

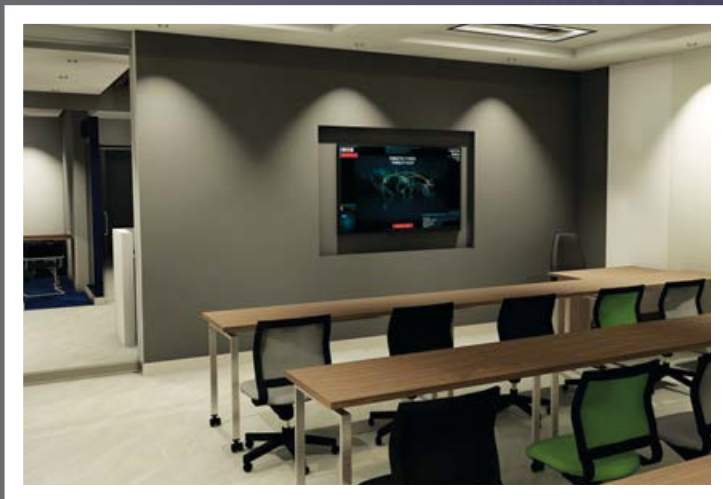
Uganda
Cyber Security
Report  2017

Demystifying Africa's Cyber Security Poverty Line





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

4 We are excited to finally publish the Uganda edition of Africa Cyber Security Report 2017.

Foreword

6 The global cyber security landscape is evolving and becoming quite complex.

Executive Summary

8 The global landscape of cyber threats is quickly changing.

Top Priorities for 2018

12 We have highlighted key priorities for 2018.

Cyber Intelligence Statistics, Analysis, & Trends

17 We have monitored organisations' network for malware and cyber threat attacks such as brute-force attacks against the organisation's servers.

2017 Uganda Cyber Security Survey

32 This survey identifies current and future Cyber security needs within organisations and the most prominent threats that they face.

Cost of Cyber Crime

42 We estimate that cyber-attacks cost Ugandan businesses around \$42 million a year.

Home Security

46 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.

Sector Ranking in 2017

56 Cyber security is no longer a concern for the financial & banking sectors only.

Africa Cyber Security Framework

59 Attackers are now launching increasingly sophisticated attacks on everything from business critical infrastructure to everyday devices such as mobile phones.

Appendixes

62

References

66

Editor's Note and Acknowledgement

We are excited to finally publish the Uganda edition of Africa 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.

Previously, we have been focusing solely on understanding the overall cost of Cyber-crime in Uganda while exposing the risk profiles of Kenya, Tanzania, Ghana and Nigeria. However with the recent increase in Cyber-attacks within Uganda, we have expanded our scope to highlight these issues and provide valuable benchmarking statistics for Ugandan organisations.

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

Survey Analysis: Our survey covered over 110 organisations in Uganda. This section highlights our findings particularly, the challenges facing Ugandan organisations such as low Cyber security budgets and inadequate security awareness.

Cost of Cyber Crime Analysis: In this section we take a detailed look at the financial impact of Cybercrime on Ugandan organisations.

Home Security: This section highlights key challenges in the modern smart home while at the same time sheds light on the ever growing issue of Cyber bullying.

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 Ugandan citizens. This section provides an in-depth analysis of these trends.

Sector Risk Ranking: Here, 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 Cyber criminals operate, from reconnaissance, gaining access, attacking and covering tracks.

Africa Cyber Security Framework (ACSF): We highlight the four (4) key domains of ACSF which serves to help SMEs to identify and prioritize specific risks and steps that can be taken to address them in a cost effective manner.

The Serianu Research Team would not have been able to compile this report without the collaboration and valuable input of key partners. They are:



We partnered with DataposIT, a company that provides state-of-the-art IT infrastructure solutions to its diverse clients base. DataposIT distributed the survey and collected the data and commentaries.



Brencil Kaimba
Editor-in-chief



The ISACA-Uganda 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-Uganda chapter members.



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



The Serianu CyberThreat Intelligence Team

Barbara Munyendo – Researcher, Cyber Intelligence

Kevin Kimani – Researcher, Anatomy of a Cyber Heist

Faith Mueni – Researcher, Sector Ranking

George Kiio – Researcher, Home Security

Margaret Ndungu – Data Analyst

Morris Ndungu – Data Analyst

Ayub Mwangi – Data Analyst

Bonface Shisaka – Data Analyst

Mark Muema – Data Analyst

Joseph Mathenge – Line Editor

Daniel Ndegwa – Line Editor

Nabihah Rishad – Line Editor

Paul Nganyi – Line Editor

USIU Team

Ms. Paula Musuva Kigen

Clive Were

Ian Omondi

Commentaries

Arnold Mangeni
Director, Information Security, NITA

Walusimbi Andrew
Head, Information Security – Eco Bank
National Information Security Advisory
Group & Uganda Bankers Association

Janey Rachel Nakato
IT Senior Manager, KCB Uganda

Ben Roberts
Chief Technical Officer,
Liquid Telecom Group

Henry Kayiza
Assistant Commissioner, Cyber Crime,
Uganda Police

Maurice Taremwa
Academic Relations Director ISACA –
Kampala Chapter
Manager Information Systems Audit,
KCB Bank Ltd, Uganda

Jeff Karanja
Information Security Consultant

Partnerships



In an effort to enrich the data we are collecting, we have partnered with The HoneyNet Project™

and other global cyber intelligence partners to receive regular feeds on malicious activity within the country. Through such collaborative efforts we are able to anticipate, detect and identify new and emerging threats using our intelligent analysis engine. The analysis engine assists in identifying new patterns and trends in the cyber threat sphere that are unique to Uganda.

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

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

Design, layout and production: Tonn Kriation

For more information contact:

Serianu Limited:
info@serianu.com | www.serianu.com

Copyright © Serianu Limited, 2017

All rights reserved

Foreword

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

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

expenditure on Cyber security. The findings from this survey shockingly suggest that a majority of businesses, especially SMEs, are struggling to put in place basic cyber security structures. More than 95% of African organisations in private and public sectors are either operating on the **"Security Poverty Line"** or below. Most of these organisations spend a maximum of **USD 1,500** annually on cyber security technologies and services.

In Africa, Small and Medium Enterprises (SMEs) create around 80% of the continent's employment (World Economic Forum, 2017), which clearly shows the importance of SMEs to African economies. The lack of adequate Cyber security controls in these organisations is an economic threat that the entire SME sector must address. Businesses within the SME sector are continually automating their processes and as a result their continued dependency on technology is driving them deeper into risk. Our research reveals that the most vulnerable SMEs are those in the financial services sector such as cooperatives, saccos, micro-finance institutions, Fin-tech service providers and mobile money transfer services.



To answer this question, we surveyed over 700 business professionals from various business settings in 10 countries across Africa. We then cross-examined their annual



“The 2017 Cyber security survey shockingly reveals that **over 95%** of African businesses are operating **below the cyber ‘security poverty line’.**”

William Makatiani

CEO, Serianu Limited



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

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

expensive for these companies to adopt complex Cyber security frameworks, leaving them exposed and vulnerable to attacks.

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

Executive Summary

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

Our research is broken down into 7 key areas:

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

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

What is the cyber security poverty line?

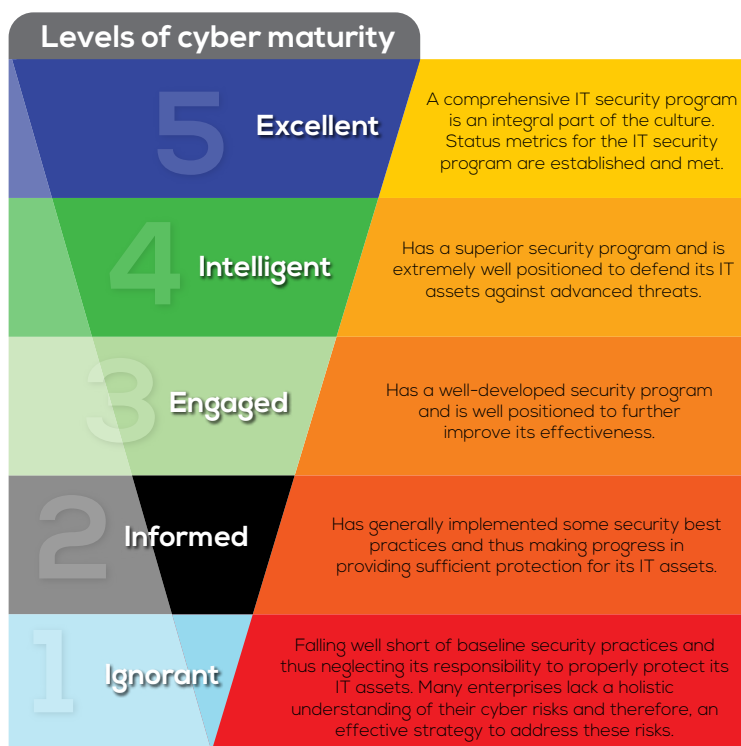
Many organisations particularly SMEs lack the basic "commodities" that would assure them of the minimum security required and with the same analogy, be considered poor.

