SERIANU

Tanzania

Cyber Security Report 2017

Demystifying Africa's Cyber Security Poverty Line

USIU AFRICA United States International University-Africa

ISACA® Trust in, and value from, information systems Tanzania Chapter

kabolik

raha LIQUID TELECOM

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

Africa Cyber
Immersion Centre
acic
Engage | Educate | Empower

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

For more information contact:

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

Content

Editor's Note and Acknowledgement

We are extremely pleased to publish the 2nd edition of the Tanzania Cyber Security Report. This report contains content from a variety of sources and covers highly critical topics in Cyber intelligence, Cyber security trends, industry risk ranking as well as home security.

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

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

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

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

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

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

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

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

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

Brencil Kaimba
Editor-in-chief

What can our readers look forward to in this report?

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

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

Appreciation

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

We partnered with Kabolik an IT and Business consulting firm based in Tanzania whose prime focus is enabling clients to get the best value from their information and IT assets by developing holistic end-to-end solutions that release customers to focus on their core business and activities. Kabolik provided immense support through research and provision of statistics, survey responses, local intelligence on top issues and trends highlighted in the report.

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

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

The Serianu CyberThreat Intelligence Team

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

Eric Ochaka
Dadi Masesa
Barbara Munyendo
Kevin Kimani
Samuel Keige
George Kiio
Margaret Ndungu
Morris Ndungu
Mark Muema
Nabihah Rishad

USIU Team

Ms. Paula Musuva Kigen
Folarin Adefemi Isaac
Kuta Jamilla Uchi

Commentaries

Aashiq Sharif
CEO - Raha - Liquid Telecom Tanzania Ltd

Ben Roberts
Chief Technical Officer,
Liquid Telecom Group

Dr. Carina Wangwe
Head, ICT - SSRA (Social Security
Regulatory Authority)

Dr. Edward Hoseah
CEO - Hoseah & Co. Advocates,
Former DG-PCCB (Prevention and
Combating of Corruption Bureau)

ASP Joshua Mwangasa
Deputy Head of Cybercrime Unit,
TPF (Tanzania Police Force)

Eng. Peter Ulanga
CEO & Fund Manager,
Universal Communications Service Access
Fund (UCSAF)

Adv. Josephat Mkizungo
Senior State Attorney -
Attorney General's Chambers

Joseph Mathenge
Chief Operations Officer, Serianu Limited

Olabode Olaoke
PricewaterhouseCoopers

Dr. Peter Tobin
Privacy and Compliance Expert,
BDO Consulting, Mauritius

Jeff Karanja
Information Security Consultant

Building Data Partnerships

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

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

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

Design, layout and production: Tonn Kriation

Disclaimer

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

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

For more information contact:

kabolik
Kabolik Company Limited,
Plot 11, Kishapu Street, Kijitonyama,
P. O. Box 31956, Dar es Salaam, Tanzania
info@kabolik.com | www.kabolik.com
Tel: +255 623 000 850

info@serianu.com | www.serianu.com

Foreword

2017, QUITE A YEAR IN CYBERSECURITY

Robert Matafu

CEO
Kabolik, Tanzania

2017 has seen a jump in cyberattacks or cybercrimes. Ransomware, DDoS attacks, data breaches were all synonymous with 2017. From negligence by system administrators to oversight by hardware manufacturers, 2017 was a year of Cybersecurity incidents that have stretched industry professionals and this is predicted to rise in the coming years. It is predicted globally that by 2021, there will be a gap of over 3.5 million Cybersecurity professionals (zero percent unemployment for the cybersecurity industry). This means that every IT professional needs to be equipped in Cybersecurity skills.

In 2017, we witnessed defacement of public institutions' websites by some disgruntled graduates in Tanzania. These may seem like incidents to take for granted compared to mega data breaches globally, but they are not. This is just the beginning as it is an indicator of things to come as our country gets more digitized and young people get various cyber skills and lack areas to apply them. If we don't start preparing now, it is going to be a long journey fixing damages in the near future.

One of the major challenges we are facing as cybersecurity professionals is lack of collaboration. Institutions and individuals are not willing to share information on cyber attacks and the solutions implemented. We understand by now that the biggest role we need to focus on is awareness. Kabolik believes in the fact that sharing of information is one step towards solving the root cause of the problem. For example, if one institution gets hit by Wannacry ransomware, that information can help rescue the next institution or ensure the damage is managed before it is too late. At the end of the day, it boils down to being ahead of the attacker.

The culture of fearing judgement or stigmatization from the public or stakeholders needs to be managed in order to effectively deal with Cyber attacks. There's a common swahili saying that goes like this:

> "Whoever hides a disease or sickness, death will expose him"

which by then it will be too late. In this case, we need to apply the same caution in Cybersecurity, we need to understand that once we are compromised, it is no longer a secret as someone else outside your organization knows. To shift the advantage, find a way to share this information and have a response and recovery framework to restore stakeholders' trust.

We have to keep in mind that the attackers are taking their job seriously, a lot of money and valuable information is at stake here. According to Forbes.com's 60 Cybersecurity Predictions for 2018, Artificial Intelligence will be used by both attackers and defenders. Attackers will use Machine Learning to speed up the process of finding vulnerabilities in commercial products, with the end result being that attackers will use ever more new exploits without signaling that AI was involved in their creation.

On the defense side, AI will also increase the number of qualified cybersecurity professionals as it lowers the barriers of entry into the profession and allows less trained individuals to still be effective on the front lines of the cybersecurity battle

Back to Tanzania, everyone needs to understand that cyberattacks are getting more complex and there is no time to hide information when they happen to us. From an individual level all the way to the corporate level, information sharing is one of the most critical ways to get advantage over the attackers. All the the attacks we witness today are founded on the basics as we know them: confidentiality, integrity and availability (CIA) of information systems. To sustain the CIA, we need skilled and prepared people, optimized processes and technology that will be effectively utilized and dynamic enough to handle sophistication of attacks as they come.

In order to move to the next level in ensuring a cybersecure future, we have to invest in Cybersecurity.

The investment includes collaborating effectively through the different platforms such as this report, the TCRA platform and other technology groups so as to anticipate attacks; analyzing the data and reports to identify focus points and priority areas that have to be addressed given the limited resources; Developing strategies, tools, skills and expertise in addressing the identified challenges; and lastly creating cyber resilience across the nation.

As we finish 2017 and going into 2018 and beyond, we need and have to invest more resources into cybersecurity. Focus must be on skills, abilities, and knowledge. The rest will follow. Its high time cybersecurity becomes one of the core strategy of any organization or nation.

Executive Summary

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

Our research is broken down into 8 key areas:

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

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

What is the Cyber security poverty line?

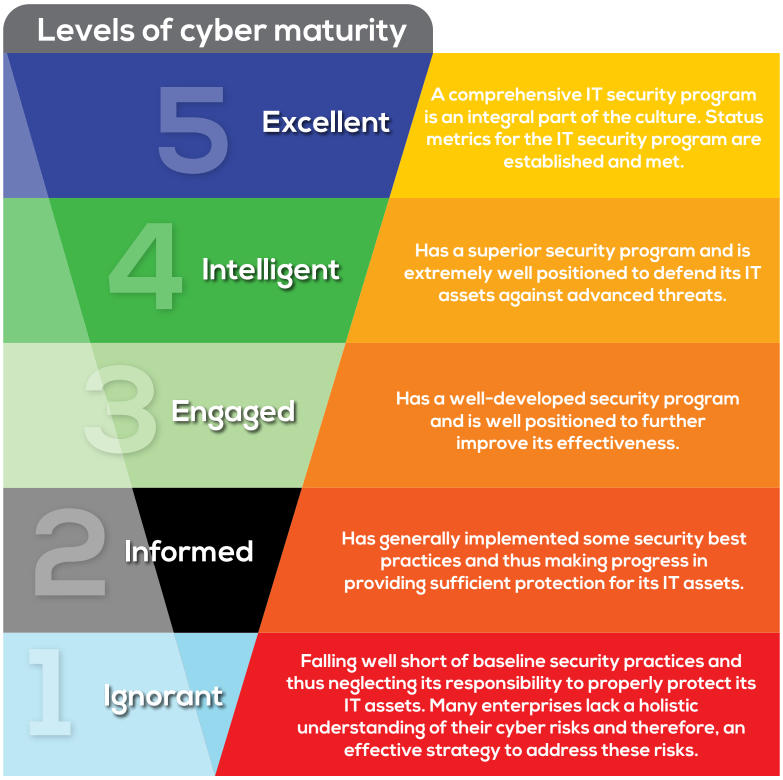
Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

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

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

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

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



Levels of cyber maturity

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

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

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

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

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

What is the impact of operating below the poverty line?

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

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

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

What does the future hold for this problem?

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

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

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

What can our readers look forward to in this report?

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

Key Highlights

Breakdown of key statistics for different countries:

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

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

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

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

Cost of cyber-attacks **$99.5M** annually

FAKE NEWS

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

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

Banking Sector is still the most targeted industry in Tanzania

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

94.4% Cyber security incidents either go unreported or unsolved

Aashiq Shariff

CEO

raha - Liquid Telecom Ltd

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

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

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

Yes.

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

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

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

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

Platforms that can be confirmed – Government sites,

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

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

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

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

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

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

Some ended up paying in order to get the data.

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

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

Awareness, appropriate firewall that can mitigate such attacks.

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

No.

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

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

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

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

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

Conduct the awareness and ready with solutions.

Ready solutions depending on the organisations/entity.

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

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

Top Trends

Fake News: Vulnerability of truth

In 2015/16 more than 7,000 cases of fake accounts and false information were reported according to Tanzania Communications Regulatory Authority.

From January to June 2017, 3,340 cases were reported to the police stations. The real impact of the growing interest in fake news however has been the realization that the public might not be well-equipped to separate true information from false information.

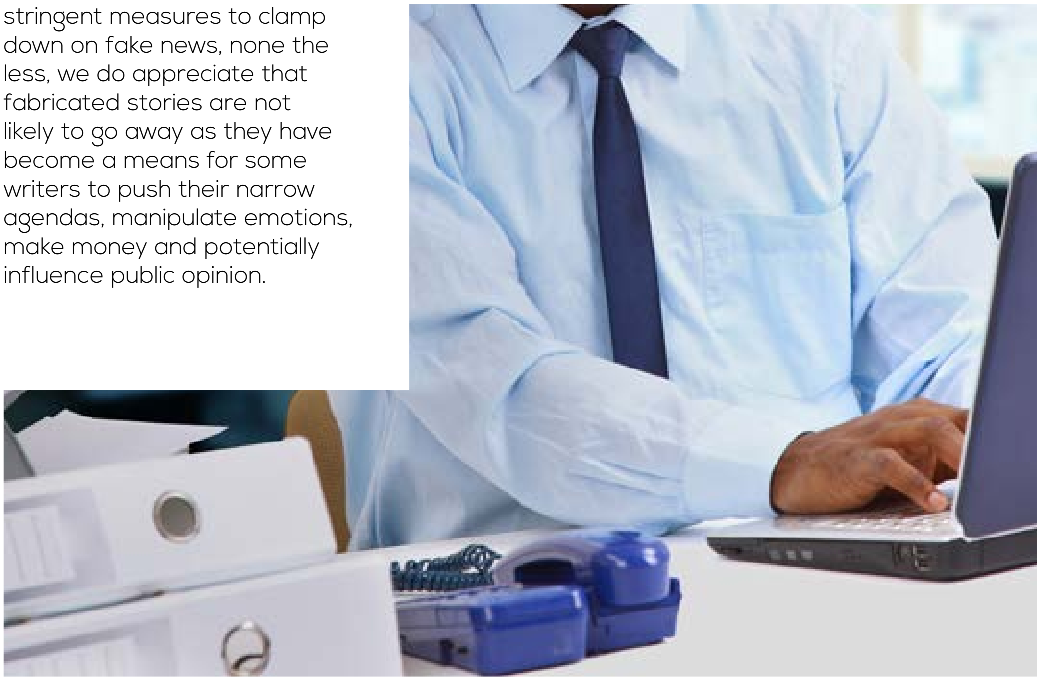
It is paramount that governments and social media platform owners lay down stringent measures to clamp down on fake news, none the less, we do appreciate that fabricated stories are not likely to go away as they have become a means for some writers to push their narrow agendas, manipulate emotions, make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

Insider Threat: The enemy within

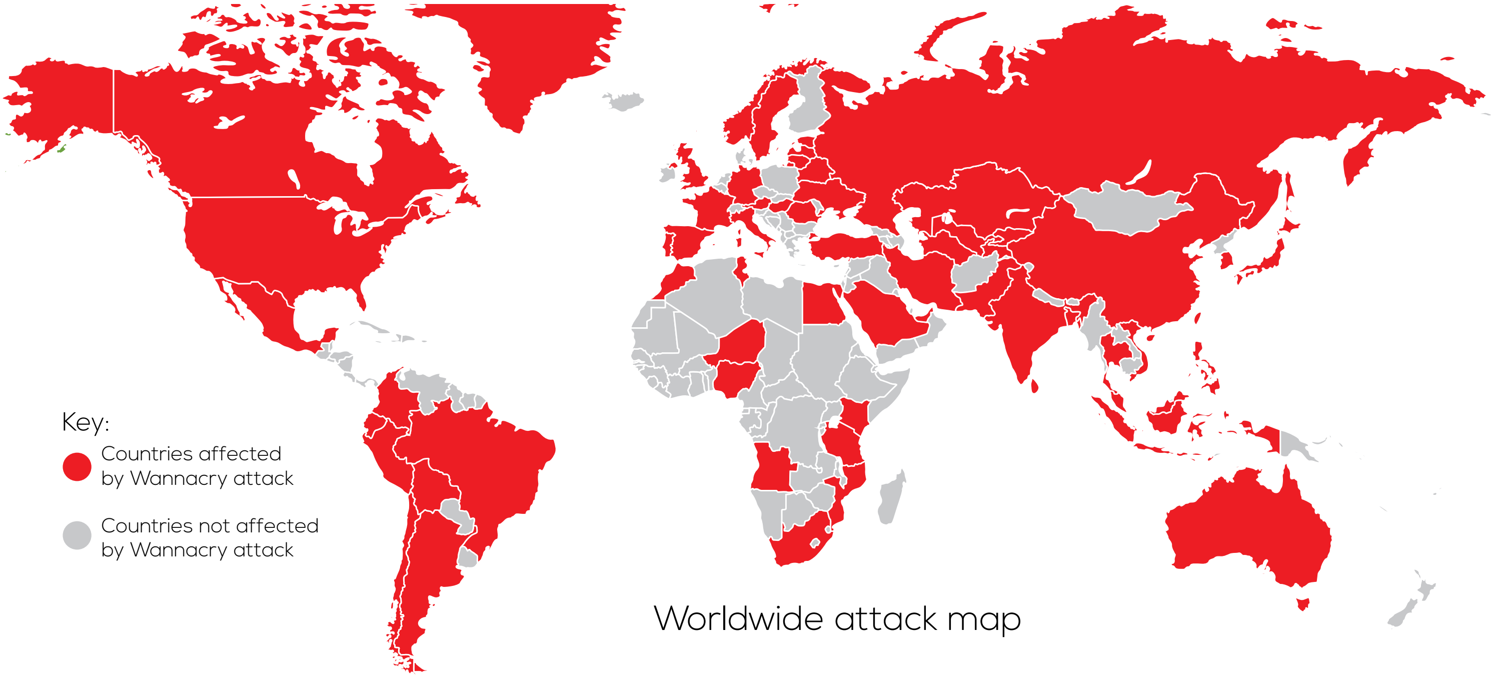
Insider threats still top our list when it comes to high risks. From the numerous cases reported this year, it's clear that the group most implicated is administrators and other privileged users, who are in the best position to carry out a malicious breach, and whose mistakes or negligence could have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

Top insider threats:

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



Ransomware: I don't WannaCry


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

Worldwide attack map

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

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

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

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

The cost of Cybercrime grew by approximately 17% but the skill gap is widening. No one knows what they're doing, majority of IT and security staff are downloading templates from the internet and applying these in their organisations. From our analysis, a key contributor to this is that organisations tend to look for people with traditional technology credentials – IT, Computer Science. But when you look at the matter, we need Technology analysts, Cyber Risk Engineers, data analysts, Risk experts most of which do not necessarily warrant a technology course. Majority of organisations encourage their IT teams to take up courses that don't necessarily add value to the security of the organisations.

