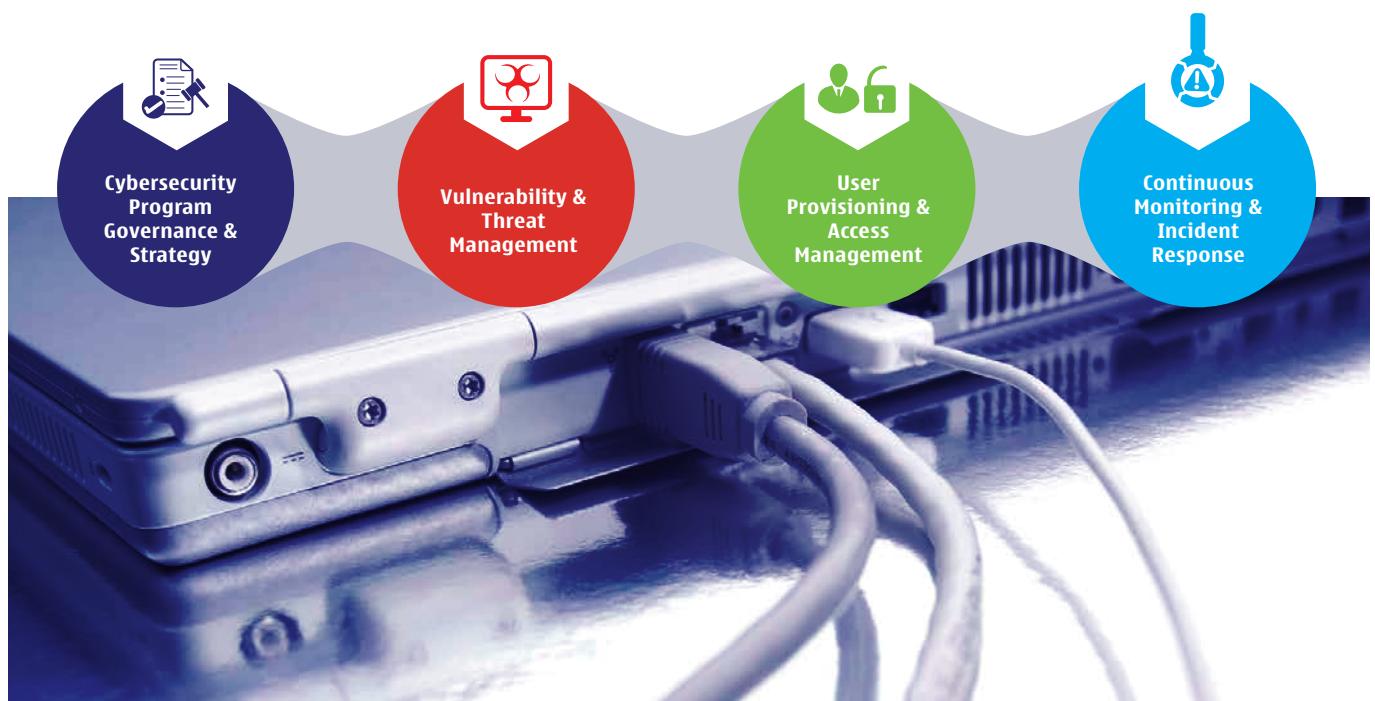
Introduction

Cybercrime in the African continent particularly within the Small Medium Enterprises (SMEs) setting is a growing concern. 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's become expensive for especially small and medium sized companies to adopt complex and or International cyber security frameworks. As such, cybercrime prevention is often neglected within the SME environment. This has resulted in a situation whereby SMEs are now one of the popular targets of cybercriminals. While at the same time, the SMEs lack a comprehensive framework that will help them determine their risk exposure and provide visibility to their security landscape without necessarily adding to the strained costs.

Solution

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, provide assurance that business operations will resume in the appropriate time in case of an attack or disruption.