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

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

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



What is the impact of operating below the poverty line?

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

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

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

What does the future hold for this problem?

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

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

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

What can our readers look forward to in this report?

This report gives insightful analysis of Cyber security threats, trends and issues in Uganda. 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



over
90%
of Ugandans

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



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



Cost of cyber-attacks



\$42m
annually



Banking Sector is still the most targeted industry in Uganda

Majority of the organisations



55%
spend less <
US \$5000

annually on cyber security



96%

Cyber security incidents in Uganda either go unreported or unsolved



Most organisations' Cyber security programs are
Tool Oriented



over
90%

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



S E R I A N U



Cyber Immersion

Hands on Cyber Security Training for Professionals



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

Uganda'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

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

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

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

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

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

3 Patch Management: To patch or not to patch

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

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

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

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

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

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

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

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

5 Endpoint Security: Cyber security front-line

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

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

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

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

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

6 Employee Security Awareness: Ignorance is not Bliss

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

7 Vendor/Third party security: Bring Your Own Vulnerability

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

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

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

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

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

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

ANTICIPATE

What are our risks and how do we mitigate them?

DETECT

Should these risks materialize, are we able to detect them?

RESPOND

What would we do if we were hacked today?

CONTAIN

What strategies do we have in place to ensure damage issues don't reoccur?

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

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

10 Continuous Monitoring: Askari Vigilance

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



WALUSIMBI ANDREW

Head, Information Security
Eco Bank

National Information
Security Advisory Group &
Uganda Bankers Association

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

Yes, it is a major problem in Uganda and Africa.

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

The rapid adoption of mobile technology and the general growth of internet usage across the continent in a time where we still lack technical know-how in terms of cyber security and the inability to monitor and defend corporate networks, making Uganda and African countries vulnerable to cybercrime.

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

The approach to security awareness campaigns needs to change going forward.

Beyond securing our networks and smart devices, we need to start changing mind-sets and provoking a secure mentality among the people.

We need to take them on a 'secure culture' journey, working and empowering them to make secure decisions. For example, to control spread of Ransomware, some organisations use ethical phishing email exercises that is introduce fake phishing email scams, educating staff who click and open them, rewarding those who avoid or spot the 'attacks', then take further action on those who persistently open these scam emails.

Such behavioural change methodologies are practical and can be used to help people reach a self-realization about why cyber security is very important; both to them and to the National Security as the whole.

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

A lot of organisations in the private sector have not attained a mature cyber security level and therefore it is a challenge getting board approvals for cyber security investment budgets. When competing for the same scarce organisational resources, cyber security budgets are most likely to suffer the cuts and as a result, the investment is either little or just as an after thought.

In your opinion, what drives criminals to commit cybercrime?

The capability of cyber criminals to monetize ransomware today has led to an increase in cybercrime. We have seen criminal groups infiltrate networks, carry out reconnaissance and plant ransomware directly onto corporate information assets to cause maximum damage, and in some rare cases, backups have also been destroyed by the same attackers. By removing all possible recovery elements, the organisation is left with literally no choice - 'Pay or lose the data' ... this has been a very effective business model for the cyber criminals.

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

The government has made known its intention to digitise critical public services during various workshops and they are trying to on-board all stakeholders including Cyber security consultants. The aim is to create a secure Cyber space in which these services can be accessed and to also build capacity to address the increasing Cyber threats for all critical national-Information infrastructure.

The Cyber security forum under Uganda Bankers Association (financial sector) too has taken a couple of steps in this same direction as they seek to leverage on these



government establishments to develop a uniform front against cyber threats. They too have realized that it is no longer sustainable to have an inward looking approach to cyber security.

This collaboration will result into formation of a FinCERT ecosystem to promote sector synergy on Cybersecurity, knowledge-sharing, intelligence gathering which will then give national security a good visibility into the security posture of the private sector.

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

I'm aware of a couple of victims of cybercrime, both individuals and organisations.

Were these cases reported to government authorities and prosecuted?

The cases were reported however the lack of clear Cybersecurity legislation negatively affected the legal proceedings.

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

Organisations in Africa need to adopt good basic security controls such as malware prevention, user/client education or awareness, incident management, rigorous patch management programs and comprehensive cyber risk assessments focused on the impact of cyber-attacks on their systems.

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

The Financial Services sector is the most affected and is going to continue facing a myriad of these threats for as long as digital / mobile transactional channels exist.

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

The top priority should be addressing the absence of established career and training pathways into the profession. Hopefully this will attract young people that will eventually fill the shortage gaps of cyber security specialists on the continent.



Cyber Intelligence Statistics, Analysis, & Trends



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



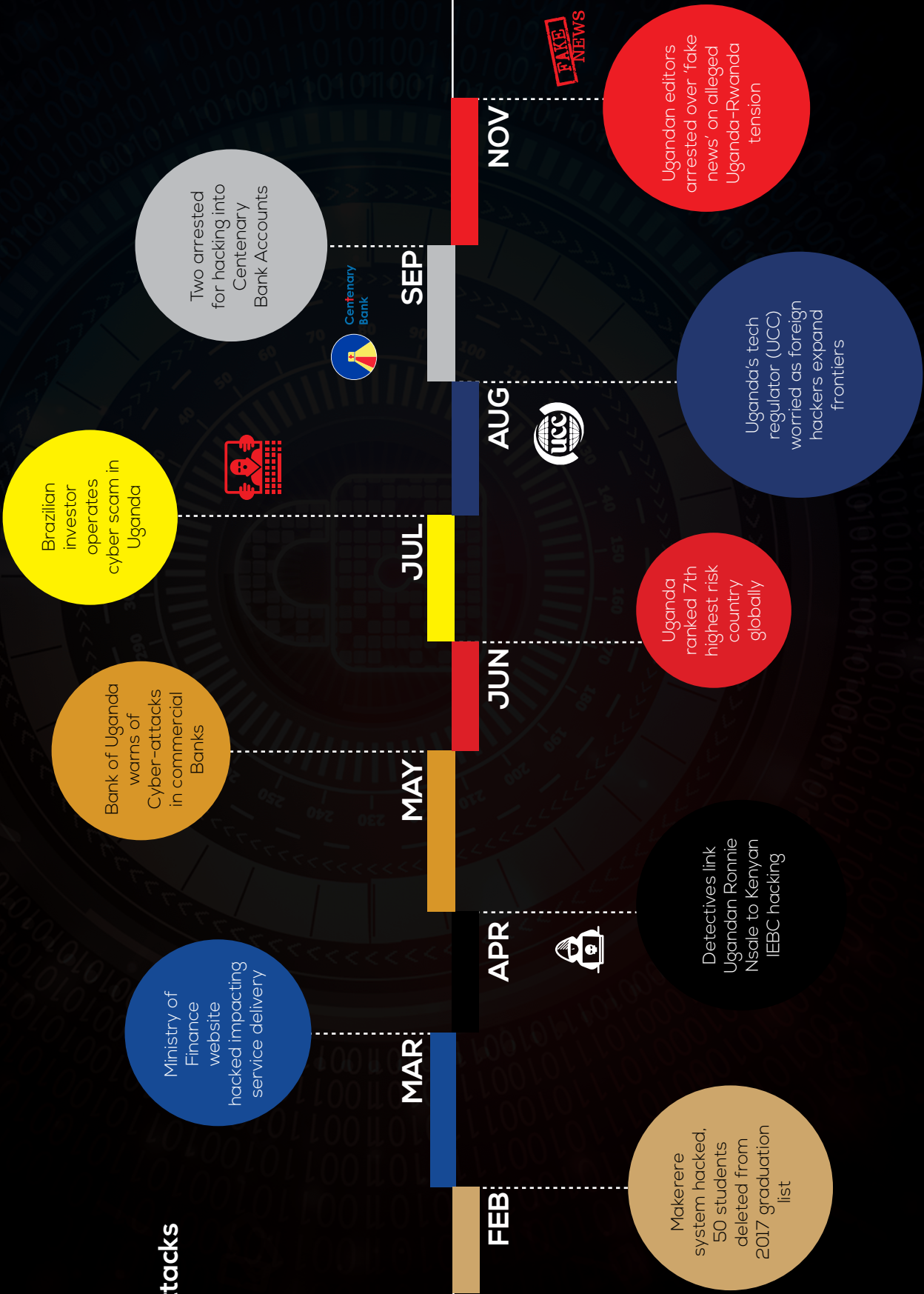
Project Honeypot Intelligence Analysis

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

2017

Top Attacks

Hacks





**JANEY RACHEL NAKATO**IT Senior Manager
KCB Uganda**Do you think Cyber security is a major problem in Uganda/Africa?**

Yes.

