



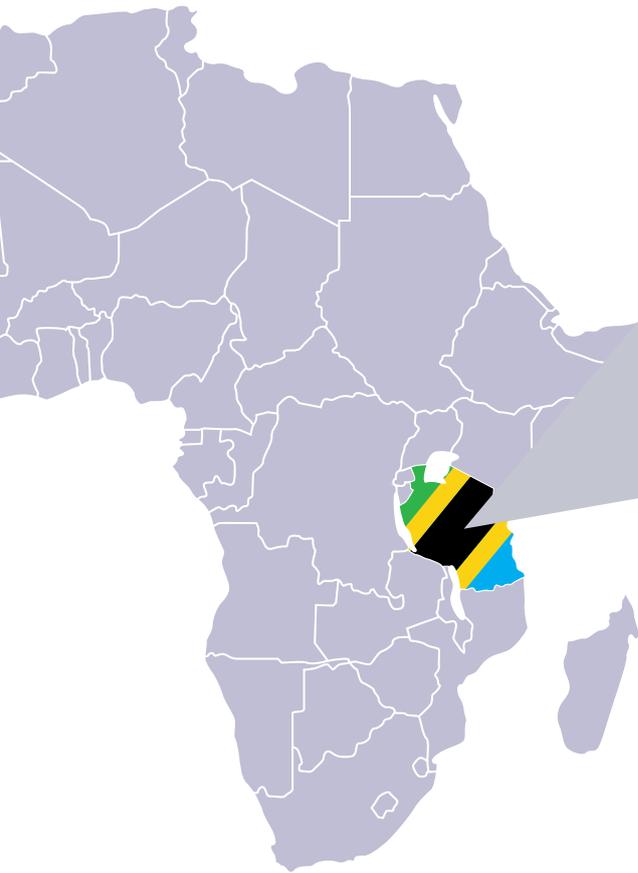
S E R I A N U

TANZANIA

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 Tanzania Cyber Intelligence Report
- 20 2016 Tanzania Cyber Security Survey
- 32 Risk Ranking by Sector
- 36 Top Cyber Security Issues in 2016
- 40 Top Trends Influencing Cybersecurity in Tanzania
- 43 The Serianu Cybersecurity Framework
- 50 References

About the Report

The Tanzania 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 Tanzania 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 Tanzania.

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

Dadi Masesa	Barbara Munyendo	Nabihah Rishad	Paula Musuva-Kigen	Newton Karumba
Robert Matafu	Faith Mueni	Samuel Keige	Secauose Onyibe	Andrew Ngari
Brencil Kaimba	Daniel Ndegwa	Jeff Karanja	Polly Mugure	Edward Owino
Kevin Kimani	Stephen Wanjuki	Hilary Soita	Kenneth Mbae	
Martin Mwangi				

Contributors

Peter Kisa Baziwe

Information System Audit and Security Professional

Robert I. Matafu

Kabolik, Tanzania

Neemayani Sanare Kaduma

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

Mike Laizzer

IT Risk Manager-NMB PLC

Paula Musuva-Kigen

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

(USIU)

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:

Kobolik Company Limited, Plot 11, Kishapu Street,
Kijitonyama, P. O. Box 31956, Dar es Salaam, Tanzania

Cell: +255 755 393 311

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

Foreword

Technology adoption is driving business innovation and growth in Tanzania while at the same time exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers and fraudsters are increasingly motivated to target our ICT infrastructure due to the value of information held within it.

The Tanzania Cyber Security Report 2016: Achieving Cyber Security Resilience; Enhancing visibility and increasing Awareness reports our technical findings from our analysis of over 1.6 million publicly accessible IP addresses and 138,000 network security events.

One of the most critical challenges facing Tanzania is the lack of awareness amongst technology users. Many of these users – mostly customers and employees, have little knowledge of the level of risk they are exposed to. Such exposure ranges 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 Tanzanian organisations to phishing and other social engineering related attacks.



We have estimated the cost of cybercrime in Tanzania to be USD 85 million. Perhaps more alarming from the analysis was the disparity between the cost of cybercrime and budget allocation to cyber security related products. While there are high levels of investment in technologies and automation across governments and the private sector, the study found that there was no matching investment in cyber threat prevention tools. Out of the organisations surveyed, (98%) did not spend any money or spent less than USD 5,000 annually on cyber security related products. Consequently, these organisations lack

Robert Matafu

kabolik, Tanzania



clear visibility (ability to accurately and completely view their posture) on the cyber security issues they need to watch out for.

As more and more Tanzanian organisations move to digitize their business processes and connect to the internet, the potential of cyber-attacks has risen across the country. This requires more capacity on the part of these organisations in being able to anticipate, detect, respond and contain (ADRC) such attacks. Unfortunately, a mid-sized business in Tanzania will lack these controls and will have at least one or two systems exposed to the internet with little or no security to prevent an attack. Such systems will have default passwords thus creating vulnerabilities that internal tech support are not aware of.



The Tanzania Cyber Security Report 2016 addresses these issues and focuses on raising cyber-attack visibility among local organisations and increasing awareness among employees and customers. Now, it's not a matter of if you will get attacked in the cyberspace, but a matter of when you will be.

98% of organisations spent less than **\$5,000** annually or none at all on cyber security related products



We need to conduct the following in order to ensure we are winning the fight against cyber crime:

- ◆ **Technical training** - there is a need for our technical staff to be equipped with hands on technical training in the concepts, principles, and techniques required to successfully prevent and/ or mitigate security issues on computing devices in a networked environment.
- ◆ **Awareness and Information Sharing** - The levels of awareness and information sharing in Tanzania needs to increase. What we know today will never be enough. We need to share information about incidents that have occurred and ways of mitigating them.
- ◆ **Collaboration** - In order to reduce cybercrime rates, Tanzanian organisations need to work together. This will require leadership at government and company level.
- ◆ **Government Policies** - Tanzania needs to strengthen the implementation of its existing cybercrime laws and policies. This will involve adopting more mature in cybercrime prosecution and raising awareness to citizens with regards to reporting cybercrimes.
- ◆ **Ecosystem Engagement** - There is need for each member of the Cyber security eco systems to be first, aware that they are part of the ecosystem and second, understand their role in the ecosystem. As Serianu, we have defined this ecosystem to contain but not limited to universities, research institutions, government Department of Defense, cyber security experts, media houses etc.

although teams can also work collaboratively to obtain greater resources and expertise in this fight against cybercrime.

Let's be ever vigilant in the protection of our information assets.

This study was made possible by the participation of our partners from research institutions, academia, legal enforcement agencies, computer security, and professional bodies. We would like to thank all the professionals, organisations and students who supported us in the development of this report.

William Makatiani

CEO, Serianu Limited



Executive Summary

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

The main objective for this study and in essence this report was to understand the current top threats, risks and levels of awareness in Tanzania.

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 Tanzania's cyber security landscape. We have broken down, analysed and summarized the top threats, risks and levels of awareness in Tanzania.

Highlights of the Report

- ◆ **The estimated cost of cyber-crime in Tanzania has soared to \$85 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 Tanzania has experienced numerous attacks through social engineering, use of malware and account impersonifications.** As one of the alternative channels for most banks, hackers are now exploiting the weak security controls around the mobile money platform to steal millions of dollars.
- ◆ **Malware targeting critical mobile and internet banking infrastructure are on the rise.** The results of the internal traffic analysis revealed that there are numerous forms of malware on systems including trojans such as Dridex and Zeus malware. Attackers are using these malware to compromise and access accounts. Unfortunately, statistics still remain vague as organisations are reluctant to reveal the extent to which they have been targeted by it.
- ◆ **Insider threat is still the largest contributor of direct losses in cybercrime in Tanzania.** Insider threats refer to fraud involving information or employee abuse of IT systems and information.
- ◆ **E-commerce growth has accelerated and we are seeing more integration of electronic payment systems into financial institutions.** At the same time, electronic banking and the cashless initiatives in the transport industry have been introduced in the country. This has resulted in some 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 which include CCTVs and nanny cams, Smart TVs, DVRs, Smart routers and printers, are routinely being hacked and used as weapons in cyber-attacks.
- ◆ **Numerous counts of vulnerabilities and systems misconfigurations.** The most vulnerable systems from the analysis were MikroTik routers, Apache HTTPD web servers, IIS Servers and Cisco routers. The most vulnerable applications identified were the exchange servers with Microsoft Outlook Web App being the most common mail server identified. Most of these devices have their administrative interfaces viewable from anywhere on the internet and their owners have failed to change the manufacturers' default passwords, making them highly susceptible to cybercrime attacks.
- ◆ **Technical training of employees is not sufficient.** The increase in

...at a glance



- ◆ Numerous attacks on mobile money through social engineering, use of malware and account impersonifications.
- ◆ Numerous attacks through social engineering, use of malware and account impersonifications.
- ◆ Malware targeting critical mobile and internet banking infrastructure are on the rise.
- ◆ Insider threat is still the largest contributor of direct losses in cybercrime.
- ◆ Acceleration of E-commerce growth and more integration of electronic payment systems into financial institutions.
- ◆ Increase in IoT threats.
- ◆ Numerous counts of vulnerabilities and systems misconfigurations.
- ◆ Technical training of employees is not sufficient.
- ◆ Lack of practical regulatory guidance from local industry regulators and government.
- ◆ Only 3% successful prosecution.

the number of home grown cyber criminals in Tanzania is not because they are more talented, it's because they are more creative, patient, single minded and they explore limitless pathways. Tanzanian organisations are not leveraging their own creative, curious analysts. Out technical teams are not empowered with tools and education to enable them explore the why.