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

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

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

Mobile and Internet Related Services. Battery is low is no longer the only warning

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

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

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

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

Ben Roberts

Chief Technical Officer
Liquid Telecom Group

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

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

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

Yes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

I would refute that statement.

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

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

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

Network Architecture: Defense In-depth

The success of most attacks in 2017 were in one way or another linked to one critical issue: Weak Security Architecture. Successful ransomware attacks were mainly due to missing patches. For example

Wannacry exploited a vulnerability by not applying a patch) and for most cases, inadequate privilege account monitoring and third party risk management. Yet these organisations have invested heavily in the latest Antivirus programs or SIEM solutions.

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

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

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

Phishing: The weakest Link

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

Cyber Pyramid Schemes: Easy come, Easy go

In an economy where it's so difficult to earn a living, many Tanzanians try out pyramid schemes with the hope of making huge profit. 2017 saw the Bank of Tanzania and capital market and Securities Authority issue warning on ponzi scheme.

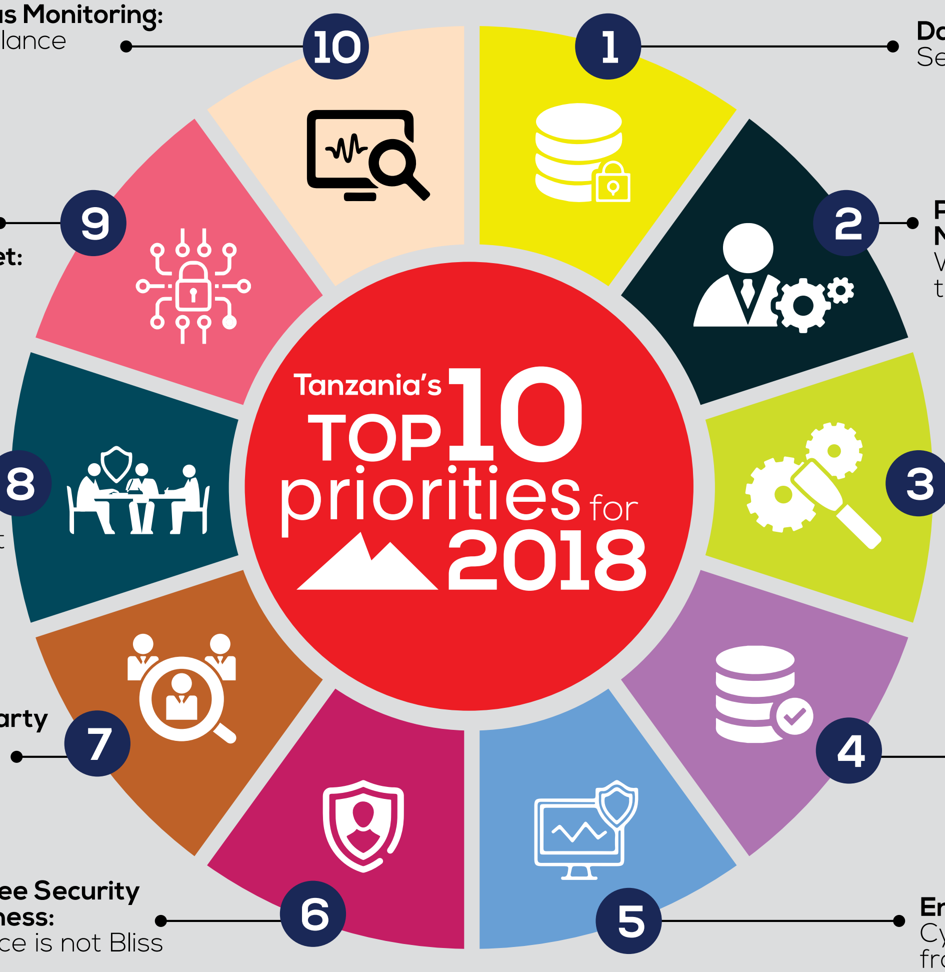
We noted that these schemes rely on a constant flow of new investments to continue to provide returns to older investors. When this flow runs out, the scheme falls apart. In recent times, we have seen these schemes evolve to now include crypto currencies.

System Integrity: Eroding Public Trust

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

Tanzania's TOP 10 priorities for 2018

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



1. **Database Security:** Secure the vault

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

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

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

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

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

7. **Vendor/Third Party Security:** Bring Your Own Vulnerability

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

9. **Security Architecture/ Engineer skill set:** Widen your employee gaze

10. **Continuous Monitoring:** Askari Vigilance

1 **Database Security:** Secure the vault

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10 **Continuous Monitoring:** Askari Vigilance

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

Dr. Carina Wangwe

Head, ICT

Social Security Regulatory Authority, Dar es Salaam

Of the three triangle components in cybersecurity, which one do you think has the biggest impact or weight in Tanzania cybersecurity scene?

I believe the component with the biggest impact is people. End-users of technology need to continually be aware of the risks and how they impact on them. IT professionals need to use their talents professionally, and not be lazy when it comes to implementing the necessary security mechanisms in their roles. With the increasing incidences of cybercrime, every person in an organization that is using IT systems cannot afford to be lax keeping aware of the risks and in implementing the necessary controls.

Which aspect of the cyber triangle can be termed as the weakest link in Tanzania?

In Tanzania, there is still room for improvement on all three components: people, process and technology.
With people – the uptake of security certifications is still low. I do not see sufficient interest from young university graduates in enhancing their technical skills be sitting for certifications such as CSX, CISSP, CISA and CISM. Within organizations, many processes are still carried out with a mentality of the manual processes of old, and sufficient controls to deal with cyber risk are lacking. With regards to technology, again uptake of any new technologies should be done with a consciousness of the attendant risks, and an articulation of what controls are being put in place to manage these risks.

Do you think the private sector is investing enough in the cybersecurity triangle: People, Process and Technology?

One area where private sector could invest more is on people. Training of employees is key to effective Cybersecurity.

What has to be done in-order to ensure balance in the cybersecurity triangle in Tanzania?

More awareness, more training and encouraging discussions around the effective management of cyber risks.
This can be done by not just highlighting horror stories about cybercrime – but also encouraging the sharing of best practices within the country of effective cybersecurity management.

We have seen a substantial number of cyber crimes are conducted via mobile communication means; In your opinion what drives criminals to commit cybercrime or cyber offenses?

I believe that easy gains with very little investment and perceived low risk, are what drive cybercriminals. In addition, the ubiquity of mobile phones in Tanzania means that the population of potential targets is very high.

What initiatives does the government have in place to support the private sector in combating cybersecurity issues in the communication arena?

The government has put in place several pieces of legislation that address cybersecurity issues including the CyberCrime Act and the Electronic Transactions Act. Section 18 of the Electronic Transactions Act lays out the admissibility of electronic evidence, which is key in prosecuting cyber crimes.

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

My opinion is the best approach to cybercrime in Tanzania, is to focus on people, that is, both end users of the technology and on professionals who should be developing, and maintaining secure systems. People need to be aware of the risks, and also the consequences of Cybercrime.

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

The priority for the African Continent should be enhancing professional skills of all professionals, IT or otherwise, so that they can design and deliver secure systems, and keep these systems secure. In addition – deliberate efforts need to be taken to align skills with ethics, such that professionals act with integrity and do not misuse the cyber skills that they may have.

What is your prediction of the future in terms of cybersecurity?

I believe that it is going to get worse before it gets better. The rise in cybercrime I believe is set to continue, and thus it is imperative for all current security professionals to keep pushing for more awareness and more risk management.

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

Top Cyber Security Issues of 2017 are rise in both sophisticated and unsophisticated Cybercrime.. Sophisticated Cybercrime would be incidents such as the ransomware attacks that rocked the cyber landscape in 2017. These have had both a positive and negative impact. Positive in the sense that, in my personal opinion, they have resulted in an unprecedented level of awareness amongst Boards and CEOs who hitherto did not have much interest in Cyber Issues. Negative Impact of course on the affected parties, and also in the rising cost of cyber protection.

Unsophisticated Cybercrime is that kind perpetuated through mobile phones or social media for purposes of defrauding individuals. There have been increased incidents of such crime in the Tanzanian media.

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

Fake news is a big a problem in Africa as it is for the rest to the world. Africa is just beginning to make progress with regards to local or localized content on the web and social media, and this progress is going to be seriously threatened, if African content consumers now need to worry about veracity of the content.

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

The Government and the Content owners. End users should be able to trust in news generated, or published through government sites and reputable content owners such as media companies.

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

Definitely – if its is proven fake news – it should be removed.

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

Fake news, I believe relates to ethical considerations and general laxity when using anonymous media platforms. This can tackled by awareness on the penalties that are in laws relating to CyberCrime.

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

African Citizenry is ready to consume these systems; and are consuming the systems especially those offered through familiar technologies like USSD based services. The worry of privacy, security and fraud remains but I do not believe that it has an impact on uptake especially if the service is cheap and quick, thus the advantages outweighing the perceived risks.

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

One risk is the consistency of service. There are some Government agencies where the e-services offered are backed by a robust back office with all the necessary infrastructure to provide a seamless service, while in other cases – the service level is inconsistent due to inadequate backend processes and or infrastructure.

Another risk is the possibility of persistent exclusion of certain segments of the population who happen to be disadvantaged because of their location, income levels or literacy level.

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

No, we were not impacted.

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

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

There is a multitude of resources on online, that even with out limited resources, we can utilize more effectively. Simple actions like ensuring patches are done as required go a long way in offering protection. We need to subscribe to and follow technological news and updates, and share the limited resources and knowledge. This way we work within our means and still achieve some level of protection.

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

For my personal experience – No.

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

Pushing for IT and Cyber Issues to form part of national and corporate agendas. Collaborating with professional and research organisations to put tangible figures to the losses arising from cybersecurity issues. Publishing such statistics in forums that have their audiences as CEOs and Policy makers

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

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

Innovation can be fostered by supporting the existing hubs, and by governments supporting the products from these hubs. Both at a policy level, with stringent controls on Intellectual Property, but also paying a fair fee for software products and services. A locally developed solution or service, should be seen as being as valuable as those sourced abroad, and especially since the local solution is likely to be better customized.

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

Pay fair value.

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

- Raise Awareness
- Cost, document and publish impact
- Encourage secure practices for all segments of the population

Cyber Intelligence Statistics, Analysis, & Trends

FOR THE PURPOSES OF THIS REPORT, WE INSPECTED NETWORK TRAFFIC INSIDE A REPRESENTATIVE OF TANZANIAN ORGANISATIONS, REVIEWED CONTENTS OF ONLINE NETWORK MONITORING SITES SUCH AS PROJECT HONEYNET 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 THE ORGANISATION'S SERVERS. IN AN EFFORT TO ENRICH THE DATA WE COLLECTED, WE PARTNERED WITH THE HONEYNET PROJECT AND OTHER GLOBAL CYBER INTELLIGENCE PARTNERS TO RECEIVE REGULAR FEEDS ON MALICIOUS ACTIVITY WITHIN THE CONTINENT.

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

Project Honeypot Intelligence Analysis

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

Dr. Edward Hoseah

CEO

Hoseah & Co. Advocates

Former DG-PCCB (Prevention and Combating of Corruption Bureau)

> “Looking at the cyber security in Tanzania; technology, people and processes are integral, if we further magnify the three; people are the most key players in cyber security. Come to think of best security measure (amounting to processes) and the best technology in the world combined, without skilled, developed and committed people to thwart cyber security challenges we may succumb to a cyber offense tragedies. Just like San Tzu once said, **“Victory usually goes to the army that has better trained soldiers”** summing it up in my point of view; People, Processes and Technology are inseparable but having the last two without better trained set of personnel both in private and public sector, the investment in the last two is worthless hence making people the most vital component of the triad (People, Processes, and Technology).
>
> As said above, people being the vital component of the triad, they pose a great amount of threat to the processes, and technologies that are meant to support businesses and organizational endeavors should they (People) be compromised. Furthermore, from the triad the later two can be easily patched up and fixed but people are hard to contain due to honesty variation, skillset variation and industrial response variation. It is therefore very important to invest more in the people as much as it is important to do on the remaining two.
>
> Technology is existent to make the way we do things more efficient, contrary to the initial purpose; people modify processes through the use of technology for personal gains. These actions ultimately translate into cyber offenses (cybercrimes). Cybercriminals are on the rise with an expectation to secure finances illegally (major motive to commit cybercrimes), to gain fame from professional peers, and the need for revenge among many others.
>
> Given that there are many variants of cybercrime and that they are on the rise day in day out, there is a great need to increase efforts in the fight against cyber crime that include: training people, having standardized best practices, and acquiring best technologies that target to solve the challenges at hand efficiently.
>
> With the rise of cybercrimes, there is a great need to thwart these crimes efficiently through the proper use of the triad (entails having honest and skilled people on deck, best technology and well-defined and understood processes). Success in fighting conventional cybercrimes will dictate how can one fight the contemporary cyber crimes now that the internet of things is booming.”