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

- Increased automation in the industry where organisations seek to drive efficiency, while at the same time putting little emphasis on security has created an open opportunity for the young informed population to exploit. The fact that all institutions operate on the internet implies that cyber security exposure goes beyond political boundaries.
- Decision makers in many organisations are profit driven and lack the appreciation of Cyber security threats. They therefore shy away from high cost of implementing security solutions and remain exposed to the Cyber security threat.

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

Deliberate effort needs to be made to train and equip cyber security professionals both in the private and public sectors. These individuals should be at the forefront to drive the agenda of awareness in organisations and the country at large. Emphasis should be made right from top management and cyber security should form part of the agenda whenever key risks are being discussed.

Full disclosure of breaches should be enforced so that Cyber security is appreciated as a local problem as well.

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

The investment in cyber security remains unbalanced in the private sector with large

multinationals investing significantly but with smaller local companies investing much less. This needs to be standardized per industry through regulatory requirements. Minimum security standards should be defined per industry with clear consequences if they are not adhered to.

In your opinion, what drives criminals to commit cybercrime?

I believe the desire to make money is the biggest motivator for cybercrime. This is further exacerbated in young qualified but unemployed adults who are cognisant of the loopholes in the cyber security posture of many institutions.

The young individuals who exploit cyber security weaknesses usually establish that the chances of being detected are low. The limited exposure of investigative officers and prosecutors to the intricacies of cybercrime and preservation of evidence has led to very low success in prosecution, and the penalties are not deterrent enough.

Other motivators are the desire for reprisal and to some extent the need to try out and exercise skills obtained.

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

The government has embarked on some remarkable effort for example the well-equipped forensic laboratory for the Uganda Police. There is, however, still a clear need to work together with the private sector to align processes, create awareness of available supporting infrastructure and drive its utilization to combat cybercrime.

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

Yes.

Were these cases reported to government authorities and prosecuted?

Yes, procedures were followed to report the cases to authorities. In many cases though, forensic data is insufficient which affects ability to apprehend and prosecute the perpetrators to satisfactory conclusions.

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

I believe the best approach should tackle awareness, regulation and building technical ability.

Cyber security awareness needs to be increased such that individuals and institutions know that breaches are happening, their nature, magnitude and

factors that increase the risk. Awareness should take the top down approach to ensure that decision makers in all organisations have a good appreciation of the cyber security threat.

Regulation should be put in place and enforced to ensure that institutions have in place the ability to deter attacks, detect breaches and respond appropriately. Currently, many institutions are attacked and never discover it, or only discover after a long time from external sources. Many incidents reported also do not get prosecuted successfully due to insufficient forensic data.

Technical capacity in terms of well trained Cyber security professionals, law-makers, prosecutors and investigative officers needs to be boosted significantly to achieve success.

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

The financial sector is the most affected for the primary reason that they hold the funds. However, government is very important in this aspect and emphasis should be put on it as well.

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

Top priority should be to drive awareness and build technical capacity to combat cybercrime.





Malware Attacks

2017

JAN



New Variant of KillDisk is Ransomware

FEB



Macro Malware for MacOS users

Torrent Locker Ransomware

DNSMessenger malware

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

MAR



TeamSpy Malware transforms Teamviewer into a Spying software



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



New Malware strain targeting Linux-based systems



False Guide malware

APR



PDF file containing Ransomware downloader



PowerPoint Malicious Hover Vulnerability

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



Fireball Malware infects 250 million computers

OakBot banking Trojan harvests financial information




Petya Ransomware has spread internationally, wreaking havoc.

A new variant of Marcher Android sophisticated banking malware disguised as

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

 Backdoor Gazer
Ransom Lukitus
IKARUS dilapidated

 Bad Rabbit Ransomware
IoT Reaper

 CoinMiner

JUL

AUG

SEP

OCT

NOV

DEC



GhostCtrl
Android-information Stealer Malware with Ransomware capabilities



FruitFly malware variant.

Android.Bankbot.211.o rigin

SambaCry Variant-CowerShell



CCleaner Malware:
Locky Ransomware Variants

Gazer Backdoor-targeting governments



Zeus/ZbotPCRat/Gh0st
Gh0st





BEN ROBERTS

Chief Technical Officer
Liquid Telecom Group

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

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

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

Yes.

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

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

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

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

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

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

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

Threat Intelligence

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

We broke down the findings into the following sections:

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

Open Ports

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

- TCP 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).



65,535 TCP ports | **65,535** UDP ports

	Top 10 Open Ports	Unencrypted Ports	Encrypted Ports
Port 80 HTTP	22%	31%	
Port 53 DNS	18%	25%	
Port 23 TELNET	16%	23%	
Port 443 HTTPS	15%		56%
Port 22 SSH	10%		36%
Port 21 FTP	4%	6%	
Port 8080 HTTP	3%	5%	
Port 25 SMTP	3%	4%	
Port 143 IMAP	2%	3%	
Port 2323 TELNET	2%	2%	
Port 110 POP3	2%	2%	
Port 993 IMAP			3%
Port 995 POP3			2%

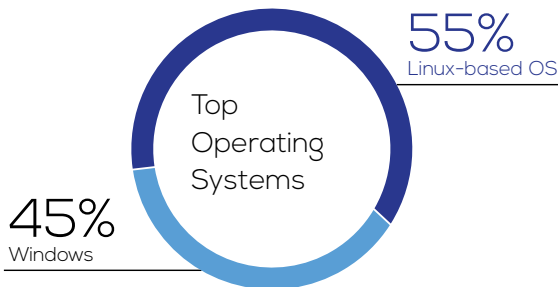
- UDP port 22 is a common target by attackers since its primary function is to manage network devices securely at the command level. Attackers commonly used brute-force and dictionary attacks to obtain the server credentials therefore gaining remote access to the server and deface websites or use the 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.



Top Operating Systems

Cisco IOS	36%
Ubuntu	20%
MikroTik Router OS	18%
Windows	18%
CentOs	7%
Debian	4%
Win32	3%
Unix	1%
FreeBSD	1%



SSL/TLS Vulnerabilities

SSL/TLS certificates provide secure, encrypted communications between a website and an internet browser. Setting up an SSL certificate is deceptively simple technology and is easy to deploy but often not easy to setup correctly. To ensure that all security loopholes are closed, system administrators must properly configure their servers to meet required security objectives.

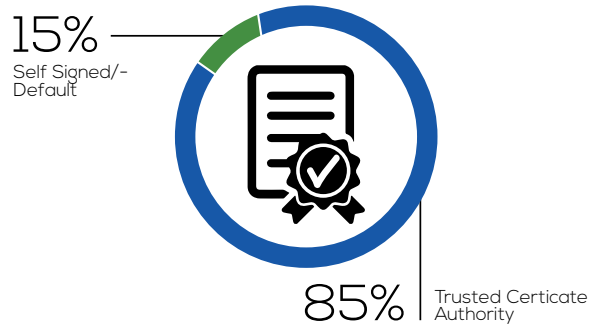
Based on our analysis, the following statistics were obtained:

Use of Self Signed Certificates

Some organisations use self-signed SSL Certificates instead of those issued and verified by a trusted Certificate Authority. When compared with certificates signed by CAs, self-signed certificates are often viewed as less trustworthy because they contain both the public and private key in the same entity.

A number of attacks have successfully been exploited on self-signed certificates. Once compromised, self-signed certificates can allow spoofing of the victim.

Self-Signed Certificates vs Trusted Certificate Authority



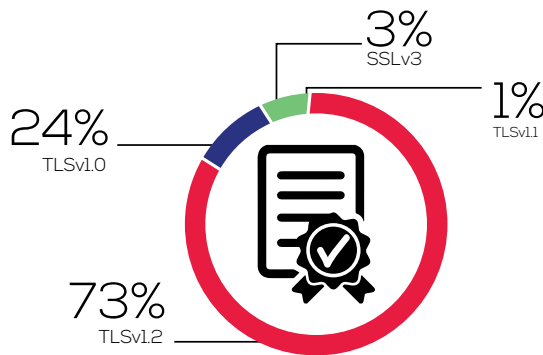
SSL Certificate Vulnerabilities

a) Weak Encryption Protocol

As with any technology, SSL/TLS has its flaws. Successful attacks on a security protocol that is designed to protect you, defies its purpose and jeopardizes the integrity, confidentiality and authenticity of information transmitted.