- ◆ Low 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 local industry regulators and government** leads to poorly implemented and unenforceable security controls since they are not locally focused and instead are copied and pasted regulations.
- ◆ **Only 3% successful prosecution.** Inadequate training and awareness amongst the law enforcement and judiciary fraternity makes prosecution of these cases impossible.



Way Forward

Based on our research findings, most Tanzanian organisations are ill-equipped and unprepared to respond to information security threats. Although there are different initiatives (guidelines from Central Bank, Tanzania Communication Regulatory Authority in place set out to address information security issues in Tanzania, 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 Tanzania 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. Tanzanian entrepreneurs need to step up and work together to build and provide information security services that address these challenges. Together with researchers, the entrepreneurs 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 these 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, an organisation should ensure a needs assessment is conducted before adopting any form of employee training program. Generally, top issues that should be addressed by the program include: Social engineering averting, detection of phishing scams, email hygiene, internet usage best practices and password hygiene.

Continuous Monitoring and Log Analysis

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



Vulnerability and Patch Management

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

Continuous Risk Assessment and Treatment

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

Managed Services and Independent Reviews

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



Tanzania Cyber Intelligence Report

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

For the purposes of this report, we inspected network traffic inside a representative of Tanzanian organizations, reviewed contents of online network monitoring sites such as Project honeypot and reviewed information from several sensors deployed in Tanzania. The sensors perform the function of monitoring an organisation's network for malware, and cyber threat attacks such as brute-force attacks against their 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 in the period under review. This data represents malicious activity captured by our sensors and publicly available intelligence.

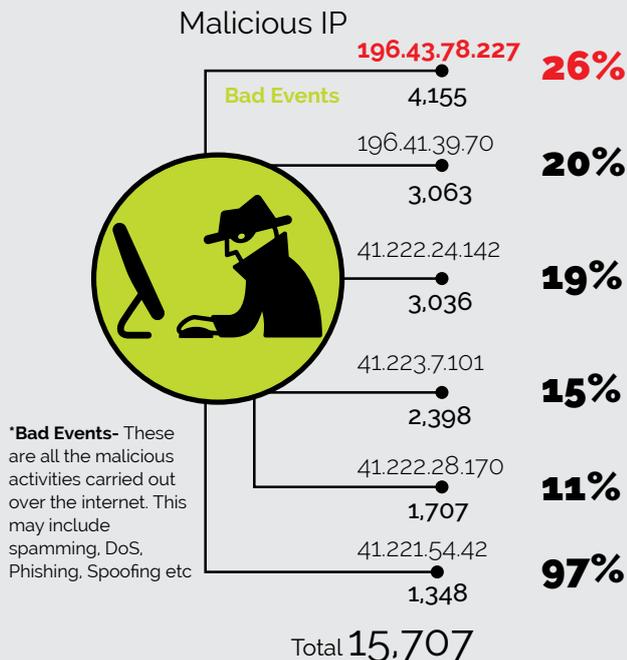


Project Honeypot Intelligence Analysis

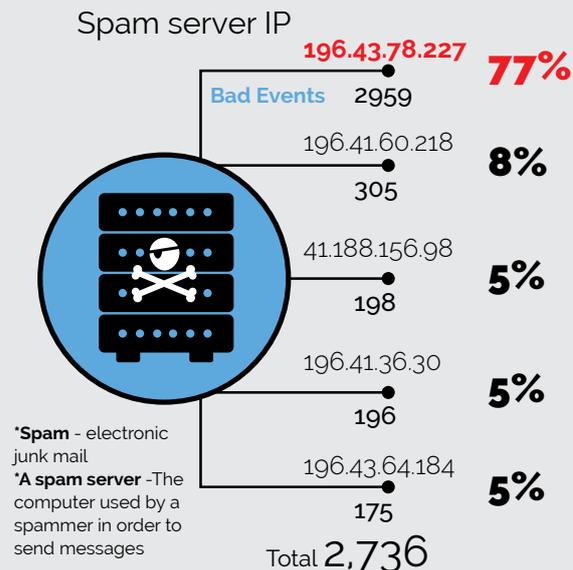
This section covers data from the honeypot project, a global database of malicious IP addresses. We analysed data specific to Tanzania.



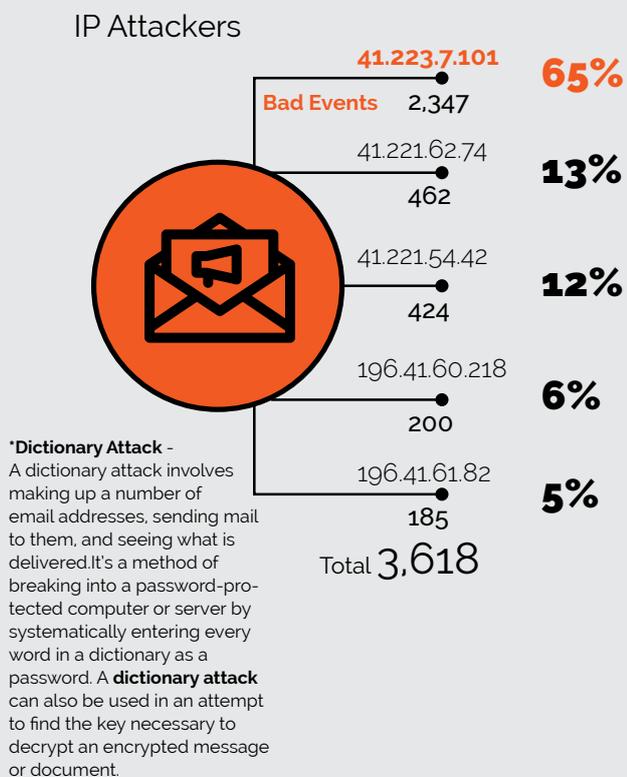
Most Malicious Local IPs



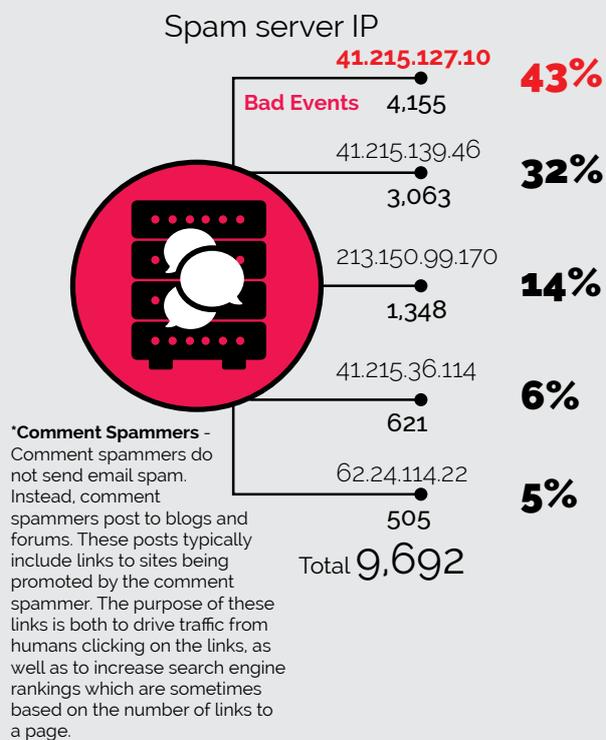
Top Spam Servers-Email



Dictionary Attackers



Top Comment Spammers



Scan Analysis

a.) Top Vulnerable Ports

Port 80 formed the highest percentage of the online running services at 16%. Running applications on this port comprised of routers, web servers, applications and web portal management systems which make them vulnerable to attack.

b.) Routers

MikroTik and DLink routers are the most vulnerable enterprise routers at 85% and 3% respectively.

c.) Web Servers

Microsoft IIS was the most vulnerable web server followed by Apache HTTPD.

d.) Applications

Hikvision formed the highest percentage of the analyzed applications.