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

The key security issues are financial crimes. These include cheque, card fraud; and identity theft/fraud to mention just a few. This is based on the clients experiences I encountered.

Pensioners for example have been a victim of such fraud. Especially those that travel from up-country to process their pension in Dar es Salaam. Some of them end up finding someone has already cashed their cheques using either forged or stolen identities and credentials. The identities of the persons who cashed the cheques are normally fictitious.

The person's details can be retrieved online using social media or other sources such as the phase 1 ID cards that had all the details of the person on easy to read QR code.

We need to invest in people.

We need to give them knowledge, give them awareness, to give them the understanding of what is happening because of Cybercrime. It is a border-less crime – it can be committed from anywhere as long as someone has the knowledge.

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

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

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

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

On one hand, the constitution of Tanzania provides freedom of speech and freedom of expression. These are fundamental freedoms in any democratic state. In order to control fake news, one has to strike a balance between the fundamental freedoms (freedom of speech, freedom of expression,…) that the constitution guarantees. However, these freedoms have limitations; that is they are accommodated within the democratic principles (freedom not to offend others, freedom not to injury another persons…) therefore in that context, regulators may play their roles by identifying those that have infringed the permissible limits of those freedoms. There is always a delicate balance. It is the court that determines the permissible limits. There is need to raise awareness on these fundamental freedoms and democratic principles.

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

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

E-services are fundamental facilities in our modern age, without which bureaucratic red-tape will continue to hinder smooth flow of business between private and public sector. In the area of procurement, according to the recent data, is where big corruption happens; so in order to limit human contact, it is a good idea to use e-services. However in every ideal situation, there are risks; one of the risks is fraud, Cyber fraud and not forgetting counterfeits.

Criminal gangs in the world use counterfeit goods to finance their operations by selling counterfeit goods online.

In Tanzania we need a lot of education, especially the private sector to disseminate preventive measures, and techniques in order to identify these threats in light of the unprecedented use of mobile phones by Tanzanians for different activities including purchasing goods.

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

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

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

I have not been impacted directly. However we should invest in public awareness through the use of different media to create awareness.

Classification of information is also crucial so that the needed security measures can be utilized based on the importance of the information.

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

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

Big NO!

They have to accept to receive specialized training both private and public organizations. They have to open doors for this knowledge. I recommend most of the public institutions especially law enforcement should cooperate with private sector experts to exchange knowledge and experience on impact of cybercafe, because criminals invent new techniques everyday. Its difficult to fight the battle where you use the same old wine in new bottle.

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

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

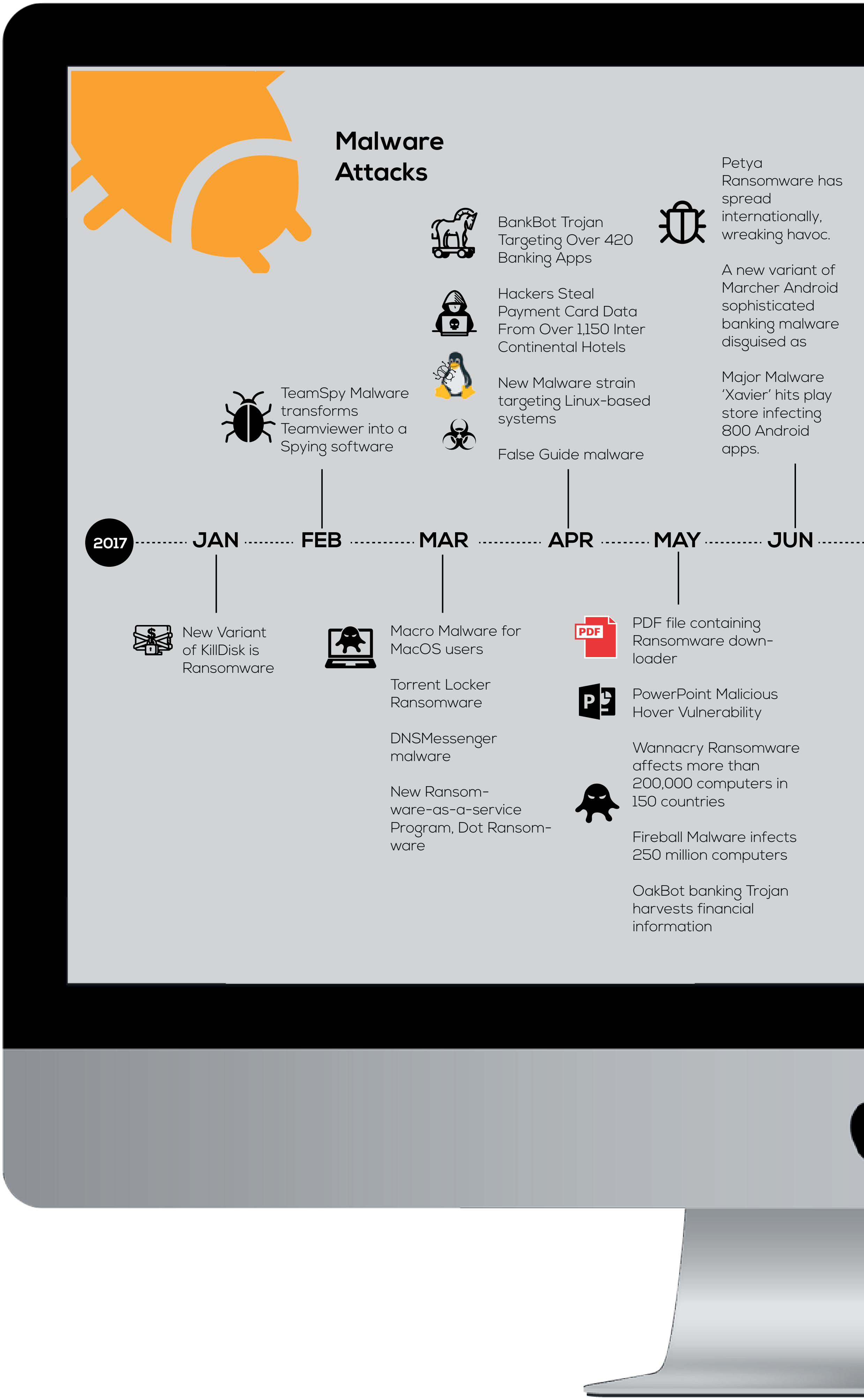
What role can the private sector and consumers of imported cyber security products play to ensure we can encourage local players to start developing African grown cyber security products or solutions or even services?

At the continental level, the African Union has a specific organ for scientific innovation and scientific data should fund this initiative in order to come up with innovative solutions. Its high time for Africa to spend more resources on scientific innovation and technology especially data. In Tanzania we have a number of institutions and the Commission for Science and Technology. They also need to invest in scientific research and scientific data gathering on the impact of Cybercrime in Tanzania. It is not an easy task but it is high time we invest on research on the current trends that are happening on the Cyber world.

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

Cybercrime posses a great threat not only to the security and defense but also in social and economic spheres. Its an area we need to give priority because the world has been shrunk into a small minute that criminals can take advantage. As we move to science and technology country, we should also take cognizance of the impact of Cybercrime.

Malware Attacks



2017

JAN

New Variant of KillDisk is Ransomware

FEB

TeamSpy Malware transforms Teamviewer into a Spying software

MAR

Macro Malware for MacOS users

Torrent Locker Ransomware

DNSMessenger malware

New Ransomware-as-a-service Program, Dot Ransomware

APR

BankBot Trojan Targeting Over 420 Banking Apps

Hackers Steal Payment Card Data From Over 1,150 Inter Continental Hotels

New Malware strain targeting Linux-based systems

False Guide malware

MAY

PDF file containing Ransomware downloader

PowerPoint Malicious Hover Vulnerability

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

Fireball Malware infects 250 million computers

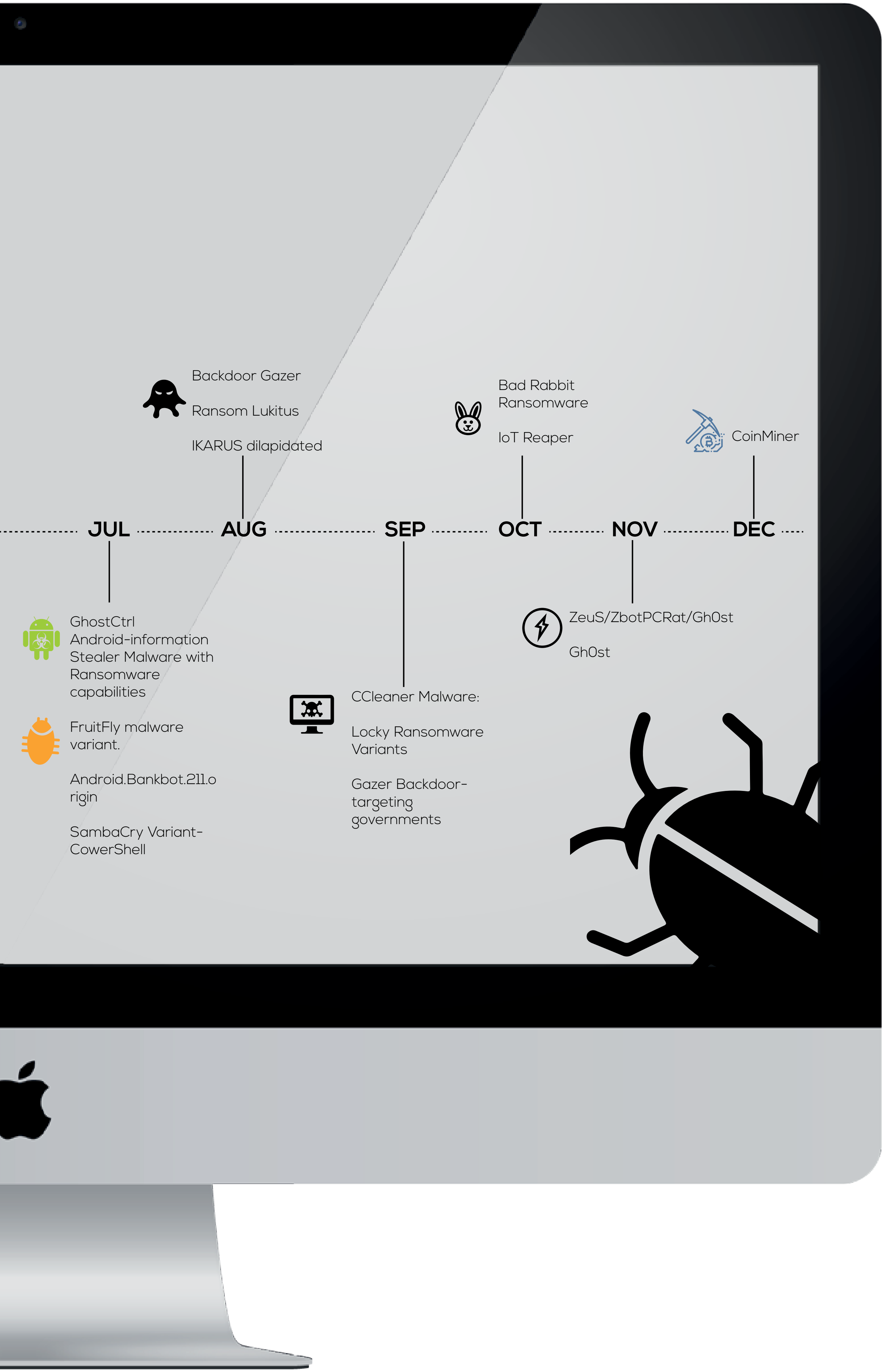
OakBot banking Trojan harvests financial information

JUN

Petya Ransomware has spread internationally, wreaking havoc.

A new variant of Marcher Android sophisticated banking malware disguised as

Major Malware 'Xavier' hits play store infecting 800 Android apps.



JUL

GhostCtrl Android-information Stealer Malware with Ransomware capabilities

FruitFly malware variant.

Android.Bankbot.211.origin

SambaCry Variant-CowerShell

AUG

Backdoor Gazer

Ransom Lukitus

IKARUS dilapidated

SEP

CCleaner Malware:

Locky Ransomware Variants

Gazer Backdoor-targeting governments

OCT

Bad Rabbit Ransomware

IoT Reaper

NOV

ZeuS/ZbotPCRat/Gh0st

Gh0st

DEC

CoinMiner

ASP. Joshua Mwangasa

OC Cyber Crime Unit, TPF (Tanzania Police Force)

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

Irresponsible sharing of personal information on social which has led to successful criminal activities.

Password sharing which has led to misuse of other people's information or profiles.

Use of personal devices for official matters which has exposed official matters to unauthorized people.

Lack of confidentiality in the work place which has led to breach of trust between employer and employees.

Leakage of top secret documents or information with unauthorized people or public which has caused mistrust between the related parties as a result of the information leaked.

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

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

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

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

Yes, the responsibility rests with the owner of the content.

Yes, the regulator should force influential platforms like Google and Facebook to remove fake news and other extreme forms of content from their platforms

With collaboration among stake holders in the government and private sector, campaigns be initiated to drive awareness on the detection of fake news in the country including online platforms, television and radio shows and regular tests to check the effectiveness of the awareness campaigns.

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

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

Yes, they are ready. The most important step is to create awareness among the citizens on how they can securely use these systems and on how to protect themselves and their devices.

Fraud of by some opportunists who take advantage of citizens with little knowledge on how to use the government e-driven services making it seem like the government has given them the mandate to render the service.

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

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

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

Yes, we experience such an attack. Through collaboration with other government institutions and also consulting experts, we were able to effectively respond to these cases

We can limit the impact of ransomware by ensuring there is frequent offline backup that is tested appropriately in case of any attack, we're able to get back online soonest possible.

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

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

This depends on the nature of the business and the level of automation in organisations.

We should create awareness to the top management to understand the importance of cyber security

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

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

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

To invest much on cyber security in terms of skills and equipment by first understanding our landscape considering what is happening through research.

The private sector and consumers of imported cyber security products can encourage local players by starting to buy the solutions after making sure that they are effective and they are addressing the cybersecurity problems. They can also encourage the local developers by clearly communicating the quality of solutions they are looking for.

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

Develop Cybersecurity skills through creation of awareness and setting up research and security operations centers with modern equipment.

Creation of awareness to the end user.

One of our key theme is "Understanding the cybersecurity triangle: People, Process, and Technology." Which do you think has the biggest impact or weight in Tanzania cybersecurity scene?

Technology.

Which aspect of the cyber triangle can be termed as the weakest link in Tanzania?

People.

Do you think the private sector is investing enough in the cybersecurity triangle: People, Process and Technology?

No as we continue to see the existing gap in people's capability, processes and technology.

What has to be done in-order to ensure balance in the cybersecurity triangle in Tanzania?