Due to weaknesses existing on HTTP, SSL was introduced as a means of securing data transmission through the use of encryption. Weaknesses on SSL (Secure Socket Layer) allowing Man-in-the-Middle attacks and information leakage led to its prohibition and use of TLS (Transport Layer Security) as its replacement. The current recommended version is TLS version 1.2.

Supported Certificate Versions



b) Heartbleed Vulnerability

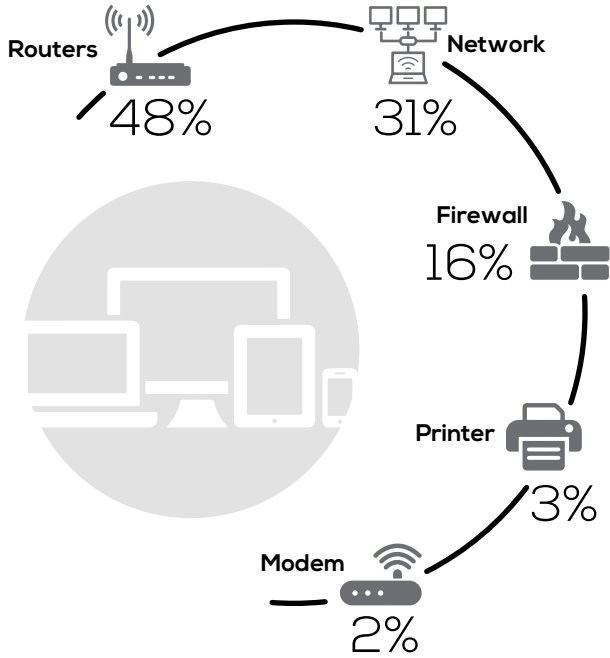
The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information such as user names and passwords, instant messages, emails and business critical documents and communication protected that under normal conditions, is encrypted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



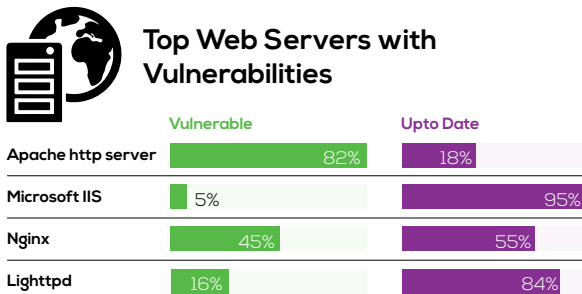
Port 443
Https

	Nigeria	27%
	Kenya	27%
	Ghana	11%
	Tanzania	11%
	Mauritius	9%
	Uganda	7%
	Ethiopia	7%
	Lesotho	0%

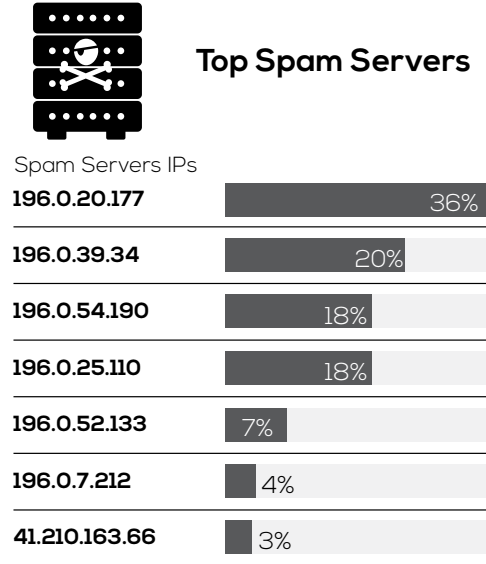
Top Device Types



Top Web Servers with Vulnerabilities

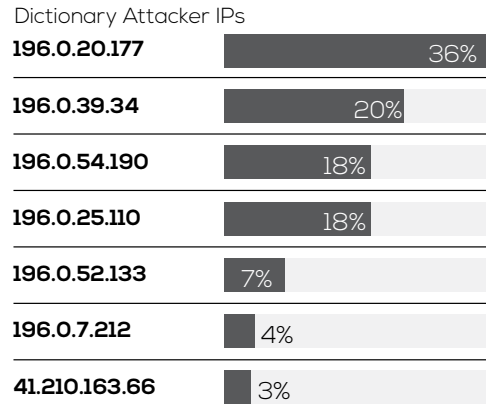


Top Spam Servers



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

Top Dictionary Attackers



*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



HENRY KAYIZA

Assistant Commissioner,
Cyber Crime Unit, Uganda
Police

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

Yes, indeed.

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

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

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

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

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

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

In your opinion, what drives criminals to commit cybercrime?

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

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

Yes there are laws in Uganda:-

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

There are also government parastatals in place:-

- NITA-U
- UCC

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

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

Were these cases reported to government authorities and prosecuted?

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

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

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

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

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

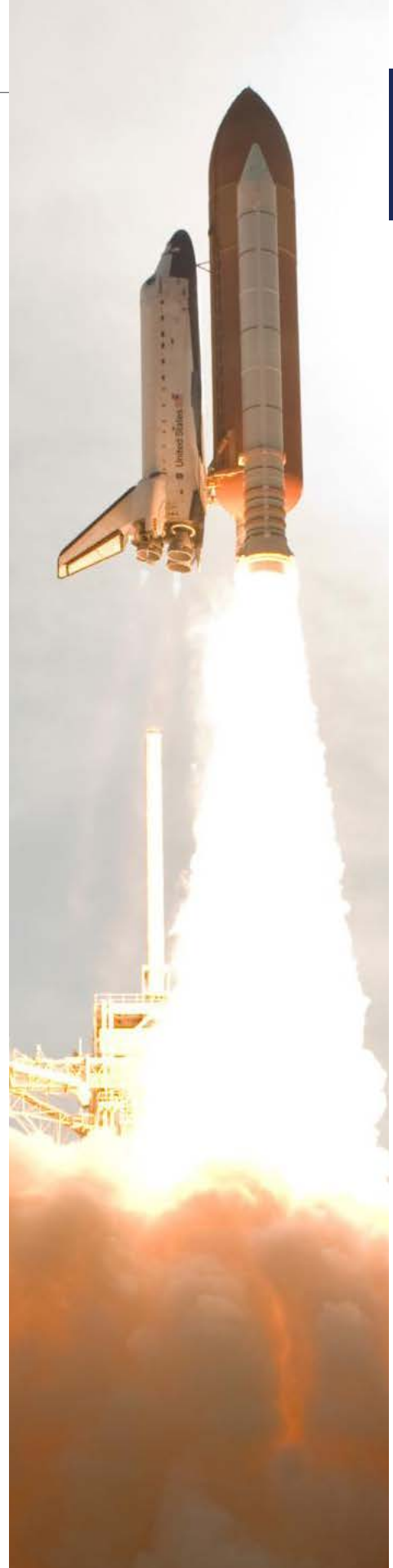
- In terms of amounts involved
- In terms of number cases (quantity)

Therefore according to my experience; I have cases of banks,

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

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

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



2017 Uganda Cyber Security Survey



Uganda



110
respondents



9
Industry Sectors

THE GOAL OF THE 2017 UGANDAN 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 UGANDA. CYBERCRIMINALS CONTINUE TO TAKE ADVANTAGE OF THE VULNERABILITIES THAT EXIST WITHIN SYSTEMS IN UGANDA 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 110 respondents across organisations in Uganda. This included companies from the following sectors:



Academic



Insurance



Banking



Legal Advisory



Financial Services



Professional Services



Government



Telecommunication



Healthcare Services



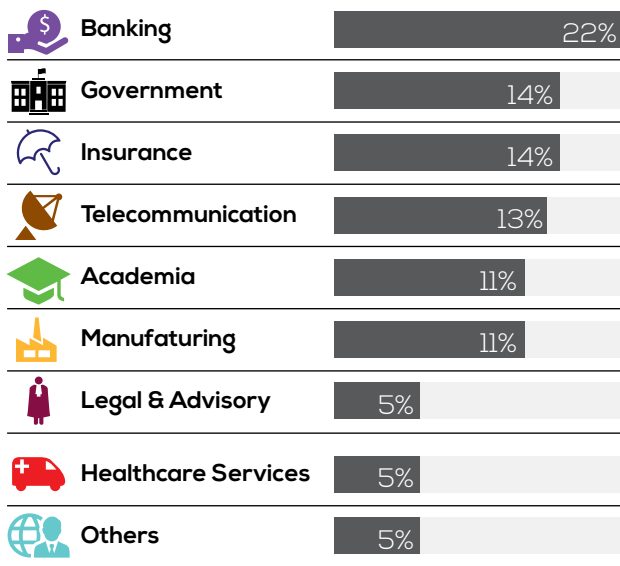
Others

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 Ugandan organisations and the security awareness and expectations of their employees.