Port 80
16%

Most Vulnerable Port

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

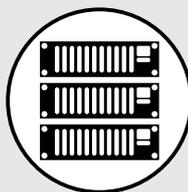
84%



MikroTik
84%

Most Vulnerable Enterprise Routers

Microsoft IIS
7%



Microsoft IIS
7%

Most Vulnerable Web Server

Apache HTTPD
4%



Hikvision

Most Vulnerable Application





Neemayani Sanare Kaduma

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

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

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

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

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

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

In your opinion what drives criminals to commit cybercrime?

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

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

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

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

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

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

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

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

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



2016 Tanzania Cyber Security Survey

The goal of the 2016 Tanzanian report was to explore the evolving threat landscape and the thousands of cyber-attacks that have been forged against individuals, SMEs and large organisations within Tanzania. Cybercriminals continue to take advantage of the vulnerabilities that exist within systems in Tanzania and the low awareness levels. This survey identifies current and future cyber security needs within Tanzanian organisations and the most prominent threats that they face.



About the Survey

This survey was prepared based on data collected from a survey of over 100 respondents across organisations in Tanzania. This included companies from the following sectors:

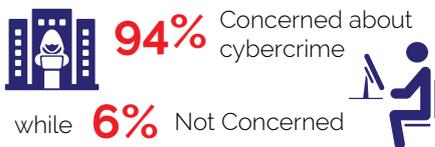


The respondents who participated in this survey included technical respondents (predominantly chief information officers, chief information security officers, IT managers and IT directors) and non-technical respondents (procurement managers, senior executives, board members, finance professionals, HR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

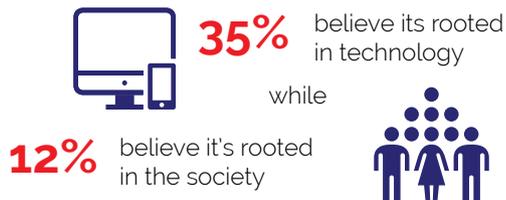
Summary of Findings

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

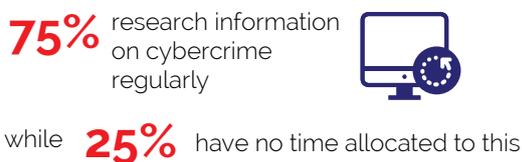
01 94% of organisations are concerned by Cybercrime.



02 CyberCrime is a problem rooted in technology, says 35% of the organizations.



03 75% research on cybercrime regularly but 25% have no time allocated to this.



04 More than 46% organisations DO NOT regularly train their staff on cyber security.



05 61% of organizations allow the use of Bring Your Own Device (BYOD)



06 59% of organizations don't have BYOD Best Practice Policies in place



07 20% of respondents have experienced Cyber crime in the last 5 years



08 71% of the victims have suffered negative impact of the effect of cybercrime



09 **91% of cybercrime cases go unreported to the police.**

91% did not report cases of cybercrime to the police




13 **87% of organisations apply system testing techniques?**

87% apply system testing techniques like penetration testing, vulnerability testing and audits.



10 **55% of organizations spend less than \$5,000 annually on Cyber security products.**

55% spend less than **\$5000** on cyber security annually



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

30% Databases contain the most critical information

followed by Emails at **23%**




11 **71% of organisations manage cyber security internally while 15% have outsourced to either an ISP or managed services provider**

15% outsourced to either an ISP or Managed Services providers while

71% manage cyber security internally



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

- 20%** Better encryption & improved privacy
- 19%** Better education of users of the Internet
- 19%** Improved technology for our networks and operating systems
- 17%** Improve our understanding of society and the cyber community
- 16%** Better laws and regulations



12 **Over 49% of organisations don't base their policies on international standards such as PCI and ISO.**

over **49%** don't base their policies on International standards like ISO 27001, PCI DSS, NIST etc while

33% 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 nothing 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 Tanzania 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, **majority of these organisations lack an internal device usage policy or BYOD policy to govern the usage of these devices.**

When it comes to managing cyber security, **the largest percentage of the respondents, 71% manage their information security in-house.** 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 30% of the respondents had Information Security Management certification while 41% did not have any information security management certification. 30% did not even know if anyone in their organisation had such certifications.

Also critical was the security testing within organisations **as 50% of the respondents carry out system testing in terms penetration testing and vulnerability testing,** 37.1% carry out audits while 11% 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.

Highlights of Tanzanian 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

! **61%** of organisations have allowed BYOD however, **59%** of these organisations don't have any BYOD policy

! **71%** manage their security in-house, **15%** have outsourced these services to either an ISP or a managed security services provider.

...cont

30% had Information Security Management Certifications,

41% don't have

while **30%** had no knowledge of the existence of such certifications within their organisation.

50% carried out penetration and vulnerability testing,

37.1% carry out audits

while **11%** 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

With the increased rate of cybercrime in Tanzania, **most of the respondents (20%) have experienced cybercrime in one way or another.** Out of these, 65.9% was through work while 34.1% at personal capacity. This highlights the importance of incorporating cyber security awareness and vigilance in work areas as it's the most targeted environment.

There are low levels of awareness within the Tanzanian region hence it is no surprise that when it comes to **reporting of cybercrime to the police 91% of cyber security incidents either go unreported or unsolved.** Only 1% of the reported cases were reported and followed through to a successful prosecution.

External infrastructure vulnerabilities identified during the survey include unnecessary services enabled such as content management and remote administration, misconfigured SSL certificates and encryption settings. These vulnerabilities can allow unauthorized access to critical systems

The results of the internal traffic analysis revealed that there are numerous forms of malware on systems including trojans such Dridex and Zeus malware. Most of these malware go undetected on systems.





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.

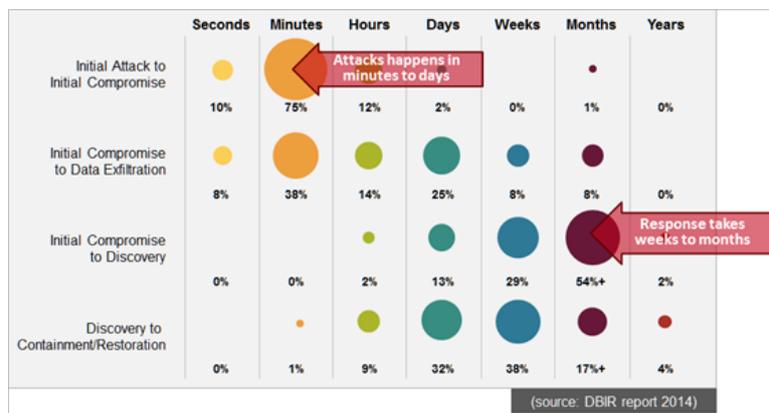
Asymmetry in Cyber Security

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.

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

State of Detection and Response

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



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

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

Speed as the new Determinant of Success

Given that breaches are inevitable and 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-

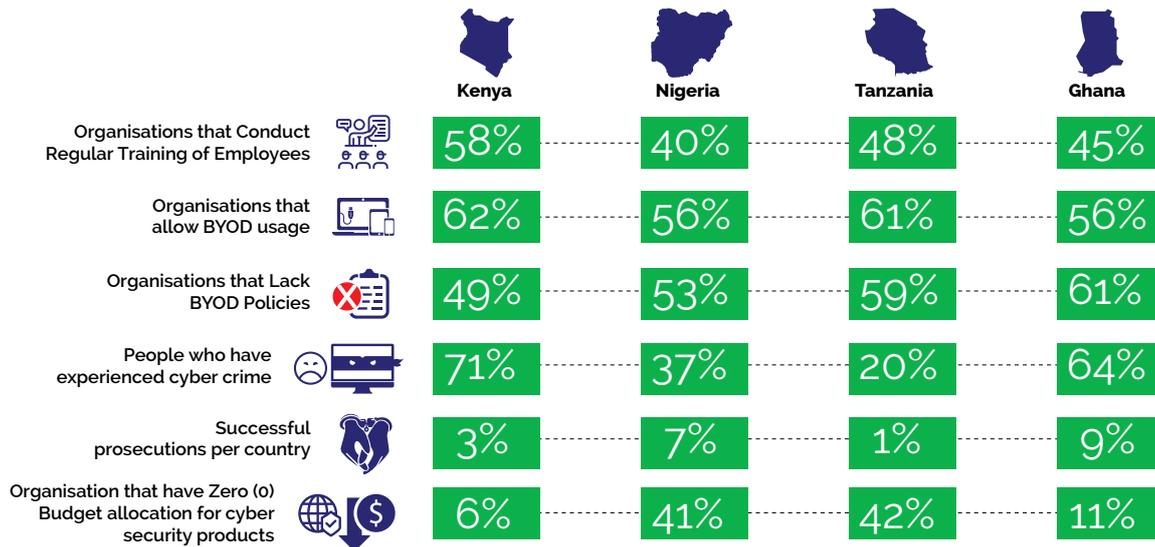
- 1. 360° Situational Awareness:** For fast discovery of attacks, the security operations should have full visibility into every asset, user activity, network traffic, system vulnerabilities and network topography at all times. Today, such visibility is limited to critical assets and users, which severely 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.