To put clear policy and create awareness.

In your opinion what drives criminals to commit cybercrime or cyber offenses?

Opportunities.

What initiatives does the government have in place to support the private sector in combating cybersecurity issues?

Ongoing of drafting National Cybersecuty strategy.

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

Creation of awareness on the different kinds of technology available to combat cybercrime.

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

To understand different technologies available and how they can be effectively customized and used to combat the various cybersecurity issues

What is your prediction of the future in terms of cybersecurity?

The future is looking promising as more people are talking about it and there are more opportunities to learn and implement what we are learning. There is a lot of room for growth and that is a great thing.

Threat Intelligence

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

We broke down the findings into the following sections:

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

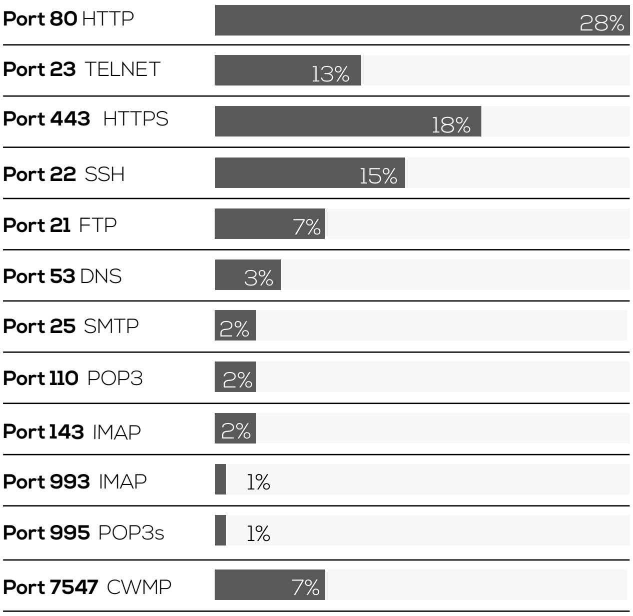
Open Ports

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

65,535 TCP ports

65,535 UDP ports

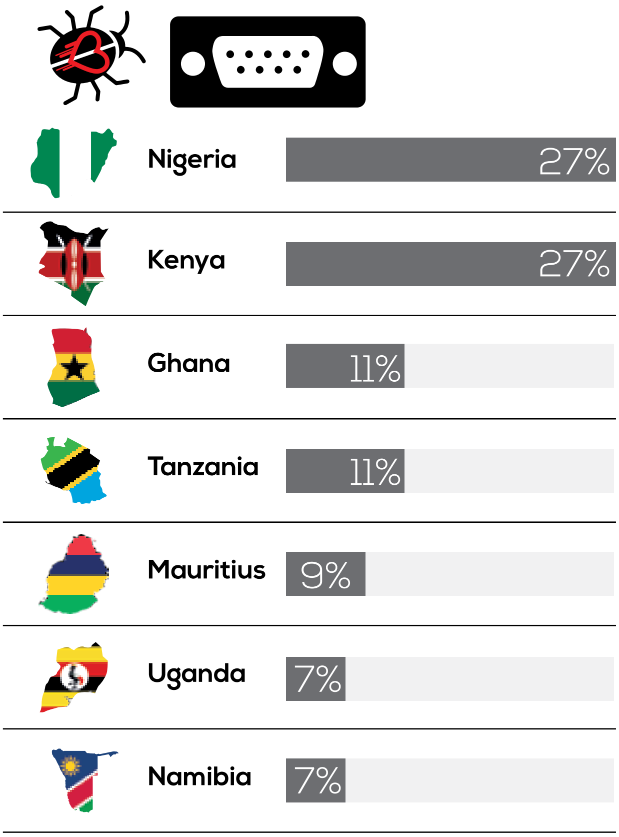
Top Open Ports



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

Heartbleed Vulnerability

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



Top Content Management System Vulnerabilities

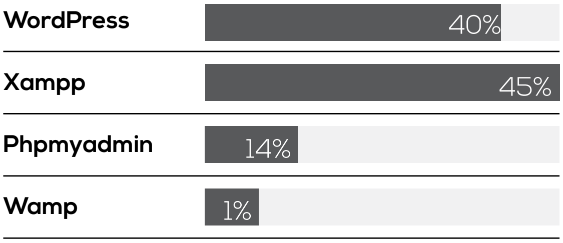
Many of the vulnerabilities of web content management systems are not specific to web content management but inherent to web technologies, server environments, and protocols as a whole.

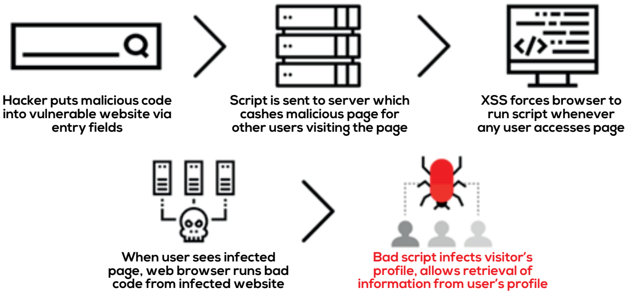
1. Privilege escalation exploits

2. Social engineering attacks

3. Cross-site scripting (XSS), combines weaknesses in the client side execution environment creatively with backend flaws of eg. lack of verification of parameters and content.

Top Content Management System Vulnerabilities




Hacker puts malicious code into vulnerable website via entry fields
Script is sent to server which cashes malicious page for other users visiting the page
XSS forces browser to run script whenever any user accesses page
When user sees infected page, web browser runs bad code from infected website
Bad script infects visitor's profile, allows retrieval of information from user's profile

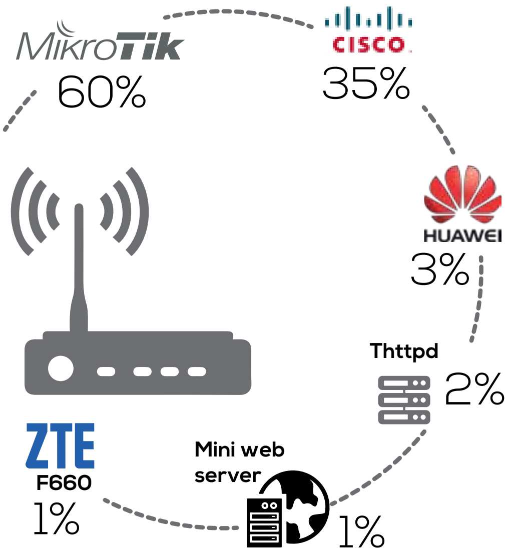
Top Web Servers with Vulnerabilities

Top Web Servers with Vulnerabilities

	Vulnerable	Upto Date
Apache http server	36%	3%
Microsoft IIS	1%	64%
Nginx	22%	1%
Lighttpd	41%	31%

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

Top Routers



In 2017, we witnessed a number of bugs and hacks such as MikroTik routers hacked to infect Windows PCs and MikroTik Routers defaced due to default passwords. Cisco and Huawei also recorded a number of security issues. Its paramount that users, regardless of the router, keep up to date with security patches.

Top Spam Servers

Spam Servers IPs	
196.46.108.187	7%
41.221.61.186	1%
196.46.108.248	14%
196.46.108.237	16%
196.46.109.97	14%
196.43.64.167	16%
196.46.108.184	21%
196.46.109.18	11%

*Spam - Electronic junk mail

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

Top Dictionary Attackers

Dictionary Attacker IPs	
196.46.108.187	7%
41.221.61.186	1%
196.46.108.248	14%
196.46.108.237	16%
196.46.109.97	14%
196.43.64.167	16%
196.46.108.184	21%
196.46.109.18	11%

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

Eng. Peter Ulanga

CEO & Fund Manager

Universal Communications Service Access Fund (UCSAF)

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

2017 brings out a very interesting complexity of technologies making someone vulnerable. The more complex the technology is, the more difficult to cope with the development in technology and to secure it. On an average week, each and every device one owns has an update and these updates have many things and one has a fuzzy knowledge of them and you have to make a decision should I update or not. Most of us take the default position of just updating. In my humble opinion, with increasing complexity, there willl be a time where our very own user, it will be difficult to confirm that they have an informed consent in most of the things they do.

How? On a security point of view, your device gives you your digital life or existence with your personal information. Installing a software in your device is like inviting a guest into your house. If there is any vulnerabilities in any of the softwares, somebody can take advantage of that. I am not even talking about apps that are spyware or malware; I am talking about legit apps but due to the complexity in development of technology, these apps can be compromised by someone who knows how they work. A good ancient example is the misuse of Microsoft Word Macros.

The philosophy behind updates includes adding features and that is how the thing breaks. If you update too many times there will be a day you will forget and something will break. Taking for instance Linux, one is required to disable and remove everything that doesnt belong to the machine they are using. This is to ensure security since the hanging, unused handles can be the source of vulnerability to be compromised by hackers. But people rarely do this anymore due to complexity.

Complexity is affecting security, and because we do not even talk about it; we do not demand it from the developers. For the normal user it is very complex. And we are victims of complexity already. Complexity is our biggest enemy in 2017 and if you follow the comments of hacking victims they did not even know they could be hacked since the system become too complex. At times until the hacker informs them that they were hacked.

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

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

To begin with, fake news did not start on the internet. Let us get the context right, fake news is a big problem now but it did not start today. According to history, fake news affected us from the start of the first printing press to present. The internet brought two aspects. It brought tools to check the authencity and unprecedented opportunity to push the news to the ends of the world.

The internet gives a person the opportunity to publish whatever they want; be it true or fake or a variation of the two. On the other hand, information posted on different media can have its authencity (facts) checked throught the internet. The dual nature of the internet, it gives you the opportunity if you have the time to check the facts and it also an opporutnity to feed people with fake news.

Before the internet, we had "media houses" that are by structure bustiones of information (they control what they tell people). Media houses had open editorial policy to inform people. They also had closed editorial policies for a certain purpose and people consumed what was given to them. With the internet its completely different. One puts up information on their social account and friends go through a very elaborate and exquiste voting process, they read thorugh the post; if they like it, they forward (otherwise they reject the post) ultimately it goes viral.

The underlying thing is these people vote on the quality, authencity and emotional aspect of the post, thus they become their own editorial policies. We have democratized editorial policies by being the ones who choose what we send to our friends. People still work on the traditional sense. They do not do fact checking on fake news and if they do then they do not trust their own intuition on fact checking.

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

Thinking traditionally, this will suffice. This is because the information is now on an individual level.

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

The solution is training people on what they need to know about technological development. We live in an informational society with a highly uninformed society.

The use of the acronym people, process and technology is very nice but at what point do you separate them? We live in a world of emerged reality where these can be in one person or device.

We have the knowledge worker and knowledge economy in 2017. Processes as we know them are out of the roof.

Right now we have VUCA – Volatility; Uncertainiity; Complexity; Ambiguity.

Lets leverage AI to atleast help in solving and addressing the challenges in complexity.

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

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

This is the mistake that we in the technology sector make. We want to think on the behalf of other people and we patronize them in a very bad way. This is when we are faced with a challenge and take the end user as not ready. By doing so we are abdicating our duty. Our duty is to make it simple. We remove the technology from the equation and we look at the service delivery.

If we really want to bridge the ICT literacy gap, we should look at ourselves. What have we done to make ICT simple? If cars were that complicated we would have very few drivers.

Ultimately we all lose since in the knowledge economy everyone who joins brings in new knowledge.

How do we ensure security of these services?

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

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

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

No.

We need homegrown techinical experts who will take a look at this new and fast evolving landscape and formulate ways to take advantage of the development and at the same time use the information acquired by our experts and use the information acquired by our experts to protect all of the society.

Due to the lack of informed consent, we need experts that will look into this and advice people.

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

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

That is not the right question. It looks more or less a sales pitch. For research lets put money aside. The IT officers always complain of lacking enough funding but in my opinion they are not doing enough.

There are enough free tools for someone to use. If one can develop their own security measures that are not standardized, they are more secure since the tools are not known.

There is no correlation between the amount of money used to fight cybercrime with the outcome.

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

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

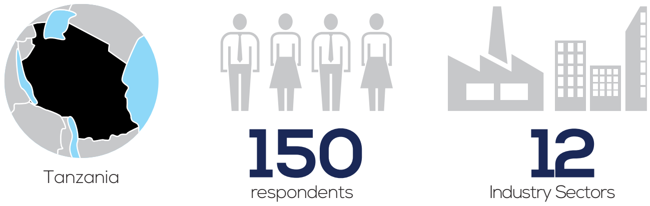
What role can the private sector and consumers of imported cyber security products play to ensure we can encourage local players to start developing African grown cyber security products or solutions or even services?

You are putting the cart before the horse. Let us focus on training the experts. They should be very versatile in using the tools and testing them. This can happen in universities that are doing cutting edge research in cybersecurity matters otherwise we are wasting time. In the private sector we have vendors and not software companies. E-Governement has programmers, but there is lack of a sharing and collaboration ecosystem thus are crippled.

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

Training. We need passionate experts in the field.

2017 Tanzania Cyber Security Survey



THE GOAL OF THE 2017 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 ORGANISATIONS AND THE MOST PROMINENT THREATS THAT THEY FACE.

About the Survey

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

Academic

Banking

Financial Services

Government

Healthcare Services

Insurance

Legal Advisory

Professional Services

Telecommunications

Others

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

Summary of Findings

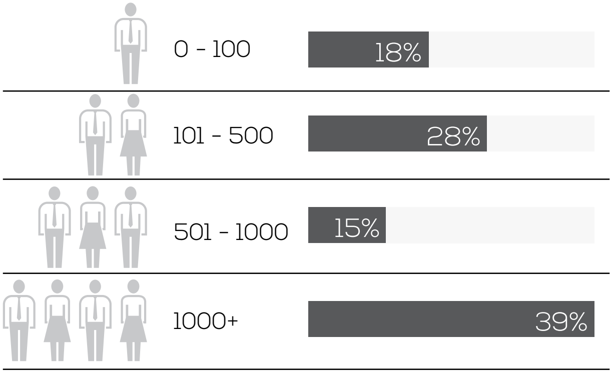
According to the survey findings, 99.4% of respondents have a general understanding of what Cybercrime is. With the many advances in information technology and the transition of social and economic interactions from the physical world to Cyberspace, it is expected that majority of individuals have a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

1. Nature Of The Survey Group

54% of the respondents of this research worked for companies with 500 or more employees, and worked within the government and banking sectors. The rest of the respondents were scattered across various sectors of the economy.

How many employees are you in your organisation?

54% of the respondents are employees of organisations with 500+ employees. These were mostly from the Banking and Government sectors.