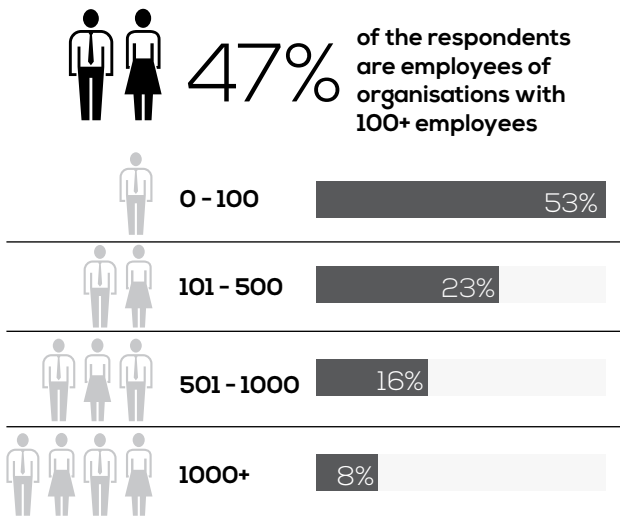
Summary of Findings

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

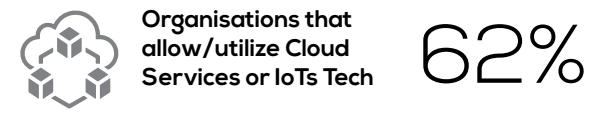
Majority of the respondents were from the banking industry



53% of the respondents are organisations with 100 and below employees



62% of the organisations allow the use of IoTs

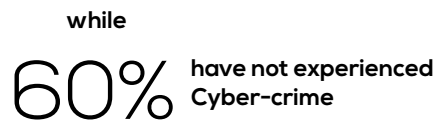


It is paramount that organisations which have adopted cloud and IoT services implement policies and procedures to govern the adoption, maintenance and retirement of these technologies.

58% of organisations are concerned about cybercrime



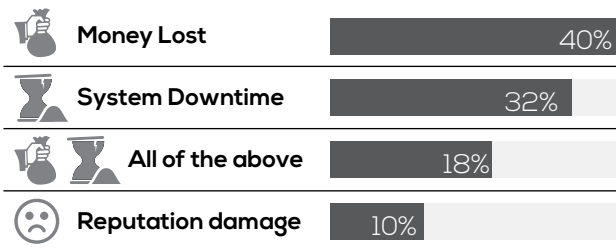
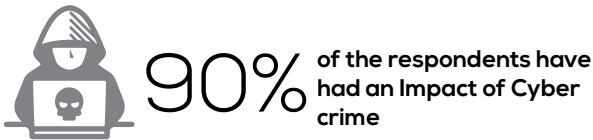
20% have experienced cybercrime in their organisation



the above can be attributed to two main issues:

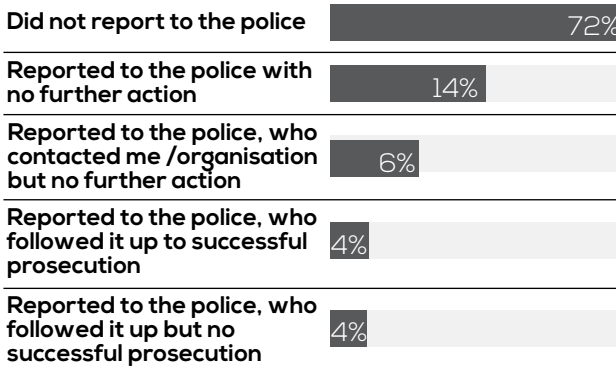
- Internet penetration in Uganda is still low
- majority of people do not understand what qualifies as Cyber-crime. As such, a huge percentage of people lack the ability to recognize a Cyber-attack when it occurs.

90% have been impacted by cybercrime

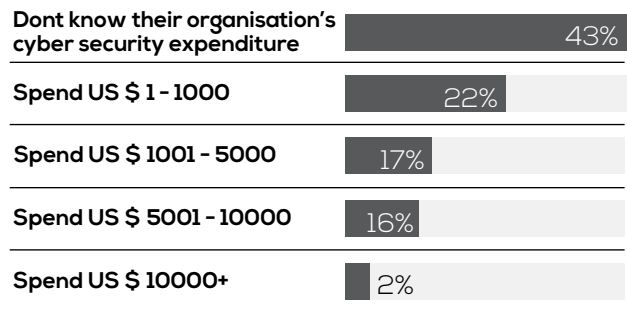


Financial institutions, Saccos and organisations that deal with transaction processing are the primary targets for the Cyber-attacks.

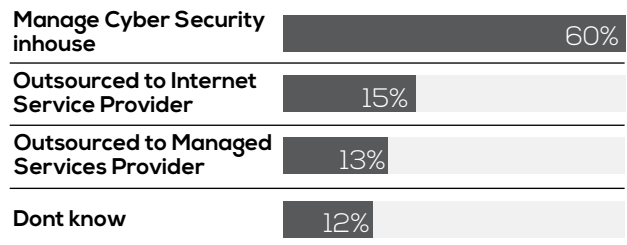
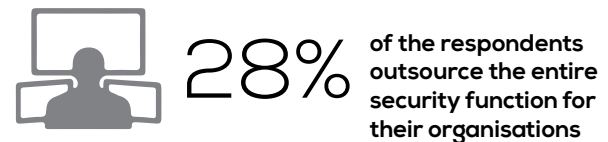
Only 28% reported cybercrime to the authorities



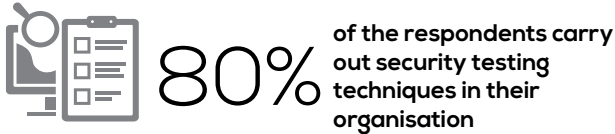
55% spend less than US \$5000 annually for cyber security



28% of the organisations outsource their entire security functions



80% of the organisations carry out security testing techniques in their organizations



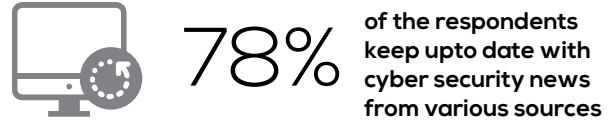
Penetration testing: Vulnerability Assessments; Audits	23%
Dont know	18%
Audits	17%
Vulnerability Assessments	12%
Penetration testing: Vulnerability Assessments	10%
Penetration testing	10%
Penetration testing: Audits Series 9	4%
Vulnerability Assessments Audits Series 10	4%

60% of the organisations regularly train their employees on cyber security issues



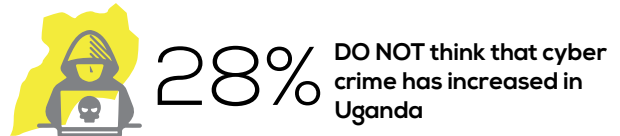
while 12.1% of organisations DO NOT train their staff on cyber security

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



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

72% believe that cyber crime has increased in Uganda

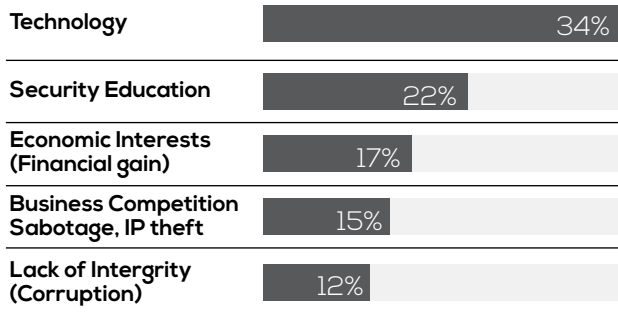


Has increased in the last year	72%
Has not changed since last year	15%
Not much of an issue	9%
Has reduced in the past year	4%