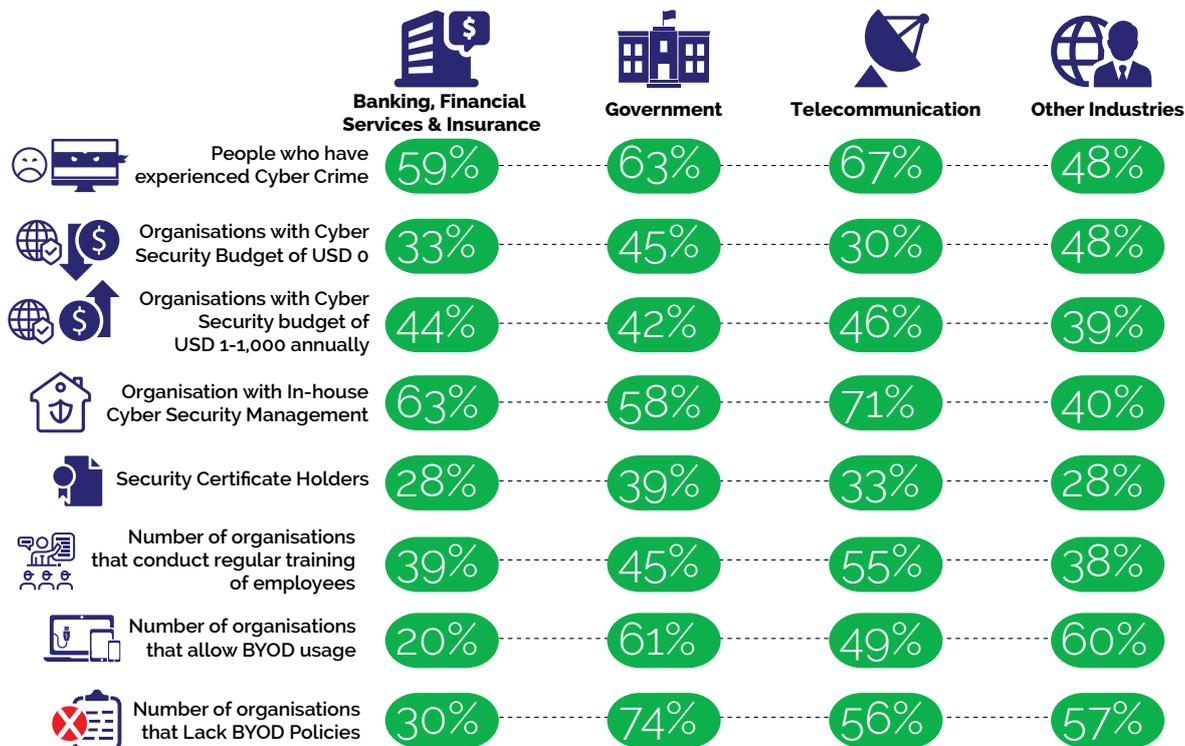
Inter Country Analysis

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 Tanzania

Summarized Findings Report – What are cybersecurity Gaps in Tanzania?

*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 Tanzanian 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



Peter Kisa Baziwe

Information System Audit and Security Professional, Tanzania



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

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

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

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

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

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

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

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

5. Big Data and the Cloud:

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

Solutions

- 1. National Cybersecurity Strategy.** This is urgently needed to direct resources and plans to securing our critical national cybersecurity infrastructure. I am glad to say this is already in the works as announced by the Permanent Secretary Ministry of Transport Communications and Works in September.
- 2. Education.** Cybersecurity awareness for citizens in use of internet, mobile banking and payment services; training of cybersecurity professionals and defenders, the Judiciary and Military; encouraging cybersecurity competitions and cyber clinics like one held at BUNI tech hub at Costech. These are crucial steps in boosting our incidence response and remediation capabilities. ISACA Tanzania is planning to be at the forefront of this by pushing the ISACA Cybersecurity certification- CSX.
- 3. Collaboration.** There is need for both Government, Private Sector and Academic institutions to have forums that discuss and tackle these cybersecurity challenges. In the Private sector we have and see different challenges and threat actors. Sharing of solutions trends, intelligence and research is vital to keeping abreast in this dynamic field. As shown in the Costech funded – State of website security report -April 2016 of Gilbert Kilimba. It enables us to gauge where we have gaps in IT Security Practices.

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



Risk Ranking by Sector



1. Banking and Microfinance

Cyber-attacks are increasingly seen as a top concern for banks and microfinance institutions. This is mainly because of the large amounts of money that these institutions hold. In recent times, we have witnessed several banks get compromised through attacks such as card skimming, use of malware and the most common attack vector, insider threat. The increased adoption of newer (and potentially high-risk) technologies including mobile and internet banking further puts these institutions at risk because these systems are more often than not configured in networks that have inferior security systems in place and weak underlying infrastructure.



2. Telecommunications

Telecommunication sector comes second in our risk ranking. With the huge volumes of data that these organisations handle and the large number of infrastructure that they support including financial institutions and government, they have become a lucrative target for cyber criminals seeking to disrupt service delivery and infiltrate critical data. In February 2016, Anonymous – a well-known Hactivist group – claimed to have hacked a state owned telecommunications firm's database and leaked 65000 employee records under their "Operation Africa" campaign. Tanzania Telecommunications Company LTD (TTCL) however denied the claim and said in a public statement that TTCL only had 1557 employees in their database. The hactivist group maintained that the records included retired and deceased personnel files. Earlier in the year, the Tanzania Communication Regulatory Authority (TCRA) fined the five largest telecommunication companies in the country for failure to protect their customers against information security threats.

This goes on to show that there is indeed a dire need for companies in this sector to strengthen security controls around their services and infrastructure.



3. Other Financial Sectors

Sacco's, cooperatives and microfinance institutions are rapidly gaining popularity and increasing their customer and financial base in Tanzania. This is mainly due to their customer friendly rates and reduced ease to which one is granted access to their facilities. However, because these organisations are so focused on customer satisfaction and reducing costs, they tend to neglect investment in cybercrime prevention. This has resulted in a situation whereby they are now one of the popular targets of cybercriminals. Even worse is that larger financial institutions/ banks are getting harder to penetrate since they've invested in security for years. This means the same hackers who once targeted these big institutions/banks are seeking the easier prey; Sacco's, credit unions, small hedge funds, PR firms, and a wide variety of other SMEs.



4. Mobile Money Services

Majority of banks, merchants and service industry firms in Tanzania are now adopting mobile money services to serve as one of their alternative channels. Mobile money is integrated into the other sectors including hospitality, banking, transportation, telecommunication, E-commerce, government and other financial sectors. With that growth comes a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks, risky consumer behavior. It does not matter whether an institution uses a proprietary or third-party mobile banking application – they still own the risks. In recent times, hackers have exploited the weak security controls around the mobile money platform to steal millions of dollars especially from banks.



5. Hospitality & Retail Sector

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



Michael Laisser

IT Risk Manager-NMB Plc



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

Yes it is one of the emerging white collar crimes in Tanzania.

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

The rise of mobile technology which increases the effect of social engineering frauds, ATM card-skimming, identity theft. The adoption of Western behaviors and Western cultures has also attributed to crime such as underage pornography.

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

Not enough effort has been done, investing in cyber security is not a onetime project. It needs long term commitment and ownership from the government and all stakeholders.

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

- ◆ Opportunistic crime
- ◆ Ease of Anonymity
- ◆ New technology
- ◆ Inadequate legal jurisdiction

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

To some extent. The enactment of Cybercrime Act, National ICT strategy, introduction of CERT-TZ-computer emergency response Team has helped to boost the fight against cybercrime. However it will take time for these processes to be fully mature and efficient.

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

Yes, I do.

Were these cases reported to government authorities and prosecuted?

Yes, some have been reported and prosecuted and some are still in investigation.

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

Educating the Community to Protect Themselves

- ◆ As with crime in the physical world, no amount of action by government and the private sector can prevent every cybercrime, those of us who use digital technologies have to take responsibility for our own security and safety and exercise safe practices.
- ◆ Most instances of financially-motivated cybercrime like social engineering fraud and ATM skimming, identity theft can be prevented by taking simple steps or by knowing what to look out for. Governments and private sectors can assist users to understand these steps and to recognize the warning signs, this can be achieved by conducting awareness programmes through different media.