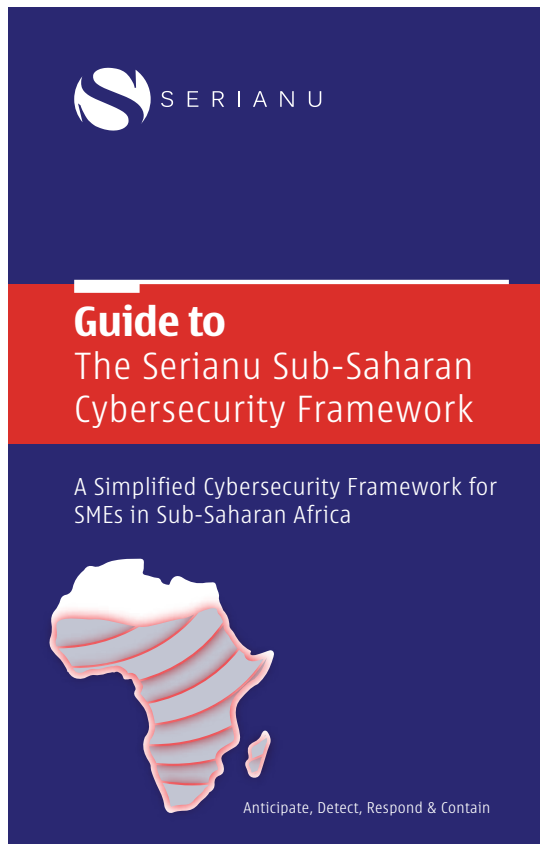


The framework is notably helpful also to small and medium-sized businesses seeking to implement global frameworks breaking down more complex categories and analysis into our four domains namely: **Cyber Security Program Governance and Strategy, Vulnerability and Threat Management, User Provisioning and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