34% believe that cyber crime is rooted in technology

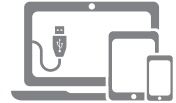


34% of the respondents believed cyber crime is rooted in technology



41% of organisations allow the use of BYOD

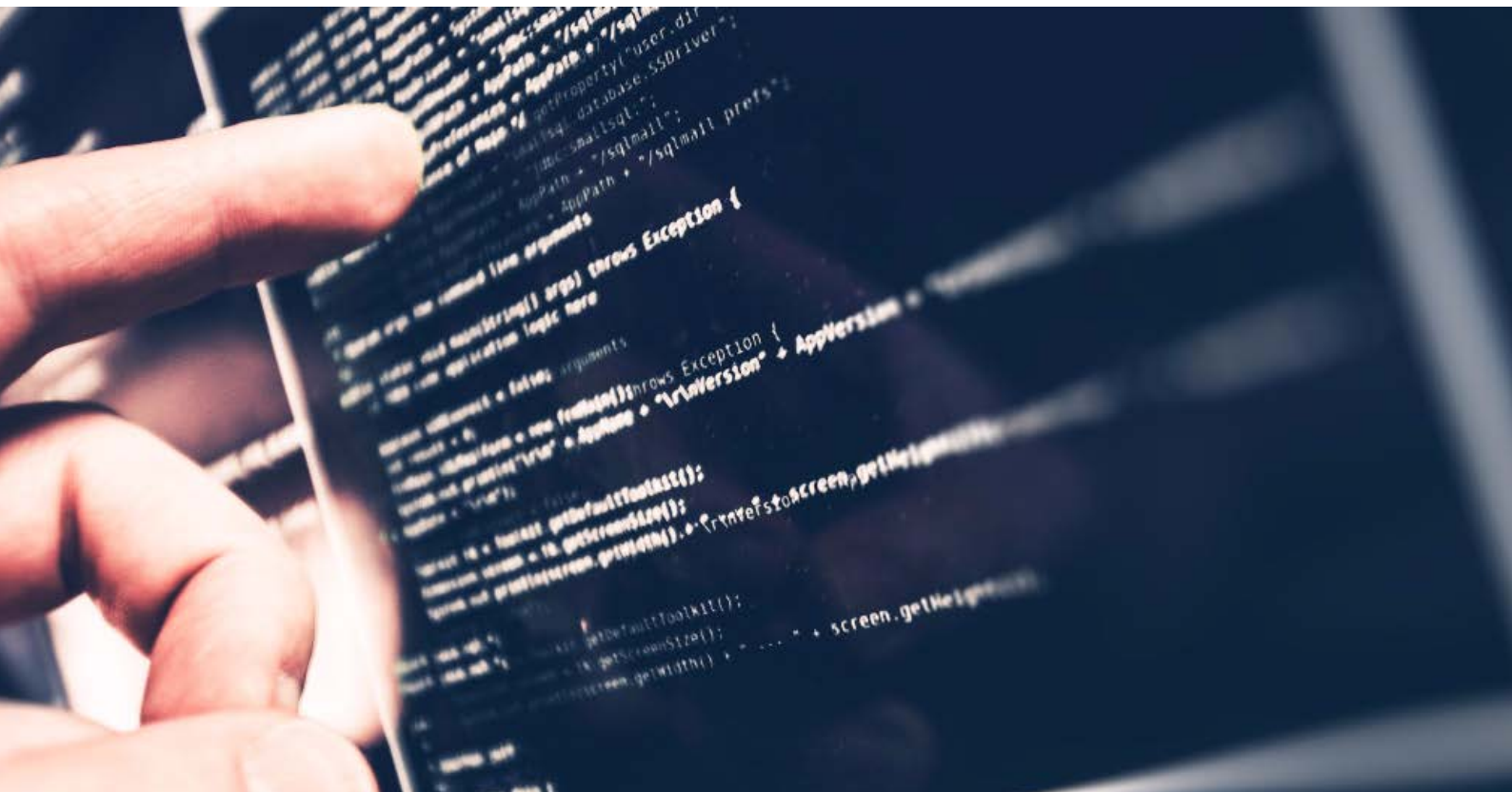
41% of organisation allow the use of Bring Your Own Devices



while









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





Summarized Findings Report – What are Cybersecurity Gaps in Uganda?













*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 Ugandan 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 Ugandan organisations maintain a patch management program without exhausting resources?
 Training and Awareness	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?
 Training and Awareness	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 Ugandan organisations share information on malicious insiders?
 Continuous Monitoring	Multiplicity-Remote Access to critical system after business hours goes undetected Velocity – Multiple failed logins to critical system within a short period of time goes undetected by security teams Volume – Bulk transactions go undetected by security teams Limits – Security personnel are unable to determine a baseline for understanding limits as an indicator of compromise.	Compromise of confidentiality, Integrity and Availability Compromise of confidentiality, Integrity and Availability Compromise of confidentiality, Integrity and Availability Malicious postings of transactions	Multiplicity as an Indicator of Compromise – Establish a baseline for what is normal. Velocity as an Indicator of Compromise – Establish a baseline for what frequency is normal for the organisations. Volume as an Indicator of Compromise – Establish a baseline for what number, bandwidth or utilization metric is normal for the organisations. Limits as an Indicator of Compromise – Establish a baseline for what threshold is normal for the organisations	How can Ugandan organisations establish a baseline for what "normal" is.

Inter Industry Analysis - Africa

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

* No statistical analysis done in 2016 on this section.



**MAURICE TAREMWA**

Manager Information Systems
Audit, KCB Bank Uganda Ltd

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

- Social media and fake news. It has increasingly become very easy to disseminate misinformation and difficult and difficult to separate fiction from reality.
- Social engineering: This has been the source or entry point for most of the cyber frauds experienced in the country. Including but not limited to email hacks and leaking of compromising private material.
- Financial crime: Financial institutions have been major victims of electronically perpetrated fraud by both insiders and third parties alike.
- Ransomware: For many organisations, the fear (ignorance driven) of ransomware, and not necessarily the actual attack, greatly and the haphazard nature of responses to the threat of ransomware and not necessarily the actual attack greatly impacted organisation with service disruption and in some instances, outage or downtime being experienced even where it could have been avoided.

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

Yes

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

All stakeholders' government, end users, Telco's/ISPs or content owners have a shared responsibility. Government should

ensure that all stake holders are held responsible for their role in generation and propagation of fake news and that there are appropriate repercussions for complicity.

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

Yes. Platforms with impact as big as Google and Facebook should be held responsible for their role in facilitating the spread of fake news.

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

People should be encouraged to look out for information from trusted reputable sources and also facilitated in their proper identification and discernment of unscrupulous ones.

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

Yes, African citizens are ready, however, governments must, as they implement e-governance projects, also demonstrate and build confidence that the accompanying risks are adequately managed. Development of local capacity to deal with the complete lifecycle is pivotal to fostering this service delivery and public confidence in the services.

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?

Given weak system controls;

- The threat of foreign aggression/ cyber war by enemy states and individuals
- Poor system/enterprise architecture designs can create single points of failure and a danger to system availability.
- The confidentiality of data is threatened as one instance of unauthorized access or disclosure can have negative impact of epic proportions.
- The integrity of data is threatened by possible ease of manipulation.
- E-governance makes it easy for criminals to assume identities of unsuspecting persons resulting in identity theft.

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?

I was not directly attacked by ransomware, however I have come across experiences of service interruption as organisations raced to patch their systems so as to increase their resilience against such attacks.

This was a case of indirect/reverse effects.

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

In my experience, increasing user awareness is the one single-most effective strategy/tool to limit impact of ransomware cases. This is because they majorly happen through social engineering.

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

Some organisations are spending a lot of money on combating cyber-crime while others are not. However I firmly believe that what matters is the appropriateness and where or what the money is spent on and not necessarily how much is spent.

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

Increasing awareness of the risk environment will encourage appropriate spending on cyber security issues.

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

In your opinion, what should African countries/universities

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

Attitude change. Africans should believe in and buy African cyber security solutions, starting with governments and corporate bodies.

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?

The private sector and consumers should give the local players a chance to prove themselves. A ready market for the locally developed cyber security solutions will make the sector commercially viable and trigger even more innovation and a beneficial relationship between the solution developers and the consumers.

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

- Talent and capacity development.
- National Defense.
- Money laundering.

Cost of Cyber Crime

Analysis – 2017

IN THIS SECTION, WE LOOK MORE CLOSELY AT THE COST OF CYBERCRIME IN UGANDA, 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 Ugandan businesses around \$42 million a year, which includes direct damage plus post-attack disruption to the normal course of business.



Uganda

Cost of cyber-attacks



\$42m
annually

Methodology

Our assessments are, essentially, based on reported incidents of cybercrime, 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 incidents.