Fostering an Intelligence Led Approach

Criminals are quick to find ways to exploit new technologies to further their illicit activities. Authorities like Police Force, TCRA, BOT and SSRA must stay up-to-date with these methods so that they can recognize emerging trends, patterns and problem areas. Sharing quality, timely and comprehensive information and intelligence will lead to better understanding of cybercrime and more effective responses.



Improving capacity and capability to fight cybercrime

- ◆ The capacity and capabilities of our agencies, particularly law enforcement agencies, need to keep pace with evolving technologies if police are to perform their duties in the digital environment. At the most basic level, all police officers need to know how to gather and analyze digital evidence, leaving specialist units to focus on more complex cybercrimes. Specialist units within law enforcement agencies must have the training and capabilities to detect and investigate the more complex and sophisticated use of technology in criminal activities.

Assisting prosecutors and the judiciary to deal with cybercrime and digital evidence.

- ◆ Prosecution of cybercrime offence is an important part of the enforcement framework to deal with cybercrime and assists in creating and maintaining public confidence in our criminal justice system, in order for cybercrime offences to be prosecuted effectively,

prosecutors and judicial officers need to be able to understand and evaluate technical digital evidence. While courts and the legal profession are becoming more accustomed to the use of new technology to commit crime, the admission of digital evidence can still be a technical process. As the use of technology in crime grows, prosecutors and judges will increasingly be required to present and understand highly technical details in order to effectively administer the cybercrime Act2015 and the like. Government can continue to assist prosecutors and the judiciary by providing the resources they need to respond to legal concepts associated with the new technology and the facilities they need to analyze and consider digital evidence in a court setting.

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

Can also be addressed by answers above.



Top Cyber Security Issues in 2016



E-payments and E-commerce Fraud

Tanzania is on the move to battle the encroaching fraud in the electronic payment system creeping into businesses and resulting in financial loss. An advancement in the tactics used by cyber criminals keep increasing and varying. A local bank in Tanzania was attacked by a wave of card skimming techniques and only discovered the loss of billions of shillings after customers complained that their accounts had been drained. The large amounts of money that these systems process coupled with their insecure configurations has contributed to them being a favorable target for attackers. Even though the government has enacted the National Payment System Bill, 2015, it is critical that these laws and policies be implemented in order to reap the full benefits.

1

Cyberstalking / Social Media Abuse

Cyber stalking is a form of harassment that involves the use of technology to pursue a victim. This year, five people were charged for comments made on WhatsApp and other social media platforms about the President. It is however encouraging to note that efforts have been put in place to curb this vice. This includes the launching of The Tanzanian Computer Emergency Response Team (TZ-CERT) to monitor the production of "racist and xenophobic" content online, child pornography and online impersonations, all of which are considered a crime under the cyber law.

3

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 that go undetected on systems. Email has been noted to be one of the most common means of transmitting malware. These usually contain malicious attachments which when downloaded infect the victim's computer. Lucrative online advertisements are also used by cyber attackers to compromise victims' systems.

2



Insider Threats - 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. Most of these insiders make use of privileged or administrator accounts to carryout malicious transactions. The motivating factors for these attacks include 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.

Identity Theft

Identity theft is a crime whereby cybercriminals impersonate specific individuals. This is particularly prominent during sim card registration where fake identity during sim card registration was noted. This year we have witnessed the Tanzania's telecoms regulator fine six mobile phone operators Tsh552 million (\$258,000) for laxity in sim card registration. The fines came less than three weeks after the Tanzania Telecommunication Regulatory Authority (TCRA) switched off 1,830,726 IMEIs.



4

Internet of Things (IoT)

IoT's have been adopted into various sectors of the economy including agriculture, healthcare, energy and transportation. Devices in the IoT have their associated vulnerabilities. Most organisations are seeking to purchase and implement cheaper devices without considering their associated vulnerabilities. These have critical security issues such as default or hard coded passwords, remote code execution, open access point connections and lack of properly segmented network.



7

Social Engineering

Organisations across all industries in Tanzania are continuously reporting an increase in a variety of technologically sophisticated social engineering attacks. This is a clear indication of the popularity of these attacks and the inability of organisations to stop them. It is however encouraging that initiatives have been put across to address this issue.



6



5



Government Response and Strategies

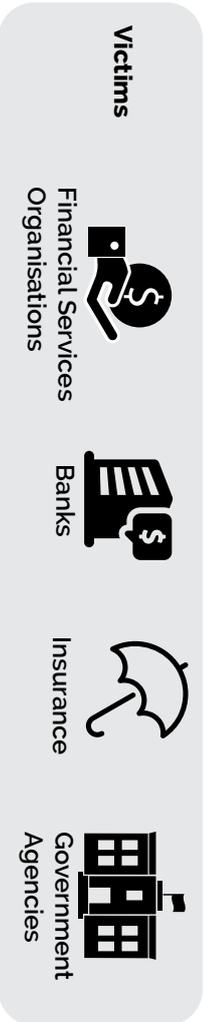
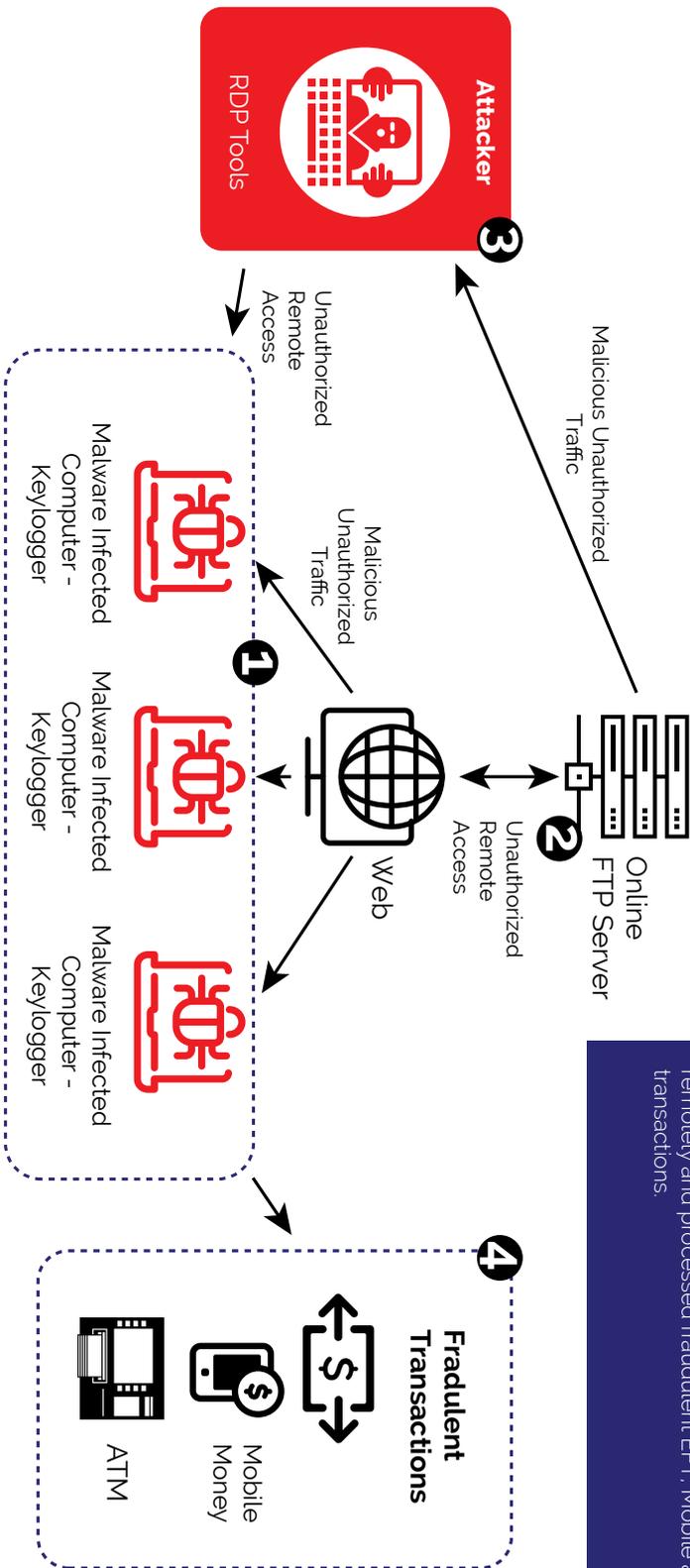
- ◆ Cyber law passed in 20th Feb 2015 has been used to combat such crimes
- ◆ Tanzania Police Force continues to conduct capacity building to its staff in collaboration with other stakeholders, procure new investigative tools, educate and make the public aware through media.
- ◆ To collaborate with financial institutions that deal with cyber crime



Total No of Incidents reported in Tanzania

2010	444
2011	542
2012	414
2013	333
2014	380
2015	1,823

Attack Vectors



Anatomy of an African Cyber Heist

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

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 ICT Trends Affecting Cybersecurity in Tanzania



Mobile and Internet Usage and Costs

The number of mobile and internet users has rapidly increased this year. Mobile money in Tanzania is now integrated into a number of industry sectors including hospitality, banking, telecommunication and e-commerce. Internet Service Providers (ISPs) are continuously expanding their network coverage areas and constantly keeping competitive prices making internet access cheaper across the country. However, we are seeing an increase in cybercrime related activities such as online scams, identity theft and social engineering. Citizens lack the necessary security awareness knowledge that is required when using the internet.

monitoring system, AMP-IFMIS integration and iTax Tanzania. With transfer of most processes from the physical world to the cyber world, this opens up the country to a lot of attack vectors. The lack of awareness on the part of the end user, privacy concerns, unreliable distribution and delivery process and lack of properly secured infrastructures has led to the increase in cyber-crime activities through these established channels. Attacks such as online scams, identity theft and credit card fraud are on the rise as a result.