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

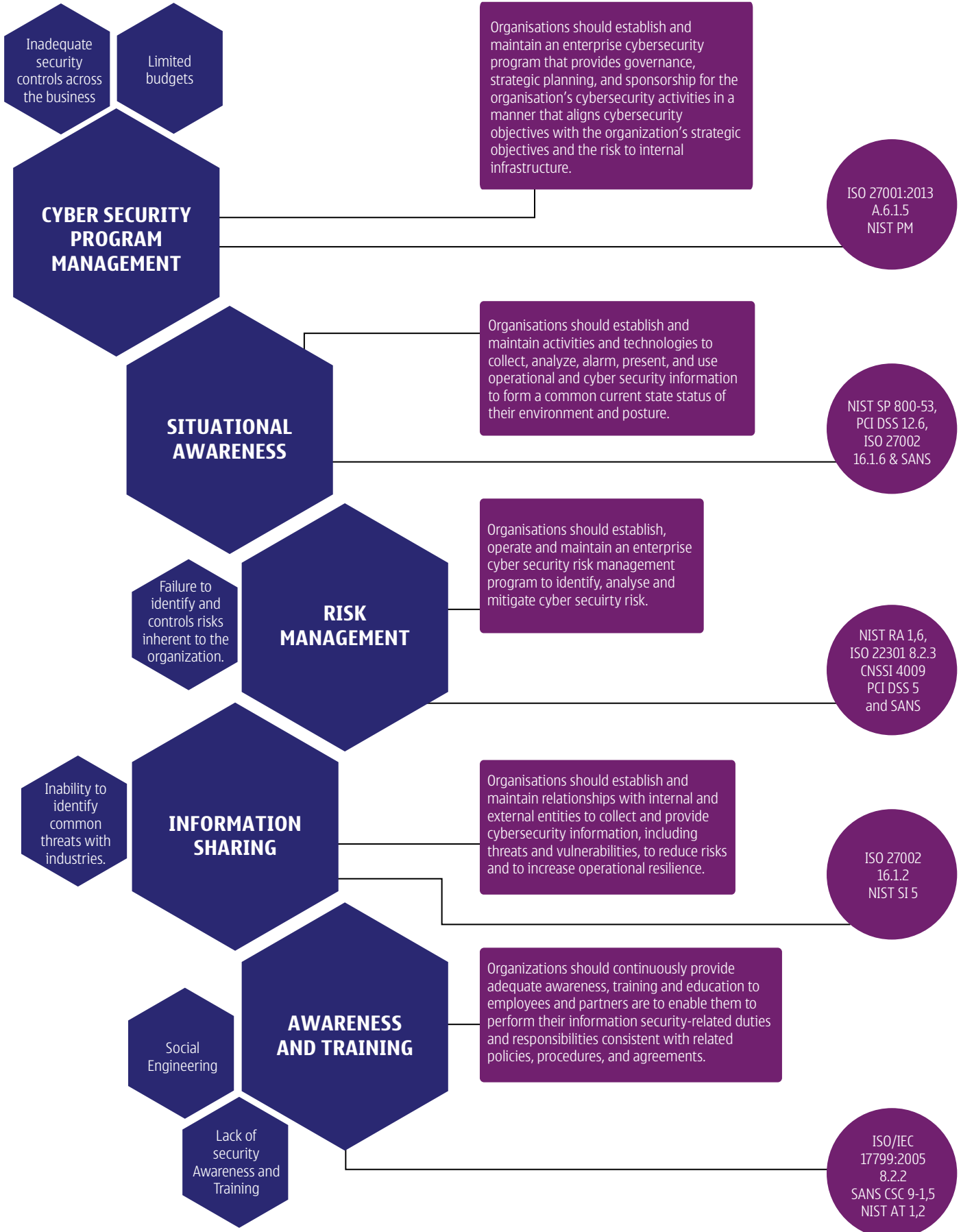
Our Framework

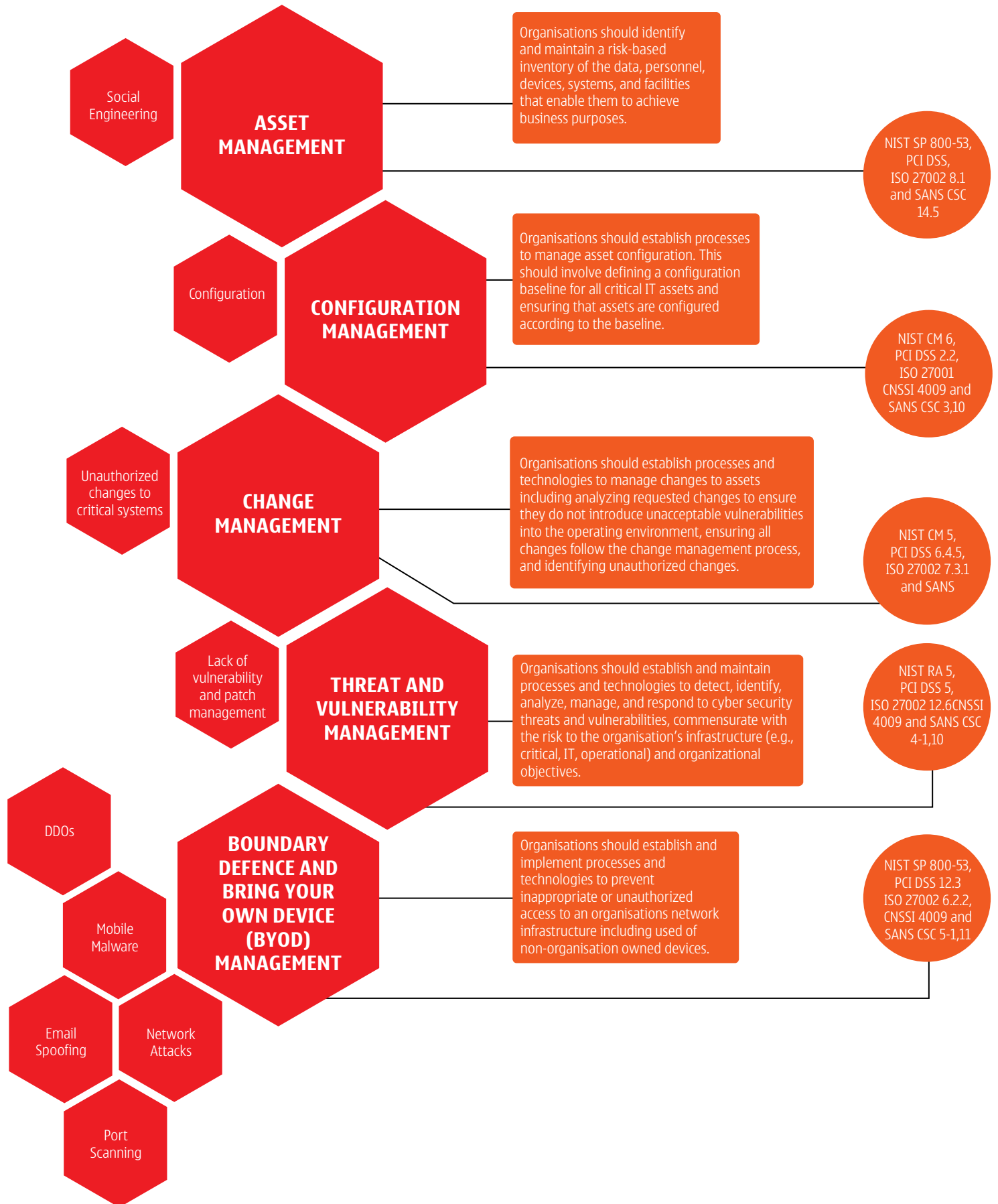
The Serianu Cyber security framework is detailed in the booklet provided separately.