2. Cloud and IoT

Respondents were asked about Cloud Services and Internet of Things Tech (Big Data Analytics) and whether or not they utilize these services in their organizations. Of the organizations surveyed, 32.9%, utilize these services. This is an increase in the adoption of cloud and IoT usage within the country with users such as Vodacom investing in Narrowband and other customized Internet of Things (IoT) orMachine-to-Machine (M2M) solutions and cloud computing services.

The Mirai botnet exploited poorly secured IoT devices to perform the largest ever distributed denial-of-service attack.

However, a large percentage of the respondents who utilize these services, 60%, indicated that they do not have policies in place to govern the usage of these technologies.

Security concerns involving these emerging technologies are rapidly evolving – with our cybersecurity research this year indicating a marked growth in the number of attacks and malware targeting cloud infrastructures and IoTs.

Does your organization allow or utilize Cloud Services or Internet of Things Tech (Big Data Analytics)?

Organisations that allow or utilize Cloud Services or IoTs Tech 67%

Does your organization have a best practice policy for IoT and Cloud Services?

60% lack policies to govern the usage of Cloud Services or IoTs Tech

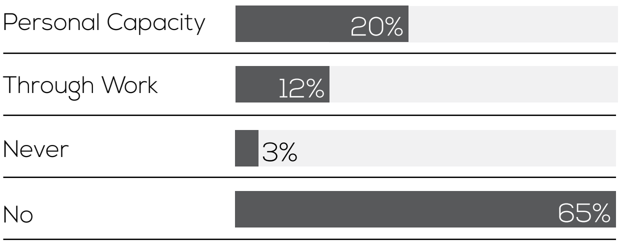
3. Cybercrime

Cyber-criminal related activity affected about 32% of our respondents, majority of whom were affected at a personal capacity. This suggests that attackers are preying on individuals personally and also directing their efforts towards organizations by targeting individuals within these organizations. It is noteworthy that about 65% of the respondents reported not being victims of cyber-criminal activities.

However, from our analysis, majority of people do not understand what qualifies as cybercrime; and therefore a huge percentage of people lack the ability to recognize a cyber-crime when it occurs.

Have you been a victim of any cybercriminal activity in the last 5 years? In what capacity?

32% of the respondents have been victims of Cyber-criminal activities

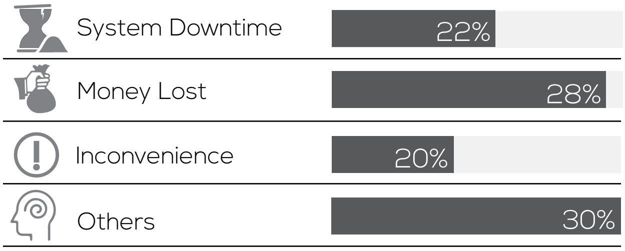


4. Impact of Cybercrime

Loss of Money, System downtime and Inconvenience were identified as the top impacts of cybercrime. This presents one conclusion that majority of attacks in Tanzania are motivated by financial gain – suggesting reasons why financial institutions, Saccos and organisations that deal with transaction processing are primary targets for the Cyber-attacks.

How has Cybercrime impacted on you?

Majority of the respondents have had an impact of cybercrime



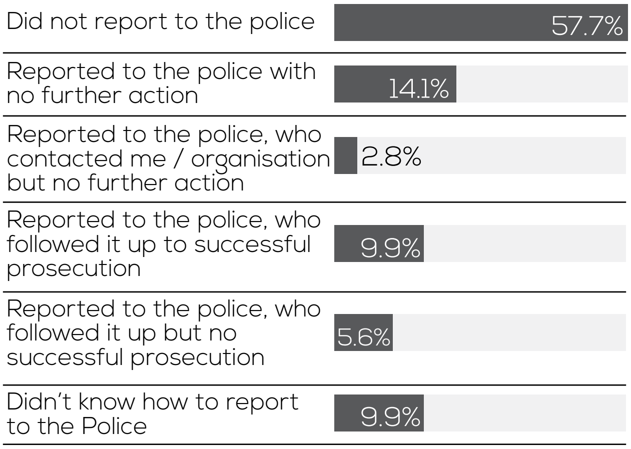
5. Reporting of Cybercrime

Internet-related crime, like any other crime, should be reported to appropriate law enforcement or investigative authorities. Citizens who are aware of federal crimes should report them to local offices of law enforcement. 57.7%, indicated that they did not report the cyber-crime to the law enforcement.

32.4% of the respondents took the matter to the law enforcement, only 9.9% of this reports led to successful prosecution – however this is an 8% improvement from 2016. This is a result of inadequate laws concerning Cybersecurity and lack of technical expertise to investigate incidents of cyber-crime. Also of is that about 10% had no idea of how to report the incidences to the law enforcement.

If you have been a victim of cybercrime, what action followed?

32.4% Reported cyber crime to the authorities

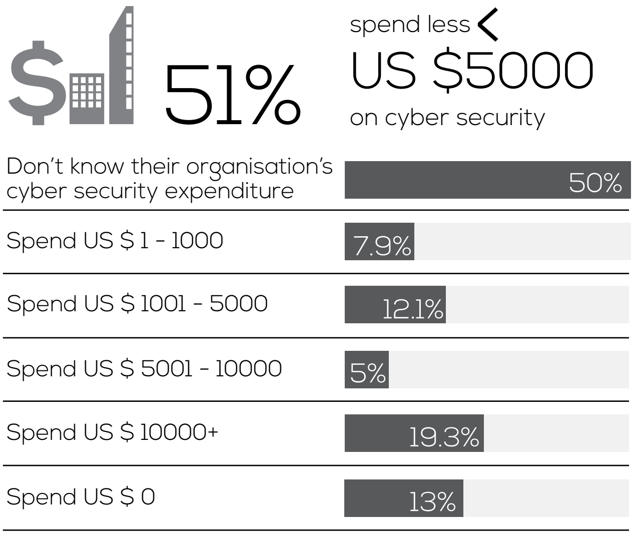


6. Cyber Security Spending

Investment in cyber-security products is increasing. In 2017, we have seen a slight improvement of 4% reported to have spent less than $5000 on cyber security from 55% to 51%. Further analysis also revealed that majority of organisations which spend USD 10,000+ came from the Banking and Financial sectors.

This is not surprising since these industries are the most targeted.

Approximately how much does your organisation spend annually on cyber security?



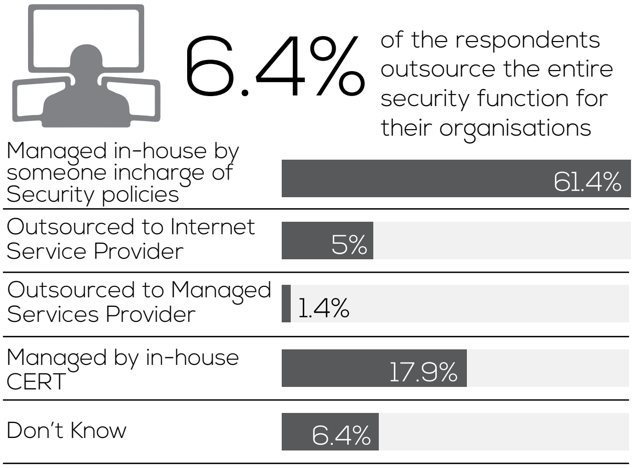
7. Managing Cyber Security

79.3% of organisations manage their cyber security inhouse as follows- 17.9% being handled by a dedicated in-house CERT and 61.4% handled by an individual in charge of security within the organisation. This is an increase of 8.3% from last year.

Only 6.4% have outsourced this services to an external party(MSSP or ISP). More and more companies are now developing inhouse capabilities to manage cyber security, this is particularly the case with Banking and financial institutions .

Our survey revealed that majority of respondents (55%) who did not know how their cyber security was managed came from the Government sector. This was closely followed by Insurance(11%) then Academia(10%).

How is your organisation's cyber security managed?



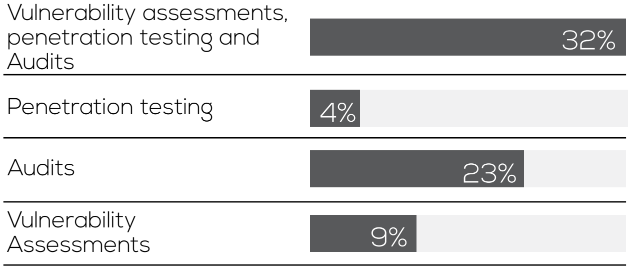
8. Cyber Security Testing Techniques

Security testing is a process that is performed with the intention of revealing flaws in security mechanisms and finding the vulnerabilities or weaknesses in the environment. Recent security breaches of systems underscore the importance of ensuring that your security testing efforts are up to date.

From the survey, 32% of respondents perform a combination of Vulnerability assessments, penetration testing and Audits. 4% perform Penetration testing while 23% perfrom Audits. All these testing techniques are not independent and in fact work best when they are applied concurrently.

Which of the following security testing techniques does your organization use?

68% of the respondents carry out security testing techniques in their organisation



9. Cyber Security Awareness

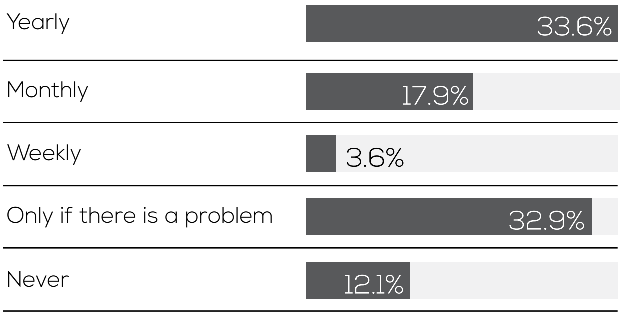
The level of awareness in Tanzania is still low with 17% of organisations not having an established cyber security training program. Most organisations (32.9%)are also still very reactive when it comes to cyber security training, these organisations train their staff only when there is an incident. This is worrying considering 40% of all cyber attacks reported in the survey was through work. In 2017 alone, over 50% of the malware reported was spread through some form of social engineering.

On the other hand, Its important to point out that 55% of respondents reported to have a regular training program in place. The importance of having regular security training for employees cannot be over emphasised.

How often are staff trained on cybersecurity risks?

55% of the respondents are regularly trained

while 12.1% of organisations DO NOT train their staff on cyber security



10. Information Sharing

Few organizations can really work in a vacuum and no single organization can see all of the threats laying in wait on the internet.Despite this, our survey revelaled that 47% of organisations do not keep up to date with cyber security trends and attacks.

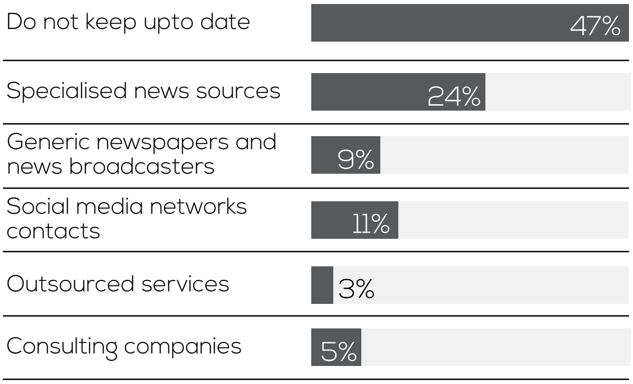
This has resulted in duplication of attacks in various industries especially with the recent Wannacry and Petya ransomwares.

On the other hand, many organizations are wary of sharing sensitive cybersecurity information, especially with governments, regulators and peers. Not only can such information jeopardize the security posture of an organization, it can damage customer impressions of a company and even affect stock values.

Still, it is important for organisations, regulators to put in place infrastructures that will ensure safe shairing of information.

Is there a dedicated role or person within your organisation assigned to distributing or communicating latest cybersecurity updates?

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

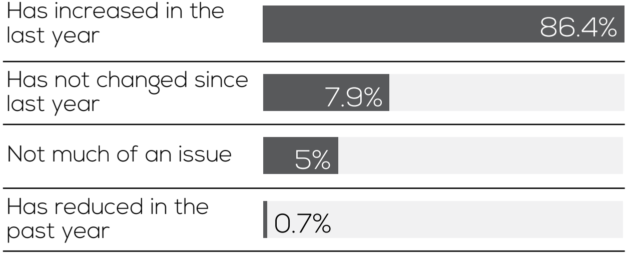


11. Concern about cybercrime in Tanzania

86.4% were of the opinion that cyber-crime related activities had been on the increase in the 2017; and a majority 97.1% of the respondents expressed some form of concern about cybercrime within their organization. This shows that organisations and individuals are starting to be aware of the threat posed by the cyber space.

What is your concern about cybercrime in Tanzania?

86.4% think that cyber crime has increased in Tanzania in the last year

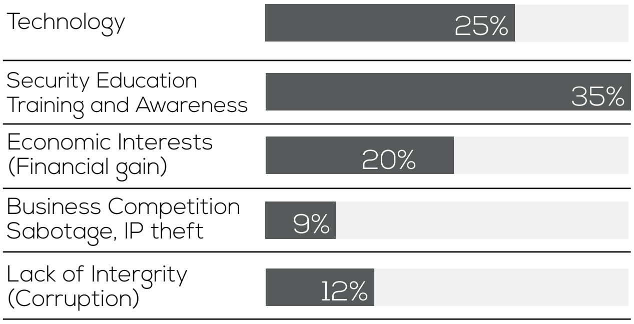


12. Causes of cybercrime in Tanzania

Inadequate security training, education and awareness was thought to be the root problem with cybercrime by 35%, this is because a large number of individuals were unaware of concepts of security. 25% thought that technology and the rapid advancements were the cause, while greed and economic gain were thought to be the cause by about 20%.

What is the underlying cause of cybercrime?

25% of the respondents believed cyber crime is rooted in technology



13. The use of BYOD in organisations.

Does you organisation allow the use of BYOD and do you have best practise policies for them?

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

while

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

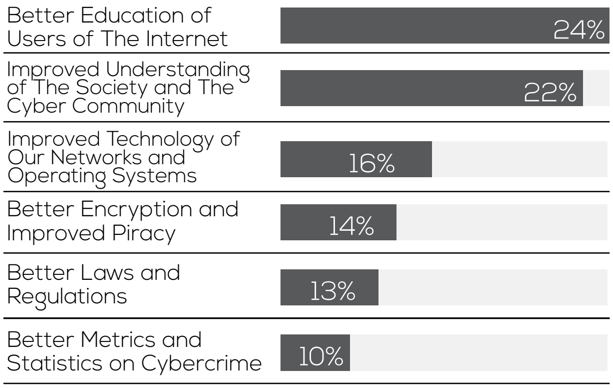
14. Topics we should conduct research on to make the Internet a safer place

24% of the respondents indicated that research should be conducted on educating users about the Internet and security as this will help make them aware of the possible vulnerabilities while using the Internet.