BYOD

Research has shown that there is widespread BYOD acceptance in Tanzania. This is reflected by the 56% of respondents who were allowed BYOD within their organisations. However, it is worrying to note that security concerns around BYOD have not been considered a top priority for most organisations that have adopted it. Most organisations lack acceptable use policies and procedures, an internal device usage policy, a security policy and/or a BYOD policy to provide guidance on the use of these devices.



Cloud – Based Solutions

Many organisations in Tanzania are steadily embracing cloud computing solutions for different business and technological benefits. Majority of these organisations have adopted cloud applications services like Oracle cloud and Microsoft 365. From a security perspective, this trend has given rise to two security issues; traditional security controls can no longer help protect local business critical systems. Also Tanzanian companies are losing visibility of their security posture. It's therefore paramount that even with cloud adoption, businesses should review the Service Level Agreements and contracts with the cloud providers to ensure security of their data and systems.



E government

Through the e-government initiatives, we have witnessed numerous reforms on government processes, ultimately making services more convenient and easily accessible. Some of the initiatives include mobile phone traffic



Outsourcing- Vendor Risk

Most Tanzanian organisations don't possess all the skills and expertise needed to complete every project in-house and as such are turning to third-party providers for a variety of essential services. However, with the increased reports of data breaches involving third party vendors, outsourced vendors are now described as the greatest risk to the security of most organisations in Tanzania. Tanzanian organisations don't perform regular risk assessments on their existing and potential vendors. Third-party management best practices and service-level agreements (SLA) are also not prioritized in most local organisations.



IoT

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



Industry Regulation

In 2015, the Cybercrimes Bill was passed into law. This was to address the different cyber related crimes within the country. E-Government is currently pushing government and parastatals to use 'go.tz' in efforts to help curb phishing. TZ-CERT (Tanzania Computer Emergency Response Team) is a team under the TCRA (Tanzania Communication Regulatory Authority) tasked with the responsibility of providing a high and effective level of network and information security consisting of services such as monitoring cyber security threats and vulnerabilities and advising constituencies and public and incidents response. Even with these measures, it's apparent that these laws alone cannot address the growing challenges of cyber security such as cyber terrorism. There is need to improve the capacity of relevant ICT and cyberspace stakeholders for the training and support of cyber security officials and the sharing of cyber security best practice from across the globe.



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. This is because the internet is far reaching and offers more media coverage.



Poverty Rates - Unemployment Rates

The high rate of unemployment in Tanzania 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.



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 needed 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

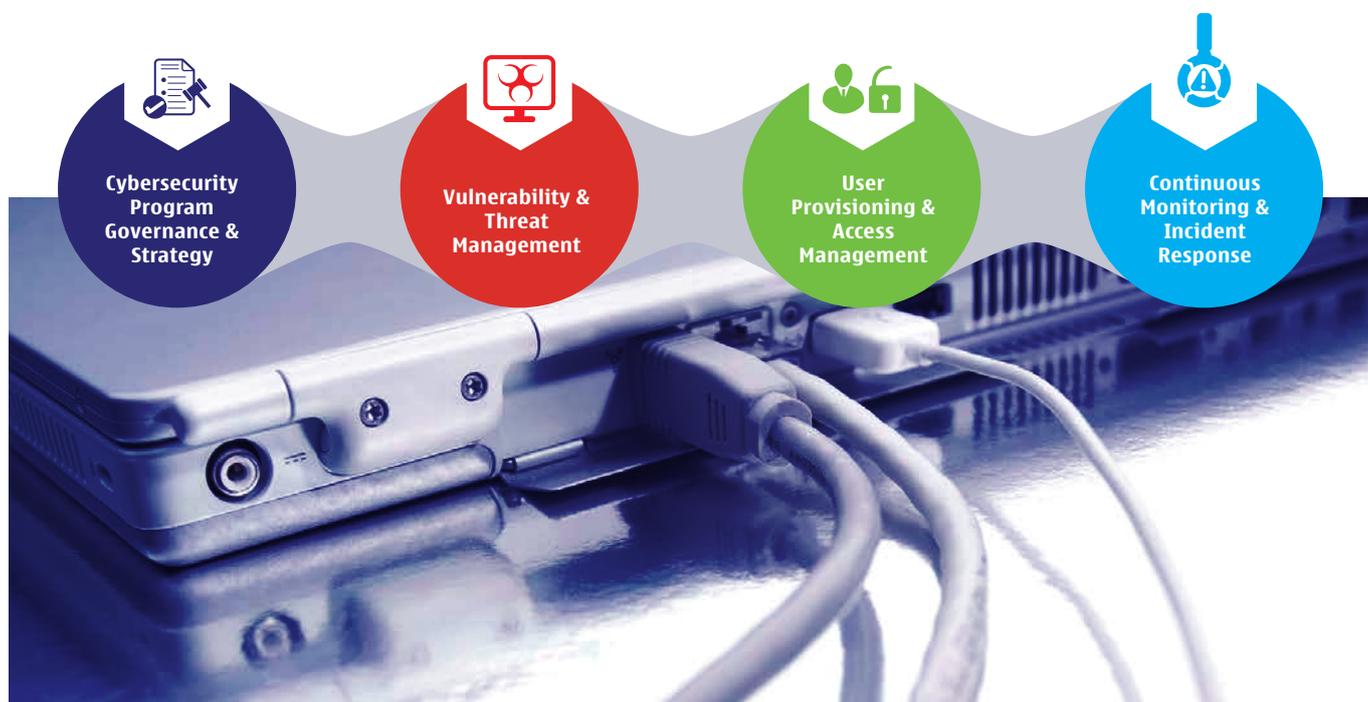
Introduction

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.

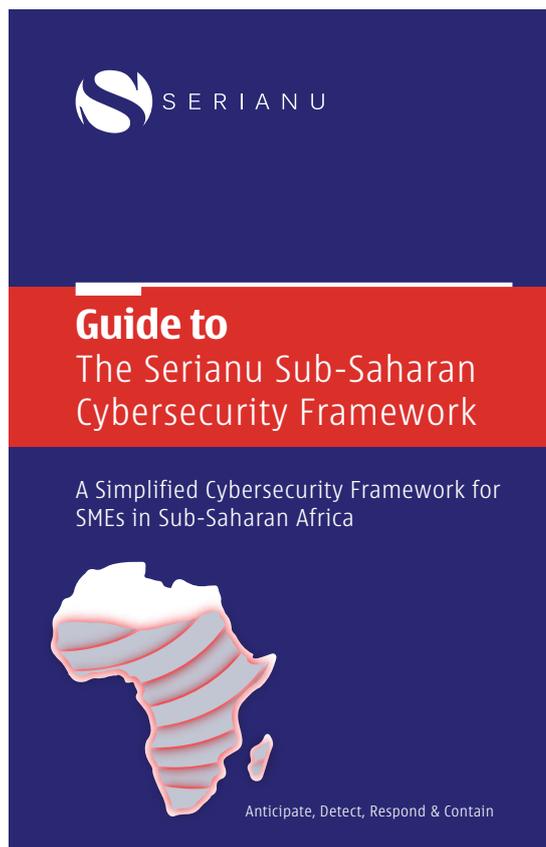


The framework is notably helpful also to small and medium-sized businesses seeking to implement global frameworks breaking down more complex categories and analysis into our four domains namely: **Cyber Security Program Governance and Strategy, Vulnerability and Threat Management, User Provisioning and 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

Cybersecurity Program Governance and Strategy

- Inadequate security controls across the business
- Limited budgets
- Lack of management buy-in
- Failure to identify & controls risks inherent to the organization
- Inability to identify common threats with industries
- Lack of security Awareness and Training
- Social Engineering