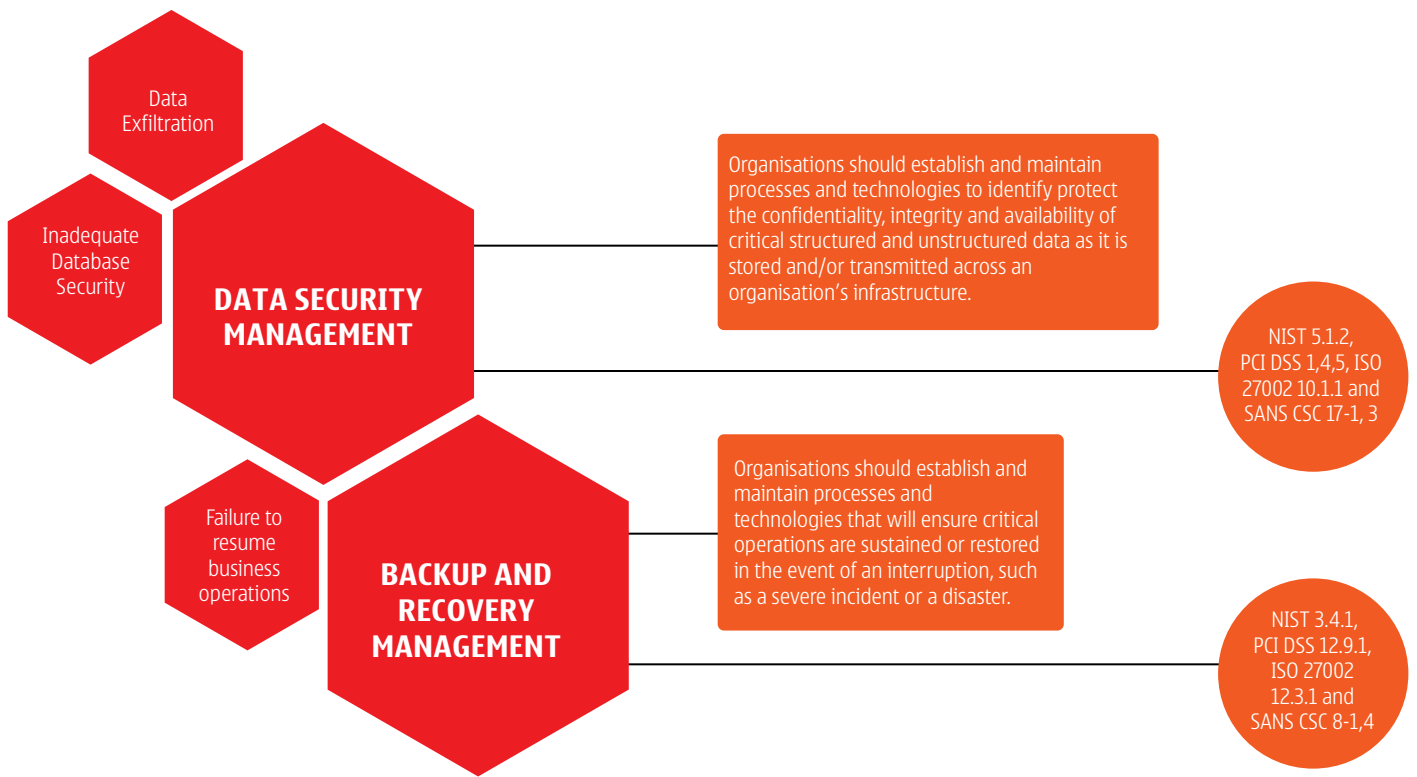


CATEGORIES