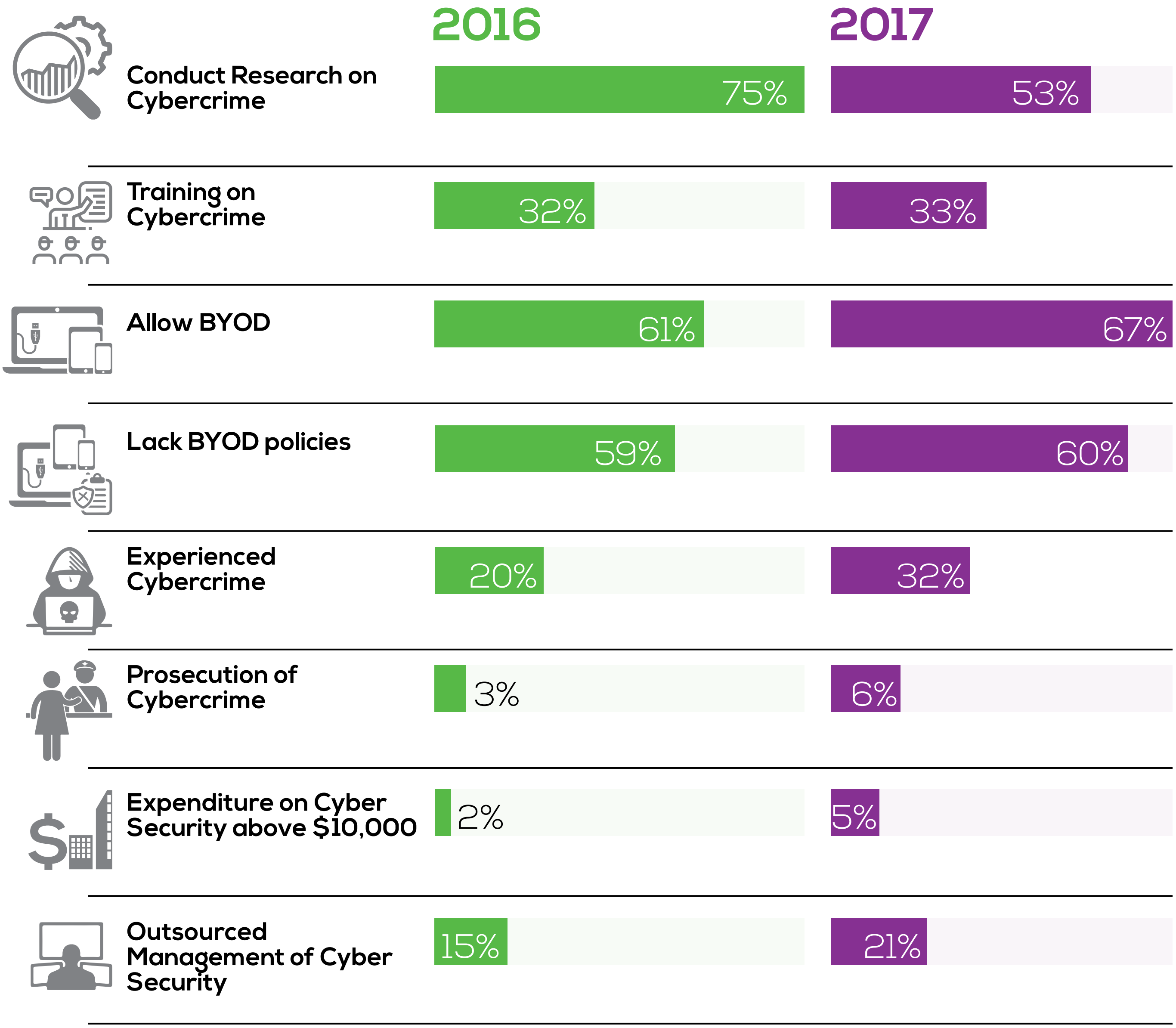
Better understanding of the society and the cyber community was thought to be a key social research area by 22% to ensure safety of the Internet while 16% were of the opinion that investment in Technology research was a major candidate.

What research should we focus on?

13% of the respondents believe we should conduct research on better laws and regulations to make the Internet a safer place



Key Trends From 2016 and 2017



Adv. Josephat Mkizungo

Senior State Attorney

Attorney General's Chambers

"Technology in the modern era created cyber space where people engage in almost everything which was previously done physically. Communication, financial transactions and even auctions are conducted in the cyberspace in recent years. Few years down the road, transactions through this technology seemed as alternative. This cannot be spoken confidently today. With this changing trend therefore security must be placed at the centre stage. Technology by itself however, cannot play protective role in the cyberspace. It is a misconception that cyber security should only depend on technology. People and process must go hand in hand.

In the wake of such trend, countries have put in place legal frameworks to regulate the use of cyberspace. Tanzania not being an exception, enacted two crucial legislation in 2015, Cybercrimes Act and Electronic Transactions Act No 14 and 13 respectively. Cybercrimes Act makes provisions for criminalizing offences related to computer systems and information communication technologies; to provide for investigation, collection and use of electronic evidence and for matters related therewith. On the other hand Electronic Transactions Act provides for the legal recognition of electronic transactions, e-Government services, the use of information and communication technologies in collection of evidence, admissibility of electronic evidence, facilitation of use of secure electronic signatures and other related issues.

Cybercrimes Act is penal and substantial in nature having 26 offences ranging from; computer related, content related, Intellectual property to; offences against confidentiality, integrity and use. Before 2007, electronic evidence was not admissible in court which could have rendered impossible to prove cybercrimes even if Legislation against such ill acts was in place.

Regardless of the admissibility of such evidence, the laws were not clear as to how to weigh such evidence once admitted. Electronic Transactions Act came to clear such a lacuna by providing criteria for authenticating electronic evidence. But, the above is not a guarantee that every offender will be arrested and prosecuted since there are so many challenges in between including; obtaining evidence or the offender as he might be sitting in another jurisdiction. On the other hand authenticating electronic evidence also requires knowledge, expertise and equipments which most developing countries lack.

It should be noted that all these legislation condemning cybercrimes plays as a last resort measure to the victim of such offences. Mindful of this note, we should not only depend on technology and legal frameworks as pillars to safe heaven. Every security starts with oneself!"

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

- Illegal access
- Fraud
- Impersonation

At the outset the society is not very aware about Cyber security issue until they fall victim of the above. Sensitization is being done to different groups but most of them they do not pay much attention unless and until they are victims. Companies are securing their systems and regulatory authorities are now becoming robust to penalize those with vulnerabilities in their processes or systems

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

- Ignorance
- Lack of awareness on Cyber security concern
- Lack of resources

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

Yes.

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

All, however Content owners, Government and users play a greater role.

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

Yes, but it is very difficult to filter the same. However if there is a way it's one good way.

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

Sensitization.

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

Most of the citizens are still in the dark, they do not understand much about Cyber issues. The worry of privacy infringement is not their primary concern. Fraud creates a bit of a worry as many have fallen victims to this due to the spread of the use of money transfer through m-pesa, tigo pesa etc.

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

The main is a security concern, even USA is said to suffer that during elections. Vulnerability of systems is the main concern.

Example: None

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

No.

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

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

Increase awareness to end users, hire resources from countries with expertise and long term plan is create our own resources.

Do you think organizations are spending enough money on combating Cybercrime?

No

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

Make decision makers conscious about the risk.

Based on our research the Africa Cyber security market will be worth USD2 billion dollars by 2020. Despite this opportunity, Africa has not produced a single commercially viable Cyber security product or solution. In your opinion, what should African countries or universities focus on to encourage innovation in the development of Cyber security solutions?

First Government through Universities should put more focus on this faculty while creating a friendly environment for innovation.

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

First they should start by embracing and trusting local resources then they should create an environment which encourage innovation eg sponsoring hubs for people with such skills and talent to share such experience also encourage Research and Development of such solutions in education centers, innovation hubs etc

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

- Sensitization
- Training

Our theme is "Understanding the Cybersecurity triangle: People, Process, and Technology." Which do you think has the biggest impact or weight in Tanzania?

People.

What has to be done in-order to ensure balance in the Cybersecurity triangle in Tanzania?

Raise consciousness especially to decision makers.

In your opinion what drives criminals to commit Cybercrime or Cyber offenses?

Some are due to ignorance especially for those content related offenses, others are greedy.

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

- Sensitization on how to avoid Cybercrime to the general public
- Setting minimum security standards for systems including processes
- Training
- Cooperation local and international
- Legal framework

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

Cooperation.

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)
Database Security	Limited visibility on activities on the databases.	**1. Fraudulent database postings!** **2. Loss of sensitive information!**	24/7 monitoring of activities within databases. Limit and monitor access to database. Audit and review privileged access to DB.	How can Tanzanian companies improve visibility on DB activities at a cost effective and resource friendly manner?
Privileged User Management	Compromised administrator accounts.	**Unauthorized access to critical systems within the organisations!**	Audit the activities of privileged users within the network.	How can organisations implement segregation of duties when resources (staff) are limited?
Patch Management	Missing patches contribute 70% of vulnerabilities identified. 60% of these are never mitigated.	**Exploitation of missing patches to compromise confidentiality, integrity and availability of critical informational assets!**	Remediation roadmaps that ensure that critical patches are applied while medium and low risk vulnerabilities are fixed within a stipulated agreed upon period.	How can Tanzanian organisations maintain a patch management program without exhausting resources?
	Employees are trained only after an incident.	**Employees fall victims of social engineering attacks!**	Regular employee training programs that have an effectiveness measuring metric.	How can organisations ensure employees understand the concepts taught during awareness workshops/ trainings?
Training and Awareness	IT Training is done on specific tools.	**IT teams lack the expertise for defensive and offensive security!**	Regular training on both defensive and offensive Cyber security concepts.	How can IT teams widen their gaze from being "tool analysts" to network engineers and architects?
	Board members lack Cyber security expertise and rely on standard audit reports to understand the security posture of organisations.	**Lack of visibility on actual Cyber security posture!** **No standard way of measuring progress and ROI on IT investments!**	Board training to involve reporting metrics for enhanced visibility that can provide a basis and guide on future decision making.	How can Board members shift from the traditional "oversight" role into the proactive Cyber security role?
Network Security Engineering	Limited expertise in the country on Security Architecture/ Engineering skill set.	**Networks are misconfigured to allow easy manipulation and system sabotage!**	Organisations to invest in or outsource security engineers/ architects for network design purposes.	Where can organisations get specialized training on security architecture/ Engineering?

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

Inter Industry Analysis - Africa

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

* No statistical analysis done in 2016 on this section.

Joseph Mathenge

Chief Operation Officer

Serianu Limited

Approach in Raising Cyber Security Poverty

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

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

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

Ability to Identify threats.

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

Actively protect information assets.

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

Ability to detect cyber incident.

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

Understand how to respond and contain cyber event.

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

Have resilience and ability to recover from cyber event

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

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

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

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

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

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

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

Cost of Cyber Crime

Analysis – 2017

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

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

Cost of cyber-attacks

$99.5m annually

Methodology

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

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

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

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

A significant proportion of this cost comes from the insider threat, which we estimate at $30M per annum. In all probability, and in line with our worst-case scenarios, the real impact of Cyber crime is likely to be much greater. As for measuring costs, this report decomposes the cost based on these 4 categories:

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

$99.5m annually Type & Cost of Cyber Crime in Tanzania

Insider Threat	30%	$29.9M
Attacks on Computer Systems (Unauthorized Access and Malware)	20%	$19.9M
Email Spam & Phishing	15%	$14.9M
Social Engineering and Identity Theft	12%	$11.9M
Online Fraud Scams	10%	$9.9M
Data Exfiltration	8%	$8M
Ransomware	5%	$5M
	TOTAL	$99.5M

Sector Ranking

Banking

Cyber criminals are going directly to where the money is – the Banking sector. Banks and financial firms are big targets for cyber-crime particularly from malicious insiders. Attacks seen over the year include Direct DB manipulation, email phishing and compromise of critical systems to cause downtime.

The increased adoption of newer (and potentially high-risk) technologies including mobile and internet banking further puts these institutions at risk. Majority of the banks do not have controls in place for maintaining transaction limits. It should however be pointed out that, out of all industries in Tanzania, the banking sector has put in more controls and spends more to ensure their cyber security as compared to the other industries.

Telecommunications

From millions of phone numbers, identification numbers, PIN numbers etc, the telecommunication industry holds a lot of personal data. As a result, these organisations are now an attractive prospect for those with malicious intent. Globally and in the past few years, we have seen several high-profile breaches involving the theft of data from numerous telecom companies such as Talk Talk and France's Orange. It is critical that Telcos adopt advanced security solutions to withstand these attacks. It is notable that majority of Telecoms manage their cybersecurity in-house.

Financial Services Mobile Money

Mobile money revolution has seen Sh43 trillion being transferred through mobile phones annually - equivalent to 47 per cent of the gross domestic product.

Majority of banks, merchants and service industry firms in Tanzania are now adopting mobile money services to serve as one of their alternative channels. The continuous integration of Mobile money into other sectors such as hospitality, banking, transportation, telecommunication, E-commerce, government and other financial sectors opens up a number of challenges that attackers are now leveraging. Users are not educated on how they need to secure their mobile phones, how to avoid social engineering that leads to monetary loss etc.

It is critical for organisations to secure their integration points with Mobile money and also educate their users on how to stay safe to avoid social engineering scams that lead them to lose money.

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

Sacco's, Cooperatives and Microfinance

These institutions are rapidly growing in Tanzania. However, they are so focused on customer satisfaction and reducing costs, they tend to neglect investment in cybercrime prevention. This has made them a popular target for cybercriminals. Larger institutions have invested more in cyber security in comparison to smaller institutions hence making them an easier attack target.

E-Commerce

Penetration of e-retailers including online shopping malls such as Jumia, E-Bay, OLX 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 have increased confidence in online shopping. Due to system vulnerabilities, an increase in the number of online scams, fraudulent transactions and breach of consumers' personal information has been noted. Merchants need to be aware of the risks electronic transactions carry, and work towards securing the systems to the highest standards.

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.

Olabode Olaoke

PWC

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

2017 was the year of the Ransomware. There was a global meltdown of ransomware attacks in the year 2017, each one improving on the success and challenges of the previous. Something became more apparent with this wave of sophisticated ransomware attacks across the globe; patching will always lag behind causing a perpetual security gap. Detection and Incident response still remains a capability yet to fully mature in most organisations. For me, it was an opportunity to get the attention of very senior leadership within organisations. In my country (Nigeria) however, too many organisations were too ashamed to disclose that they had been hit - a bad day for the cybersecurity community as we did not get an opportunity to correctly measure our exposure and capabilities to deal with the reality.