Vulnerability & Threat Management

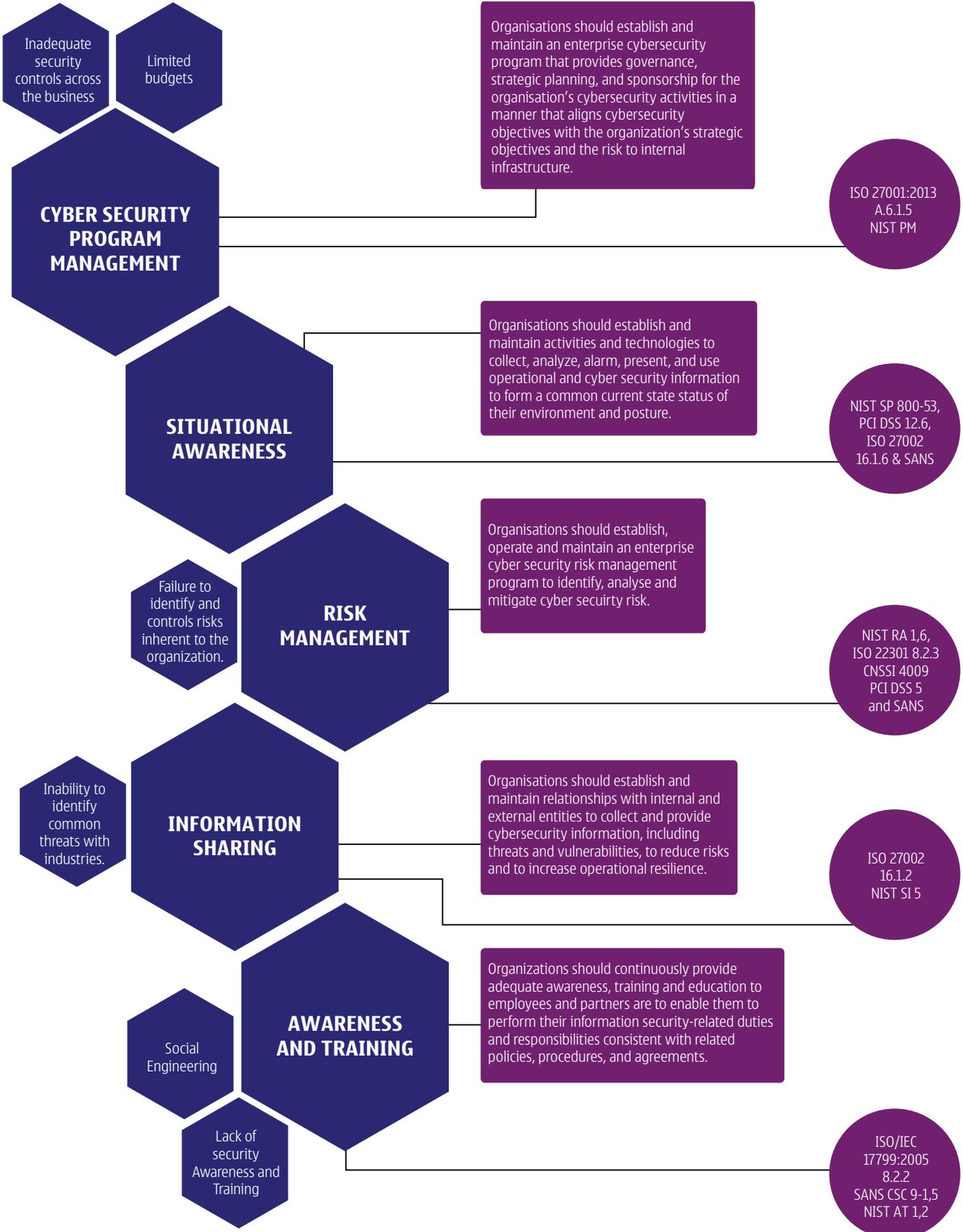
- Failure to identify all possible risk prone assets to the organization
- Misconfigurations
- Unauthorized changes to critical systems
- Lack of vulnerability and patch management
- DDOs
- Mobile Malware
- Email Spoofing
- Network Attacks
- Port Scanning
- Data Exfiltration
- Inadequate Database Security
- Failure to resume business operations

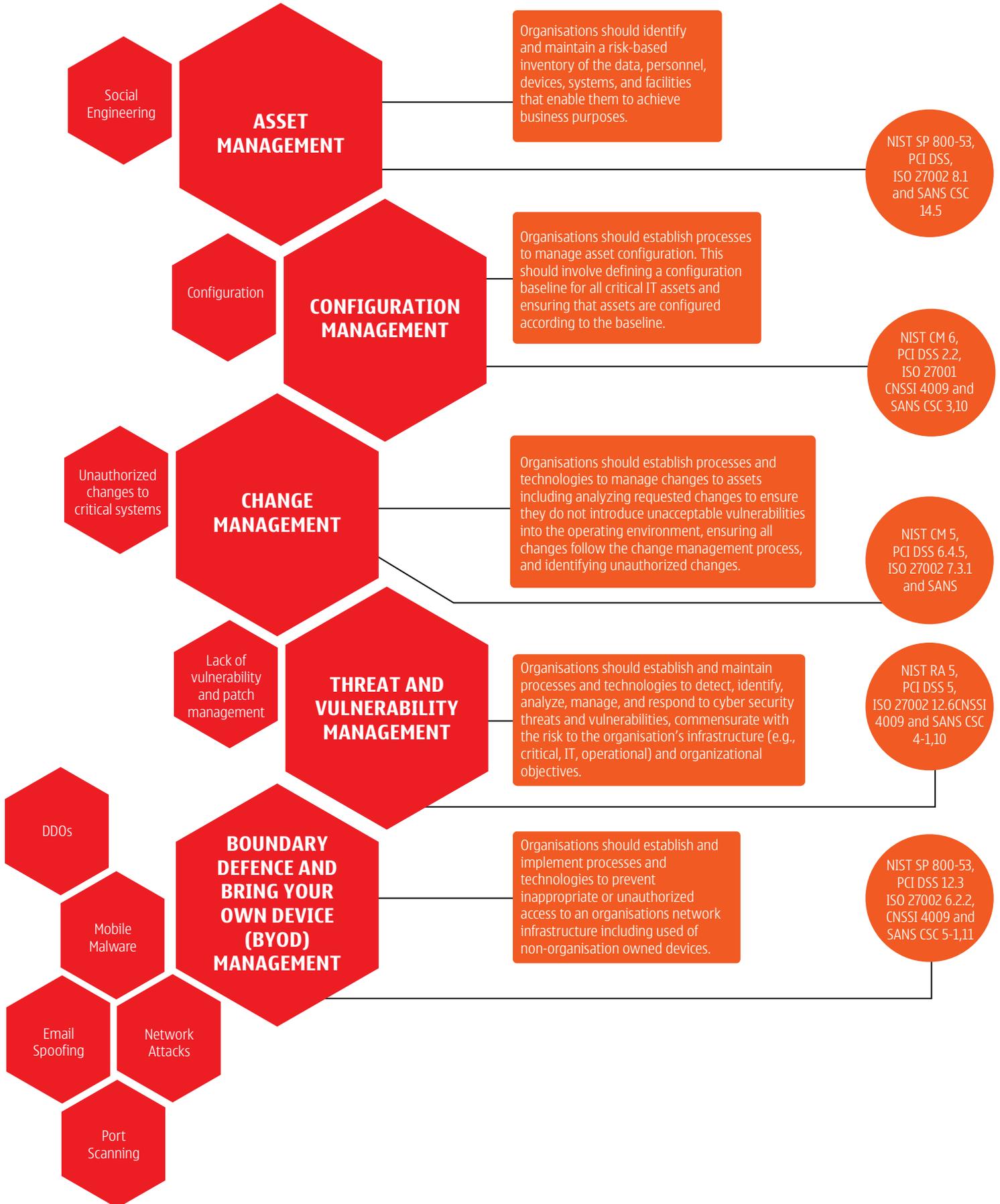
User Provisioning & Access Management

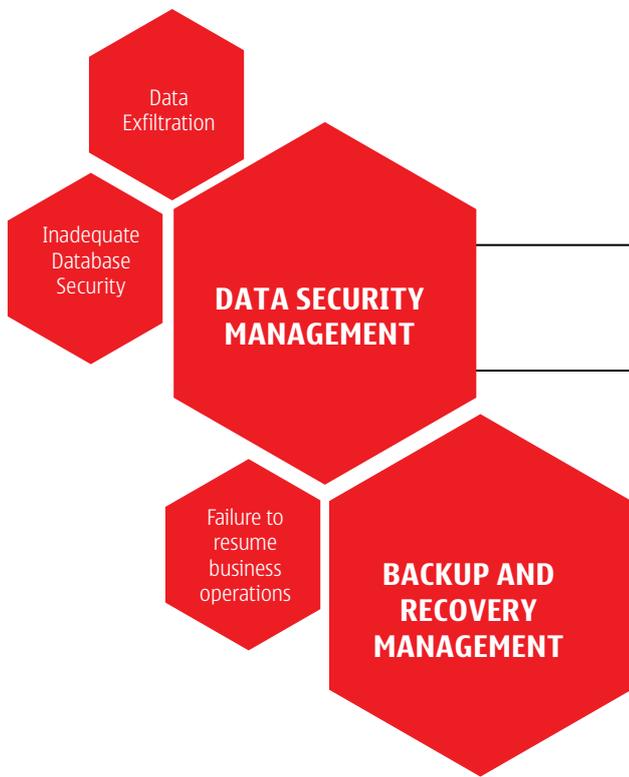
- Insider Threats
- Poor Identity and Access Management
- Unauthorized changes to critical systems
- Use of stolen user accounts
- Abuse of privileged accounts
- Inappropriate access to systems
- Password sharing
- Use of generic accounts