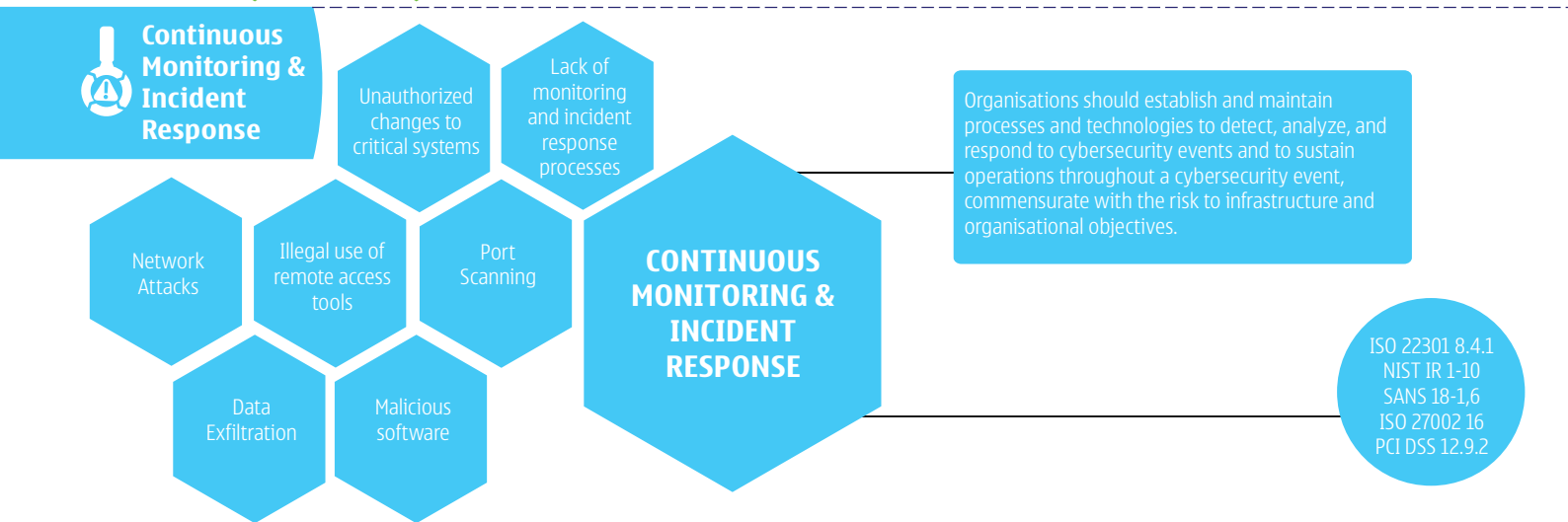
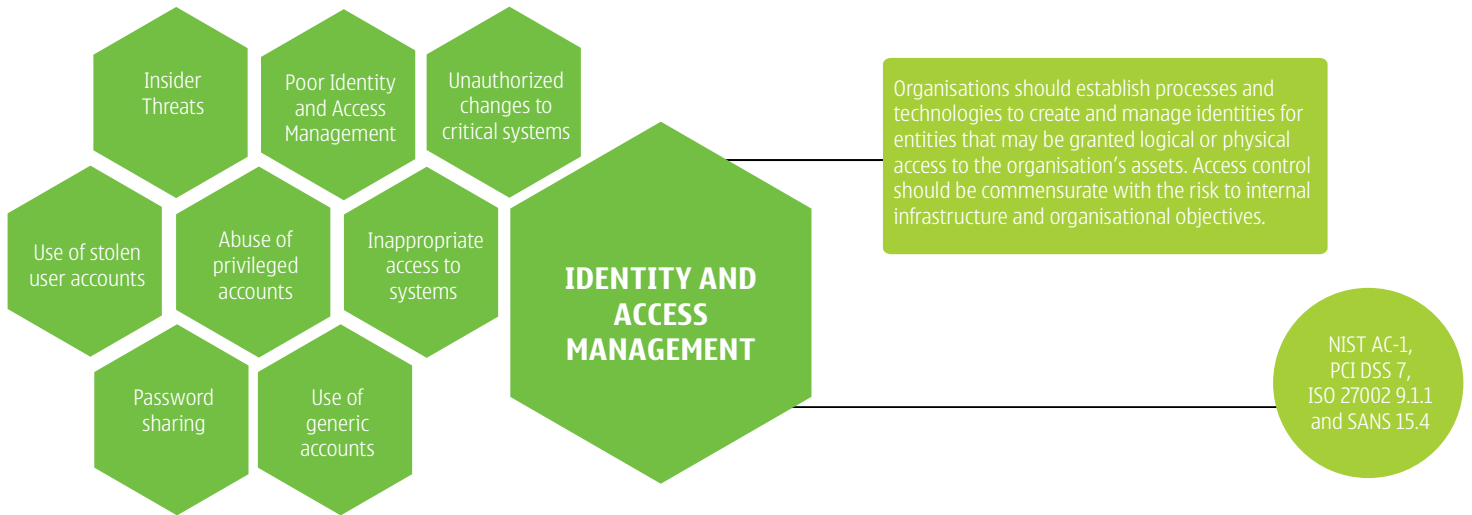