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 \$12,600,000.00 per annum. In all probability, and in line with our worst-case scenarios, the real impact of cybercrime is likely to be much greater. As for measuring costs, this report decomposes the cost based on these 4 categories:

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



\$42m
annually

Type & Cost of
Cyber Crime
in Uganda

Insider Threat



\$12.6m
annually

30%

Attacks on
Computer Systems
(Unauthorized
Access and
Malware)



\$8.4m
annually

20%

Online
Scam



\$4.2m
annually

15%

Email Spam &
Phishing



\$5.04m
annually

12%

Social Engineering
and Identity Theft



\$4.2m
annually

10%

Data Exfiltration



Ransomware



\$2.1m
annually

5%

\$3.36m
annually

8%

Banking & Financial
Services



Government



Telecommunications



\$14.3m
annually

34%

\$10.5m
annually

25%

Other Sectors/
Industries



\$6.3m
annually

15%

\$4.2m
annually

10%

Internet/online
based services



\$3.4m
annually

8%

Mobile based
transactions/
e-commerce/e-
payment



\$3.4m
annually

8%



\$42m
annually

Cost of
cyber crime
Industry/Sector
Analysis in Uganda



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.

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.

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

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 – **Archivus**: 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 – **SimpleLocker**: 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 – **Syngeng**: 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 – **LOcky**: Aggressively spread via spear phishing campaigns and leveraging the Dridex infrastructure.
 2016 – **SamSam/SAMAS**: The threat actors specifically distributed it to vulnerable JBoss servers after vulnerability assessment using JexBoss tool.
 2016 – **KeRanger**: First official Mac OSX-based ransomware. Delivered via a Transmission BitTorrent client and signed with a MAC development certificate, effectively bypassing Apple's GateKeeper security software.
 2016 – **Petya**: Delivered via DropBox and overwrote the MBR (Master Boot Record). Used a fake CHKDSK prompt while encrypting the drive.
 2016 – **Maktub**: Used a Crypter. Performed offline encryption using Windows CryptoAPI.
 2016 – **Jigsaw**: Threatened to delete a file every 60 minutes if the \$150 ransom was not paid.
 2016 – **CryptXXX**: Spread via multiple exploit kits, primarily Angler. Includes ability to monitor mouse activity, Anti-Sandbox detection, custom C2 communication protocols, and payment through Tor.
 2016 – **Zcryptor**: One of the first "CryptoWorms", primarily spread through spam email.
 2016 – **Cerber**: Leverages Ransomware-as-a-Service (RaaS) model whereby malware author nets 40% of paid ransom and affiliates keep 60% via Bitcoin and Tor. Uses RC4 and RSA algorithms for encryption.
 2016 – **Petya**: Infected Master Boot Record (MBR) used by NTFS file systems. Installs a payload that encrypts the file tables the next time the system is booted, essentially blocking the system from booting into Windows until the ransom is paid.
-
- 2017 – **WannaCry**: Rapidly spread through the internet by leveraging the EternalBlue exploit.
 2017 – **NotPetya**: It erases the first sectors of a disk, and although it demands a ransom to be paid, victims have little to no chance of recovering their data even if the ransom is paid as the MBR is completely overwritten and not encrypted like Petya does.



Home 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/Nanny 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 interact with our homes. A number of houses, apartments and estates in Kampala have CCTV surveillance, Smart TVs, DVRs and connected thermostats that you can monitor and handle from any part of the world. These gadgets add convenience like locking your door or shutting off the lights all from a smartphone app, but

they come with certain risks. In October, hackers took over 100,000 IoT devices and used them to block traffic to well-known websites, including Twitter and Netflix.

Home Routers

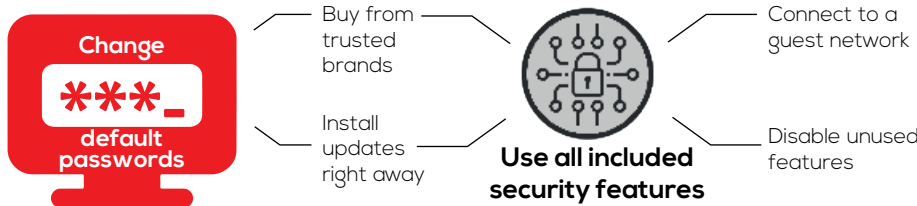
When buying a home router, no consideration is put on the security of these devices. Recent research has shown that your home routers can be used by malicious outsiders to launch attacks against websites belonging to other organisations without your direct involvement.

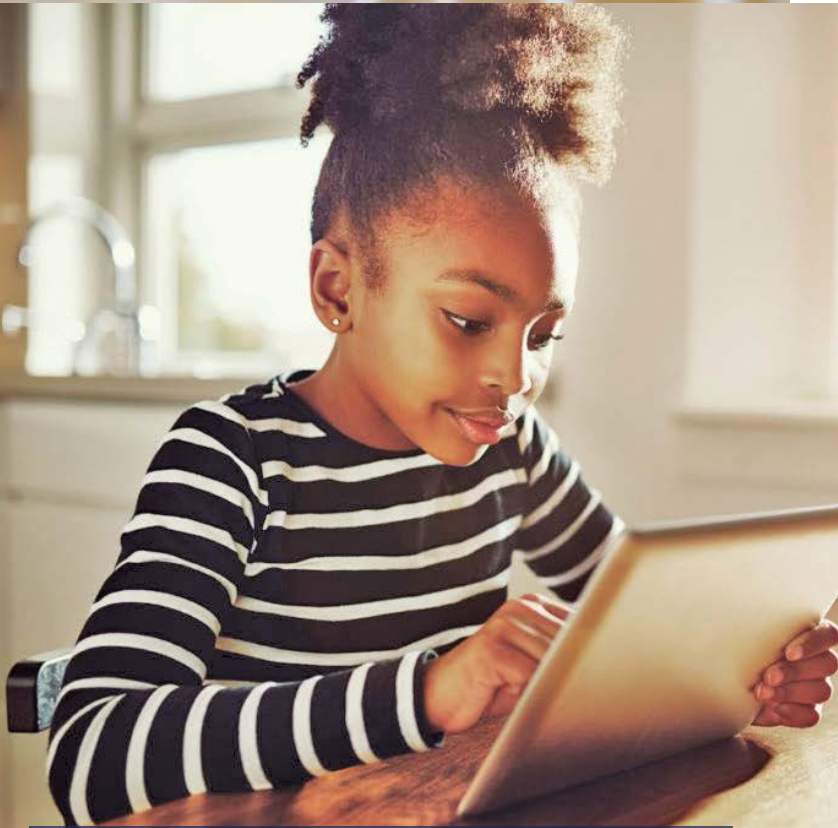
As a home owner, you run the risk of being blocked by certain sites, your internet speed may be slow due to the excessive bandwidth utilization and you will incur higher costs.

Security Begins at Home

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

Security Tips





Securing the Child

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

Teach Yourself

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

Check Privacy Settings

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

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

Get them offline

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

Cyber Bullying

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

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

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

Parents can

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



Top Trends

Fake News: Vulnerability of truth

The inception of Facebook, Twitter and Instagram have revolutionized the way we consume information with SPEED being a key selling point. Individuals now have a constant need to 'be in the know'. Through features like feeds, profiles and groups we get instantaneous access to information from any location.

In 2017 however, these platforms were overwhelmed by rogue politics, misinformation and dubious claims. In 2017, the editors and directors of one of Uganda's most popular tabloid newspapers were detained over what authorities called a fake news story about a political plot implicating the president. The real impact of the growing interest in fake news has been the realization that the public might not be well-equipped to separate truthful information from false information.

It is paramount that governments and social media 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 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.





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

The cost of Cyber crime grew by approximately 20% but the skill gap is widening. No one knows what they're doing, majority of IT and security staff are downloading templates from the internet and applying these in their organisations. From our analysis, a key contributor to this is that organisations tend to look for people with traditional technology credentials – 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's 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's 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

Mobile money transfer is gaining grounds as a fast and easy way to transact business; however criminals try to swindle unsuspecting victims. Our statistics reveal that half of the banking users are using internet banking and three quarters use mobile banking services.

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.

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.



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/ 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 Ugandans try out pyramid schemes with the hope of making huge profit. 2017 saw the Bank of Uganda (BoU), suspend accounts belonging to an online to an sports trading platform which was deemed a

Ponzi scheme - an unlicensed deposit-taking firm.

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. The recent revelations about Cambrige Analytica spring to mind. 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.



ARNOLD MANGENI

Director Information Security
NITA, Uganda

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

Yes.