Continuous Monitoring & Incident Response

- Lack of monitoring and incident response processes
- Unauthorized changes to critical systems
- Network Attacks
- Port Scanning
- Data Exfiltration
- Malicious software
- Illegal use of remote access tools







Organisations should establish and maintain processes and technologies to identify protect the confidentiality, integrity and availability of critical structured and unstructured data as it is stored and/or transmitted across an organisation's infrastructure.

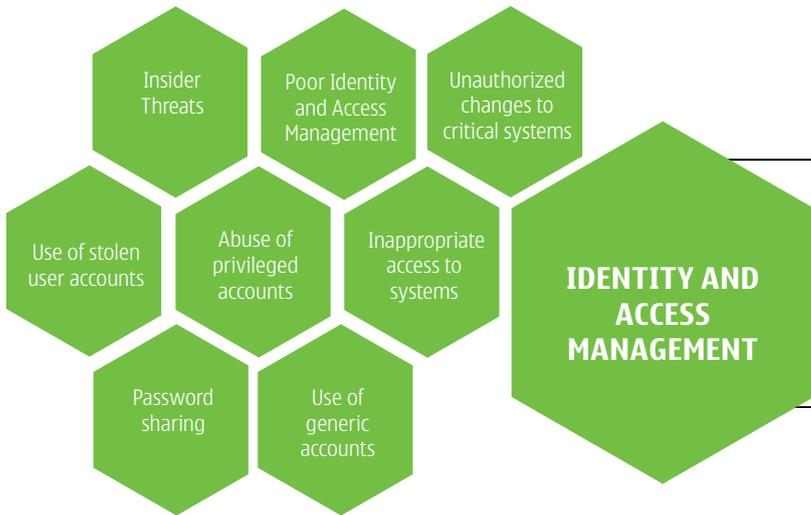
NIST 5.1.2, PCI DSS 1,4,5, ISO 27002 10.1.1 and SANS CSC 17-1, 3

Organisations should establish and maintain processes and technologies that will ensure critical operations are sustained or restored in the event of an interruption, such as a severe incident or a disaster.

NIST 3.4.1, PCI DSS 12.9.1, ISO 27002 12.3.1 and SANS CSC 8-1,4

CONTROLS

User Provisioning & Access Management | Definitions | Global Frameworks Reference



Organisations should establish processes and technologies to create and manage identities for entities that may be granted logical or physical access to the organisation's assets. Access control should be commensurate with the risk to internal infrastructure and organisational objectives.

NIST AC-1, PCI DSS 7, ISO 27002 9.1.1 and SANS 15.4

CONTINUOUS MONITORING & INCIDENT RESPONSE



Organisations should establish and maintain processes and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to infrastructure and organisational objectives.

ISO 22301 8.4.1, NIST IR 1-10, SANS 18-1,6, ISO 27002 16, PCI DSS 12.9.2

Anonymous Leaks Details for 64,000 Tanzania Telecommunications Company Employees

OpAfrica continues to make new victims, it's Tanzania's turn

Feb 15, 2016

TECHZIM

About Techzim Contact Us Send A Tip

Cyber Crime bill at work in Tanzania, 5 arrested for insulting their President

Posted 16 Sep 2014 by Batsirai Chikadaya @bdr091

Read 2 Comments



image credit: BBC

Yesterday, 5 Tanzanians were charged with insulting their President John Magufuli on social media in some interesting cases of the application of their newly enacted Cyber Crime law.

Type keyword



Ano Tele

OpAfrica

Feb 15, 2016

By Catalin Cimpanu

OpAfrica continues to make new victims, it's Tanzania's turn

Share: WhatsApp Facebook Twitter Google+

Assessed since the most recent Anonymous attack and the lack with another one, this time against Tanzania

Telecommunications Company Limited (TTCL) basic telephone service

group's most active subdivisions

64,000 TTCL employees, data leaked, the department in which



image credit: BBC

Anonymous Leaks Details for 64,000 Tanzania Telecommunications Company Employees

OpAfrica continues to make new victims, it's Tanzania's turn

5 arrested for

Concern as TTCL data reportedly stolen by hackers

TECHZIM

About Techzim Contact Us Send A Tip

Cyber Crime bill at work in Tanzania, 5 arrested for insulting their President

Posted 16 Sep 2014 by Batsirai Chikadaya @bdr091

Concern as TTCL data reportedly stolen by hackers

Share: WhatsApp Facebook Twitter Google+



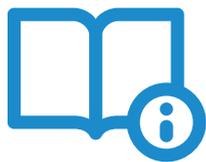
Telecommunications Company Limited (TTCL).

Media reported on Monday that the data was leaked and dumped on the web. It included details for thousands of TTCL employees, including names, email addresses, telephone numbers, departments and job titles.

By Athuman Mtulya @mtulya
amtulya@tcnationmedia.com

Dar es Salaam, Tanzania
Telecommunications Company Limited (TTCL) yesterday denied reports that its website had been attacked by a group of international hackers known as Anonymous and data stolen.

Telecommunications Company Employees



References

Telecommunications

<http://www-03.ibm.com/security/xforce/xfisi/>

<https://asokoinsight.com/news/banks-siege-atm-hackers-tanzania>

<http://www.dailynews.co.tz/index.php/home-news/45592-big-telecoms-five-fined-for-cyber-crime-inaction>

<https://www.tzcert.go.tz/>

ATM Fraud

<http://www.thecitizen.co.tz/News/national/Banks-under-siege-from-ATM-hackers-/1840392-2631726-u277o6/index.html>

E-government

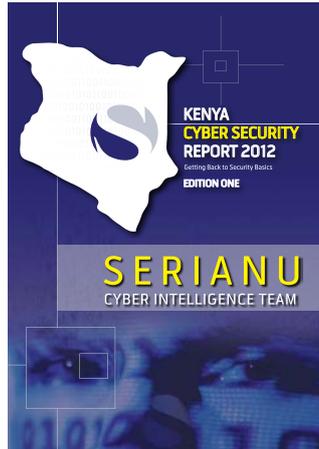
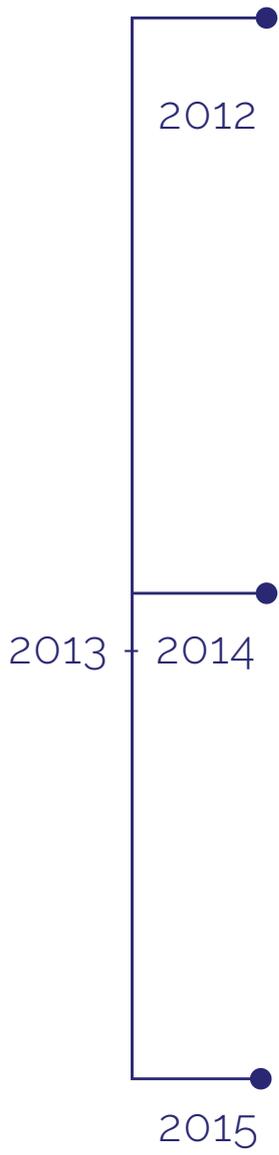
<http://www.ega.go.tz/uploads/publications/>

Mobile money

https://faculty.haas.berkeley.edu/przemekj/Mobile_Money.pdf

Cloud

<https://www.flexiant.com/news/tanzania-based-service-provider-spicenet-deploys-public-cloud-with-flexiant>



Hon
virus
Risk
COBIT
DMZ
Phishing
Outsourcing
Firewall
attack
infection
Risk
warfare
websites
router
fraud
Cyber T
child
Financial fraud
Cyber T
CSOC
Regulations
cyberspace
computers
social engineering
intrusion prevention system
organised
spam
Business disruption
Insider/disgruntled employee
defense
pornography
DMZ
port
access
Botnet
Audit
spam
Security