User Provisioning & Access Management **CONTROLS** **Definitions** **Global Frameworks Reference**



Central Bank of Kenya warns Employees of Imminent Cyber security attacks

By Eric Wainaina - May 25, 2016

#Anonymous #Leaks Employee Details from National #Oil Corporation of #Kenya

RECENT POSTS

#ANONYM #MESSAGE #CORRUPT #MAINSTR #MEDIA



CYBER SECURITY

University of Nairobi Twitter Account compromised by hackers

July 16, 2016 Nixon Kanali 0 Comment Communication Authority, Cybersecurity,

DAILY NATION NEWS BUSINESS COL

home > counties > kilifi >

Kilifi County loses Sh51 million to thieves

FRIDAY NOVEMBER 11 2016

HACKREAD

Security is a myth

HACKING NEWS TECH CYBER CRIME HOW TO CYBER EVENTS SECURITY SURVEIL

ASK TOOLBAR UPDATE FEATURE HACKED TO DROP MALWARE

MICROSOFT'S COLOR BINOCULARS APP LETS COLORBLIND PEOPLE SEE THE NORMAL WAY

CANADIAN ARMY RECRUITMENT SITE HACKED REDIRECTED TO CHINESE GOVT WEBSITE

PS TO PIRATE WEBSITE SHUT DOWN AFTER UKRAINE'S NATIONAL POLICE RAID

ANONYMOUS HACKING NEWS LEAKS

Anonymous Leaks ITB of Data from Kenya' Ministry of Foreign Affairs

by Waqas 7 months ago

STANDARD Digital

HOME KENYA WORLD BUSINESS OPINION HEALTH SPORTS ENTERTAINMENT BRANDING VOICE LIFESTYLE GE REPORTS



CARRY UP TO 1.3 TONS OF CARGO.