Do you think fake news is a major problem in your country or Africa? Well, to some extent

Yes.

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

Content Owners. Fake or real, consumers of news should develop the capability to validate the content they consume.

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

No, I believe in net neutrality and freedom of Internet content. However, organisations like Google, Facebook etc. should determine what kind of content they 'permit/air' on their platforms.

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

Create platforms that can objectively fact-check such fake news and aggressively promote them till they become de facto sources for news validation by anyone who truly cares to check

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

We are not ready as most countries in Africa are not sufficiently prepared for the risk associated with data collection, handling, storage and protection. Where laws/regulation around the management and security of such data exists, they are very limited in scope with almost zero enforcement capability.

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

First problem is that we have limited or no knowledge of how the data is handled, stored, protected and accessed. There is absolutely no insight into what is happening to all the data and information associated with these services, we have no way of knowing who is accessing the data, when where, for what purpose etc. yet, we are expected to trust government to do the right thing with the services even when we often don't trust the government itself. We risk having a lot of personally identifiable data and information fall in the wrong hands and have absolutely have no way of protecting ourselves when this happens.

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

Not directly. I however had to help with a few cases where professional incident response was required.

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

We had quite a lot of security advisory from relevant government agencies and professional services firms and associations. That was really all that happened.

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

Awareness, awareness, awareness! Also, organizations should embrace practicing good information security and where possible ensure that they are making the right amount of investment in cybersecurity as informed by a credible risk management process. Sometimes, ist easier to simply outsource to competent hands.

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

NO!

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

More "evangelizing" by those of us in the profession as well as professionals stepping up to the game. Too many organisations are not getting the right return for their cybersecurity investments and therefore struggle subsequently to make the appropriate investments.

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

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

Invest substantially in research. Research is the soul of cybersecurity; it is a big part of the investment required yet, we focus only on consumption of what's already created. Research software, research data and analytics, build analysis engines etc.

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

Promote competition for the development of local products, patronise them and invest in local capability. Demand excellence and quality from local products

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

Establishment of sound laws, regulatory frameworks around cybercrime, data protection 2. Implementation of cybersecurity frameworks aimed at identification, protection, detection, response and recovery of e-Services with capabilities up to detection and response at a minimum. Organisations should focus heavily on building a human-firewall through effectively targeted TEA (training, education and awareness) initiatives as well as developing technical capabilities for detection and response to cybersecurity incidents.

Home Security

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

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

IP Cameras/Nannny Cams

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

Smart Homes

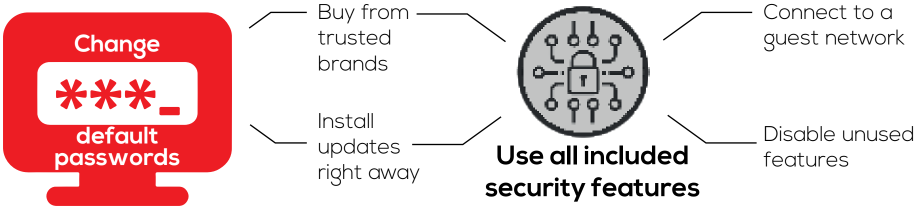
IoT is changing our traditional approach to how we live and interract with our homes. A number of houses, apartments and estates in Dar es Salaam have CCTV surveillance, Smart TVs, DVRs and connected thermostats that you can monitor and handle from any part of the world. These gadgets add convenience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

Home Routers

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

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

Security Tips



Buy from trusted brands

Install updates right away

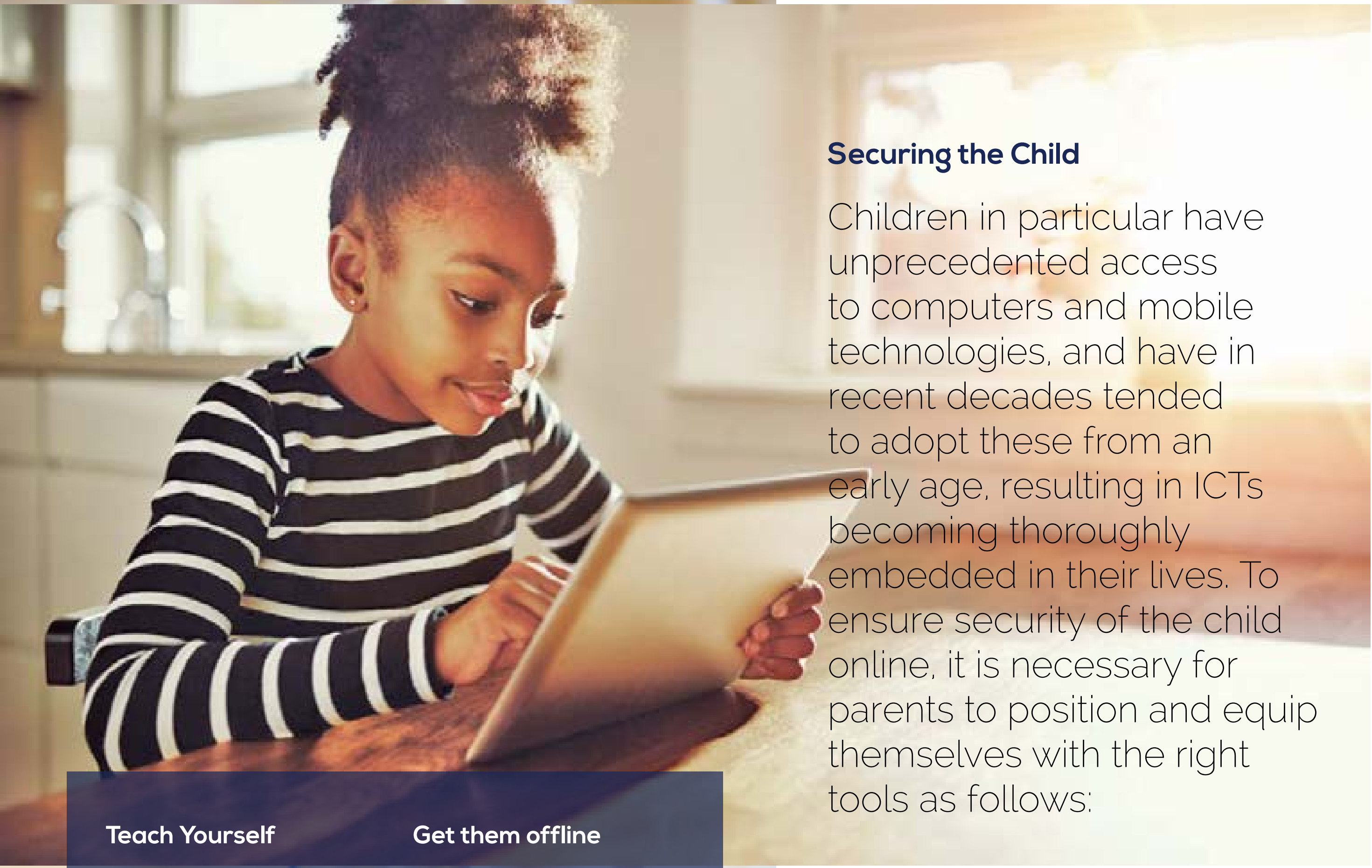
Use all included security features

Connect to a guest network

Disable unused features

Security Begins at Home

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



Securing the Child

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

Teach Yourself

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

Check Privacy Settings

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

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

Get them offline

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

Cyber Bullying

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

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

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

Parents can

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

Dr. Peter Tobin

Privacy and Compliance Expert

BDO IT Consulting Ltd

Mauritius

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

Historical context for the GDPR

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

African personal data privacy and protection developments

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

So what is the European Union GDPR?

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

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

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

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

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

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

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

Key changes in the GDPR

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

Beyond the vanilla GDPR

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

So how is your compliance status?

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

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

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

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

Anatomy of a Cyber Heist

INDICATORS OF COMPROMISE

MULTIPLICITY
VELOCITY
VOLUME
LIMITS

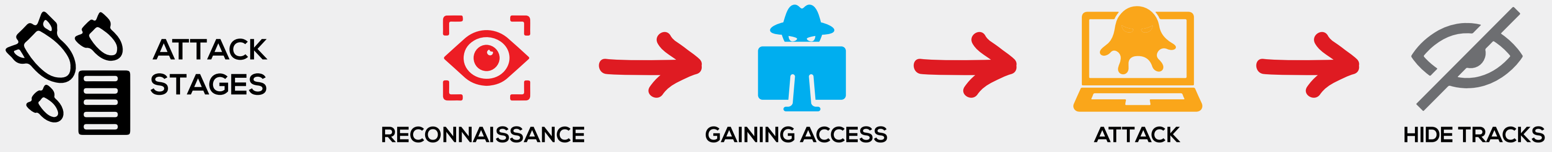
- Scanning from external IP
- Bruteforce attempts
- Excessive DNS queries
- IP conflicts

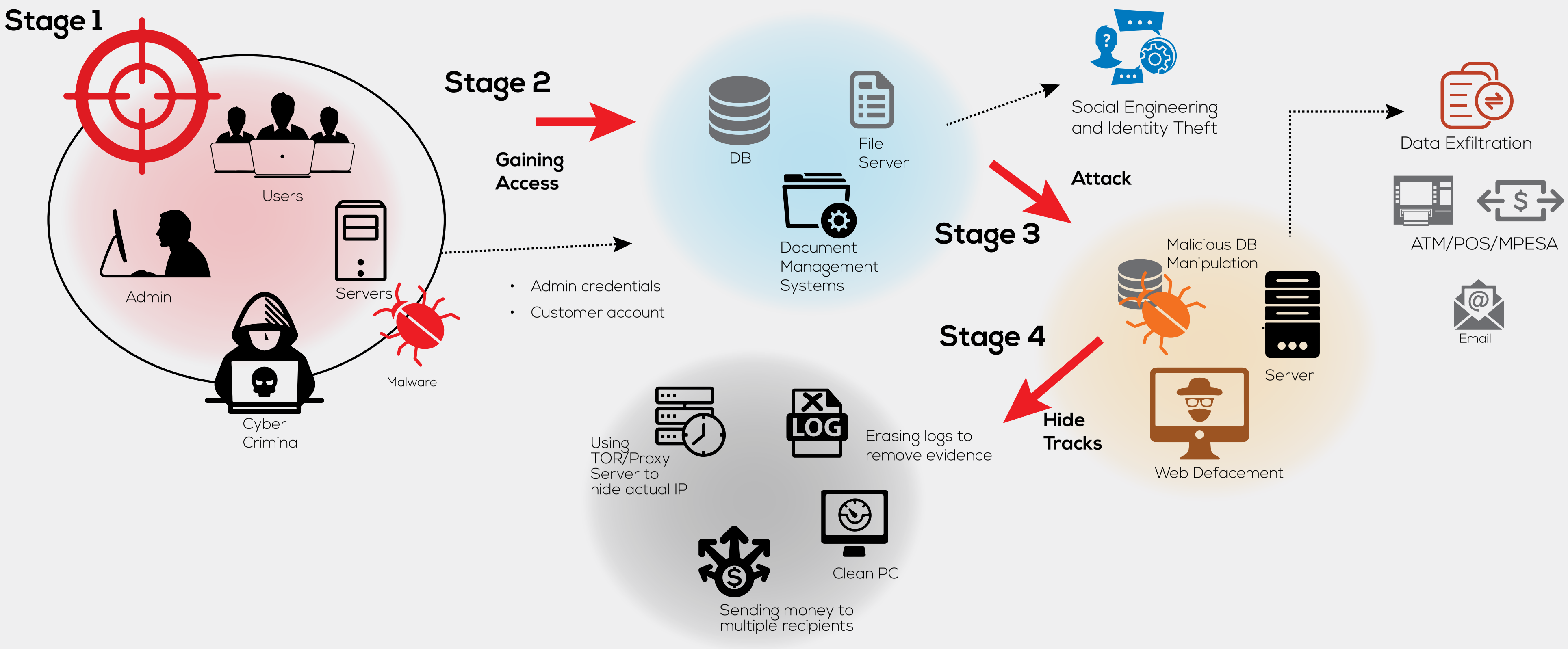
- Traffic to core VLAN from extenal IP
- Multiple posting on DB
- Remote Access tool detected
- Auditry disabled

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

- Logs deleted
- System unavailable
- AV disabled

KEY SYSTEMS
Firewall
Antivirus
DNS
DHCP
AD
Active Directory





Jeff Karanja

Information Security Consultant

Ransomware: A Growing Threat

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

Anatomy of a Ransomware Attack

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

Organisational Challenges

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

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

Counter Measures

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

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

History of Ransomware

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

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

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

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

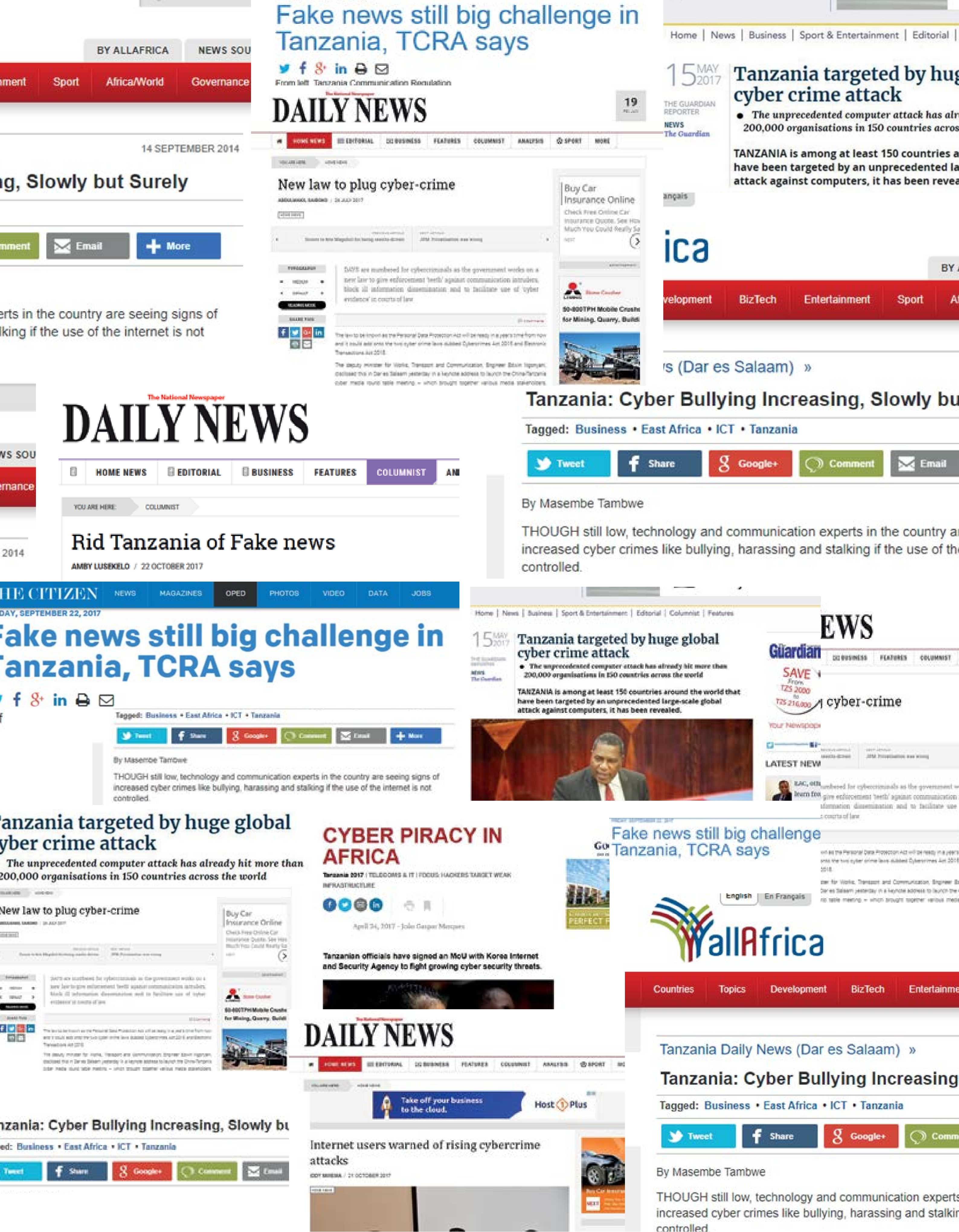
2013 – **Cryptolocker:** uses e-mail as primary attack vector.
2013 – **Locker:** Extorted $150 ransom, payable via Perfect Money or QIWI Visa Virtual Card number.
2013 – **CryptorBit:** corrupts the first 1,024 bytes of data on any file. Leverages Tor and Bitcoin for anonymity and payment.

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

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

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

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



BY ALLAFRICA | NEWS SOU

nment | Sport | Africa/World | Governance

14 SEPTEMBER 2014

ng, Slowly but Surely

mment | Email | More

erts in the country are seeing signs of
lking if the use of the internet is not

Fake news still big challenge in Tanzania, TCRA says

From left, Tanzania Communication Regulation

The National Newspaper
DAILY NEWS

19

HOME NEWS | EDITORIAL | BUSINESS | FEATURES | COLUMNIST | ANALYSIS | SPORT | MORE

New law to plug cyber-crime

Buy Car Insurance Online
Check Free Online Car Insurance Quote. See How Much You Could Really Sa

DAYS are numbered for cybercriminals as the government works on a new law to give enforcement 'teeth' against communication intruders, block ill information dissemination and to facilitate use of 'cyber evidence' in courts of law

The law to be known as the Personal Data Protection Act will be ready in a year's time from now and it could add onto the two cyber crime laws dubbed Cybercrimes Act 2015 and Electronic Transactions Act 2015.

The deputy minister for Works, Transport and Communication, Engineer Edwin Ngonyani, disclosed this in Dar es Salaam yesterday in a keynote address to launch the China-Tanzania cyber media round table meeting – which brought together various media stakeholders.

50-800TPH Mobile Crushe for Mining, Quarry, Buildi

Home | News | Business | Sport & Entertainment | Editorial |

15 MAY 2017

THE GUARDIAN REPORTER
NEWS
The Guardian

Tanzania targeted by hug cyber crime attack

- The unprecedented computer attack has alr 200,000 organisations in 150 countries acros

TANZANIA is among at least 150 countries a have been targeted by an unprecedented la attack against computers, it has been revea

ançais

ica

BY A

velopment | BizTech | Entertainment | Sport | A

s (Dar es Salaam) »

Tanzania: Cyber Bullying Increasing, Slowly bu

Tagged: Business • East Africa • ICT • Tanzania

Tweet | Share | Google+ | Comment | Email

By Masembe Tambwe

THOUGH still low, technology and communication experts in the country ar increased cyber crimes like bullying, harassing and stalking if the use of the controlled.

WS SOU

ernance

2014

The National Newspaper
DAILY NEWS

HOME NEWS | EDITORIAL | BUSINESS | FEATURES | COLUMNIST | AN

YOU ARE HERE: COLUMNIST

Rid Tanzania of Fake news

AMBY LUSEKELO / 22 OCTOBER 2017

HE CITIZEN | NEWS | MAGAZINES | OPED | PHOTOS | VIDEO | DATA | JOBS

DAY, SEPTEMBER 22, 2017

Fake news still big challenge in Tanzania, TCRA says

Tagged: Business • East Africa • ICT • Tanzania

Tweet | Share | Google+ | Comment | Email | More

By Masembe Tambwe

THOUGH still low, technology and communication experts in the country are seeing signs of increased cyber crimes like bullying, harassing and stalking if the use of the internet is not controlled.

Home | News | Business | Sport & Entertainment | Editorial | Columnist | Features

15 MAY 2017

Tanzania targeted by huge global cyber crime attack

- The unprecedented computer attack has already hit more than 200,000 organisations in 150 countries across the world

TANZANIA is among at least 150 countries around the world that have been targeted by an unprecedented large-scale global attack against computers, it has been revealed.

Guardian

SAVE From TZS 2000 to TZS 216,000

Your Newspape

LATEST NEW

EWS

BUSINESS | FEATURES | COLUMNIST

cyber-crime

anzania targeted by huge global yber crime attack

The unprecedented computer attack has already hit more than 200,000 organisations in 150 countries across the world

New law to plug cyber-crime

Buy Car Insurance Online

CYBER PIRACY IN AFRICA

Tanzania 2017 | TELECOMS & IT | FOCUS: HACKERS TARGET WEAK INFRASTRUCTURE

April 24, 2017 - João Gaspar Marques

Tanzanian officials have signed an MoU with Korea Internet and Security Agency to fight growing cyber security threats.

PERFECT F

Fake news still big challenge Tanzania, TCRA says

English | En Français

allAfrica

Countries | Topics | Development | BizTech | Entertainme

Tanzania Daily News (Dar es Salaam) »

Tanzania: Cyber Bullying Increasing

Tagged: Business • East Africa • ICT • Tanzania

Tweet | Share | Google+ | Comm

By Masembe Tambwe

THOUGH still low, technology and communication experts increased cyber crimes like bullying, harassing and stalkin controlled.

nzania: Cyber Bullying Increasing, Slowly bu

ed: Business • East Africa • ICT • Tanzania

Tweet | Share | Google+ | Comment | Email

The National Newspaper
DAILY NEWS

HOME NEWS | EDITORIAL | BUSINESS | FEATURES | COLUMNIST | ANALYSIS | SPORT | MO

Take off your business to the cloud. Host Plus

Internet users warned of rising cybercrime attacks

EDDY MFEMA / 21 OCTOBER 2017

Africa Cyber Security Framework

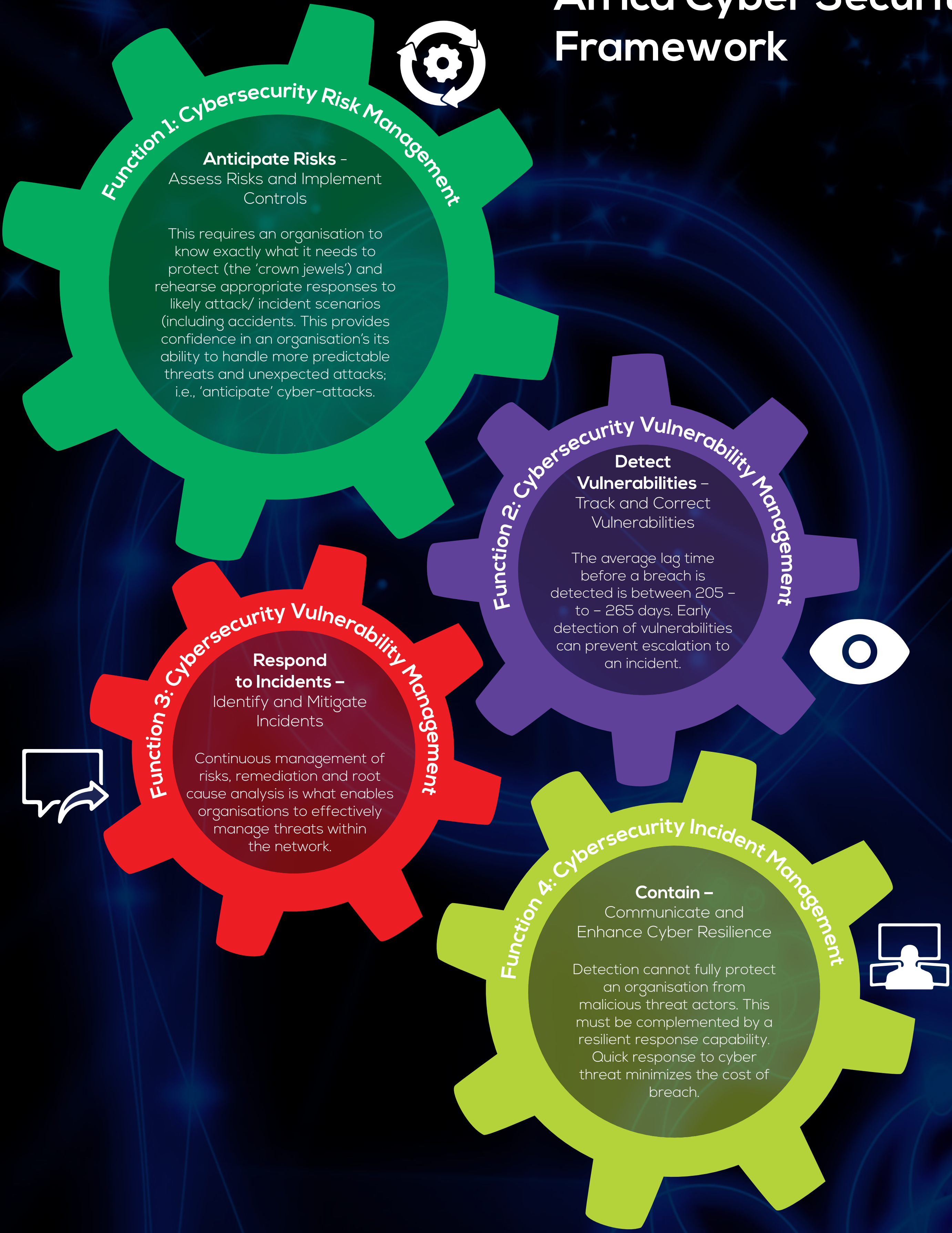
Cybercrime in the African continent particularly within the Small Medium Enterprises (SMEs) setting is a growing concern. SMEs are especially expanding the use of cloud, mobile devices, smart technologies and work force mobility techniques. This reliance has however unlocked the doors to vulnerabilities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

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

Solution

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

Functions of the Africa Cyber Security Framework



Function 1: Cybersecurity Risk Management

Anticipate Risks - Assess Risks and Implement Controls

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

Function 2: Cybersecurity Vulnerability Management

Detect Vulnerabilities – Track and Correct Vulnerabilities

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

Function 3: Cybersecurity Vulnerability Management

Respond to Incidents – Identify and Mitigate Incidents

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

Function 4: Cybersecurity Incident Management

Contain – Communicate and Enhance Cyber Resilience

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

Appendix

List of Remote Access Tools for Database

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

Remote Access tools for Endpoints

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

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

References

Top Issues

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

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

The Computer and Cybercrimes Bill, 2017 - Tanzania Law

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

Attacks

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

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

Cyber Intelligence

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

&sourceid=chrome&ie=UTF-8

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

List of Open Source Tools

Vulnerability Scanners

1. OpenVAS

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

2. Retina CS Community

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

3. Microsoft Baseline Security Analyzer (MBSA)

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

4. Nexpose Community Edition

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

5. SecureCheq

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

6. Qualys FreeScan

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

SERIANU

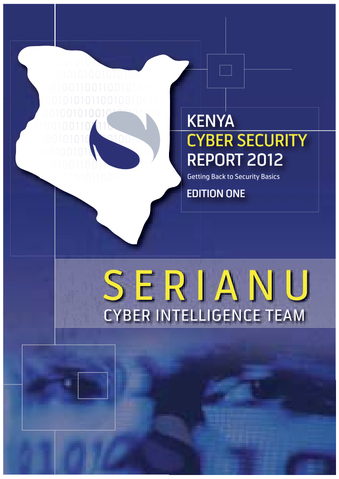
Cyber Immersion

Hands on Cyber Security Training for Professionals

Africa Cyber Immersion Centre
acic
Engage | Educate | Empower

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

info@serianu.com | www.serianu.com



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

SERIANU
CYBER INTELLIGENCE TEAM

KENYA
CYBER SECURITY
REPORT 2014

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

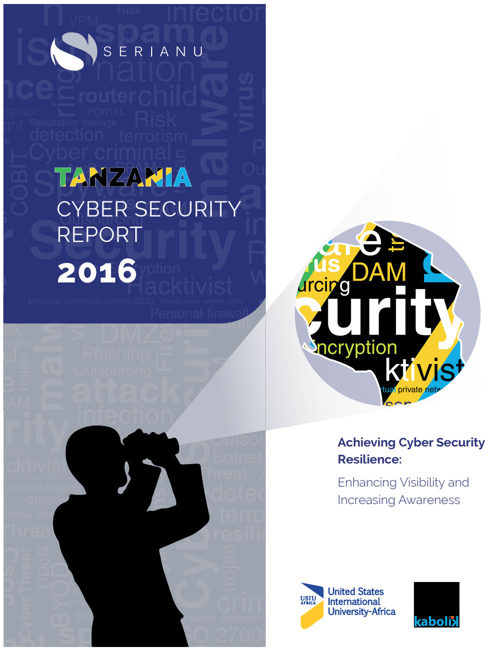
Compiled and published by the Tespok iCSIRT in partnership with the Serianu Cyber Threat Intelligence Team and USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology

SERIANU

KENYA
CYBER SECURITY
REPORT 2015

Achieving Enterprise
Cyber Resilience Through
Situational Awareness

PKF
United States International University-Africa



SERIANU

TANZANIA
CYBER SECURITY
REPORT
2016

Achieving Cyber Security Resilience:
Enhancing Visibility and Increasing Awareness

United States International University-Africa
kabolik

SERIANU

USIU AFRICA United States International University-Africa

ISACA Trust in, and value from, information systems Tanzania Chapter

kabolik

raha LIQUID TELECOM

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