Your are here - Home - Business News

Equity Bank surrenders staff to KRA over fraud

By Paul Wafula

SHARE THIS ARTICLE

SOFTPEDIA DESKTOP MOBILE WEB NEWS

Softpedia News Security Security Blog

FLASH SALE: VDownloader 50% OFF!

Anonymous Rickrolls Kenyan Petrol Refinery as Part of Its Anti-Corporations Op

Group continues rickrolling campaign against corporations

Advertisements



Get paid faster Grow your business faster than anyone else

80% off limited time only

Mar 29, 2016 18:55 GMT By Catalin Cimpanu Share

After resurrecting #OpCanary two days ago, Anonymous hackers are continuing their defacement spree with a new rickroll of another corporation,

2 PHOTOS



ADVERTISEMENTS

HACKRI

HACKING NEWS

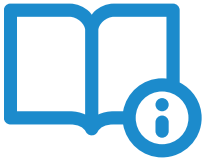
ANONYMOUS HAC

Anonymous Kenya's I

by Waqas 7 months ago

BUSINESS COUNTIES SPORTS BLOGS & OPINION LET A

loses Sh51 million to



References

Banking

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

Government

<http://ca.go.ke/index.php/component/content/article/93-general/333-ca-to-receive-itu-technical-support-to-fight-cybercrime>

Mobile money

<http://blogs.ft.com/beyond-brics/2016/06/14/mobile-moneys-unique-moment-in-kenya/>

<http://arcmediaglobal.com/index.php/events/mobilemoney-2016>

Betting

<http://www.nation.co.ke/sports/football/Betting-firms-cash-in-on-Kenyas-gambling-craze/1102-3067790-374h8f/index.html>

E-Commerce

<http://www.nation.co.ke/business/E-commerce-gaining-popularity-in-Kenya/996-3039162-d3q9j4/index.html>

Cyber Stalking

<http://www.standardmedia.co.ke/article/2000128956/kdf-and-spokemans-twitter-accounts-hacked-and-used-to-send-abusive-information>

Incidents

<http://www.reuters.com/article/us-cyber-kenya-idUSKCN0XP2K5>

<https://www.hackread.com/anonymous-hacks-kenya-ministry-foreign-affairs/>

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

<http://news.softpedia.com/news/anonymous-leaks-employee-details-from-national-oil-corporation-of-kenya-504671.shtml>

<https://www.hackread.com/anonymous-hacks-kenyan-oil-firm-against-police-brutality/>

<http://www.anonymouslatest.com/single-post/2016/05/30/Anonymous-Leaks-Employee-Details-from-National-Oil-Corporation-of-Kenya>

<http://news.softpedia.com/news/anonymous-rickrolls-kenyan-petrol-refinery-as-part-of-its-anti-corporations-op-502325.shtml>

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

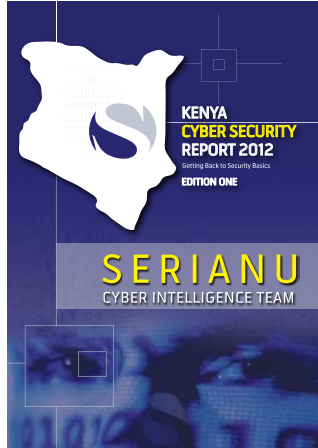
<http://www.standardmedia.co.ke/business/article/2000195162/equity-bank-hit-by-sh124m-fraud-in-tax-scam>

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

<http://techtrendske.co.ke/university-of-nairobi-twitter-account-and-blog-site-hacked/>

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

2012



2013 2014



2015