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

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

The main causes of the cyber security problem are;

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

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

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

Ultimately the NISF seeks to achieve the following amongst others;

- i. Provide a conceptual structure for guiding information security activities
- ii. Provide a common risk based approach for addressing information security issues
- iii. Secure Government of Uganda information and other assets
- iv. Improve understanding of information security risk, roles and responsibilities
- v. Guarantee information security compliance by critical national information infrastructure operators
- vi. Improve information security governance and the environment

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

- i. Governance; Structures must be created to enable people perform specified roles and responsibilities. The first step, thus, is to ensure that organisations create clear structures to enable staff at all levels to perform information security & risk roles effectively.
- ii. Information Security; Organisations must protect both the information they handle internally and that which they share with external partners. Assuring the confidentiality, integrity and availability of information is a corporate-level concern because security incidents threaten organisational reputations, legal positions and the ability to conduct business operations.

- iii. Personnel Security; Employees are the most important asset for any organisation. However, staff could also be potent threat sources and actors. Indeed, changes in national information security policies worldwide have roots in high-profile accidental and deliberate disclosures of sensitive national security and personal information. Therefore, it is vital to reduce the likelihood of staff exploiting legitimate access to critical infrastructure facilities, sites, information and staff for unauthorised use. Personnel security is important in the context of defending the cyber supply chain against State and industrial espionage threats.
 - iv. Physical Security; Managing unauthorised physical access, damage, and interference to information, premises and resources by a range of physical security threats including crime, espionage, natural disasters and acts of terrorism, must be of paramount importance to organisations. Physical security also protects personnel against violence and other sorts of harm.
2. Education, training and awareness sessions are routinely being carried out. Plans are underway to carry out massive nationwide awareness and training for the Financial Year 17/18.
 3. Adoption of the National Cyber Security Strategy (NCSS) which has been drafted following the revision of the National Information Security Strategy (NISS). The NISS was implemented in 2011, to address matters of Information Security. Currently the NISS has been revised to establish the NCSS. The guiding principles for the National Cyber Security Strategy include but are not limited to the following:
 - i. Enhancing private public partnership in development of cyber security capacity;
 - ii. Ensuring trust and confidence of citizens in the use of Information Technology enabled services;
 - iii. Taking into consideration international collaboration due to the borderless nature of cyber space;
 - iv. Promoting a culture of cyber security across all levels of society;
 - v. Promoting continuous improvement in cyber security and;
 - vi. Promoting responsibility and action amongst CII operators as regards Cyber Security readiness.
 4. Utilize the national Computer Emergency Response Team / Co-ordination Center (CERT / CC) (established in 2014) to:
 - i. Ensure the protection of the nation's Critical Information Infrastructures through incident management amongst other measures;
 - ii. Assist in drafting the overall plan on the country's approach to cyber security related issues; and
 - iii. Serve as a focal point for further building and implementing the National Culture of Cyber security.
 5. Make the most out of our international and regional collaboration on cyber security with a number of liked minded organisations and governments. These include; Korea Internet Security Agency (KISA), the Government of Estonia, International Security Forum (ISF), Global Forum on Cyber Expertise (GFCE) , amongst others. Out of these collaborations is skilling of our information security professionals, technical support, information sharing, amongst other benefits.
 6. Maximize the benefits from the National Information Security Advisory Group (NISAG), whose mandate is to advise, protect and respond to the nation's critical infrastructure, we are achieving collaboration with the private sector who run majority of the nation's critical infrastructure. This ensures robust Cybersecurity implementations.

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

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

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

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

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

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

- ii. Hacktivism; activists have increasingly taken to breaking into computer systems demonstrate for political or social causes.
- iii. Industrial Espionage; illegally and unethically obtaining confidential information from competitors with the intention of using the said information to gain a competitive edge.
- iv. State Espionage; State sponsored cyber espionage is becoming a common occurrence and is being used as a form of intelligence gathering.

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

Yes, included among the initiatives is;

- 1. An Enabling legal and Regulatory environment. Included are the cyber laws;
 - a. The Electronic Transactions Act (2011) to make provision for and to regulate the use of electronic signatures, to provide for the use, security, facilitation and regulation of electronic communications and transactions;
 - b. The Electronic Signatures Act (2011) to encourage the use of e-Government and to make provision for the safety and security of electronic transactions and information systems; and

- c. The Computer Misuse Act (2011) to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment.
- 2. National Information Security Advisory Group (NISAG). This NISAG encourages collaboration between public and private stakeholders to ensure robust Cybersecurity is implemented.
- 3. The National Information Security Framework (NISF) with its 6 security standards;
 - a. SS1 - Technical Risk Assessment
 - b. SS2 - Risk Management & Accreditation
 - c. SS3 - Security Classification
 - d. SS4 - Personnel Security
 - e. SS5 - Physical Security
 - f. SS6- Incident Management

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

- 4. Capacity development on the application of the cyber laws for both investigating and prosecuting officers. Application of these cyber laws should be guided by adhering to principles of digital forensics as well as chain of custody.
- 5. Through the CERT/CC Identification and prioritization of key resources is being done. This is aimed at improving the country's security, resilience, operational capacities to effectively manage and respond to cyber incidents as well as protect against ever persistent threats.

- 6. Establishment of the Uganda Police Cyber Crime Unit, whose is to;
 - a. provide enforcement of cyber security related laws
 - b. provide efficient cybercrime investigation
 - c. ensure collaboration with similar international institutions

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

Yes

Were these cases reported to government authorities and prosecuted?

Yes.

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

Some Notable case below:

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

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

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

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

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

- Enabling environment. Enact laws and regulations to comprehensively address Cyber issues. This should



be reinforced with awareness and support through initiatives like capacity building for investigating, prosecuting and judicial officers.

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

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

- Banking and Financial Services
- Telecommunication
- Government

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

- African states need to work closely and directly through the African Union and other regional frameworks to implement enhanced measures for cooperation, mutual assistance and coordination among security agencies, prosecutors and judges.

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

Sector Ranking

CYBER SECURITY IS NO LONGER A CONCERN FOR THE FINANCIAL AND BANKING SECTORS ONLY. AS THE ADOPTION OF INTERNET USE AND AUTOMATED SERVICES INCREASES ACROSS ALL INDUSTRIES, CYBER SECURITY COMES ALONG AS PART OF THE PACKAGE. IN UGANDA, 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.



Banking

Amidst the current climate of major data breaches, banking institutions in charge of vast volumes of valuable financial data are under increasing pressure to keep customer data safe from hackers and fraudsters. In 2017, we saw attackers leverage weaknesses found in the Automated Teller Machines (ATMs), Mobile applications and core banking misconfigurations to steal money from the banks. More advanced attacks in banks mostly perpetrated by insiders are raising the concerns that the banking sector in Uganda is unprepared to deal with insider threats.



Mobile Money

2017 has seen an explosion of mobile money services with integrations into numerous platforms such as banking, insurance and e-commerce, among others. A report by Bank of Uganda (BoU) ascertained that the annual amount of money transferred through mobile money totaled US\$ 43.83tn in 2016, up from US\$ 32.7tn in 2015. BoU said the volume of transactions also increased by 40.5 per cent to 974.7 million in 2016 from 693.3 million a year before. Unfortunately, the adoption of these technologies has not been supplemented by secure controls, with most mobile money applications lacking basic security controls such as encryption of data.



E-Commerce

E-commerce has exploded in the recent past in Uganda due to the widespread use of mobile money and e-commerce sites such as Jumia, Amazon, OLX on which Ugandan entrepreneurs advertise and sell their merchandise. These sites have attracted a new breed of online scammers and online fraudsters who are now preying on online shoppers.

Uganda's Ranking on
**ITU Global Cybersecurity Index
& Cyber Wellness Profiles**



**SACCOs,
Microfinance
and
Cooperatives**

SACCOs and Cooperatives in Uganda are quickly gaining large customer base and great transactional amounts due to their competitive rates compared to larger financial institutions. This has led them to automate their processes in an effort to manage their growing scope. This uptake has led to increased exposure to technology based fraud risks.



**Hospitality &
Retail**

The hospitality industry is primarily client facing and as such deals with a great deal of sensitive customer information from reservation details, payment, travel and customer information collected from multiple systems. 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.



Telecommunications

The telecommunications industry in Uganda handles large amounts of confidential customer data – phone numbers, names, ID numbers. Additionally they provide supporting infrastructure for organisations to transmit sensitive information. As a result, the threat map and cyber-attack vectors have increased with attackers leveraging attacks such as SIM swap and identity theft. Efforts in place to minimize the risk include the initiative by Uganda Communications Commission (UCC), in April 12, 2017 to compel all mobile phone subscribers to be registered. Even with these efforts, it's still clear that the risks facing the telecommunications industry are vast and that attackers are continuously discovering new ways to exploit them.

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 external IP
- Multiple posting on DB
- Remote Access tool detected
- Auditory disabled

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

- Logs deleted
- System unavailable
- AV disabled

KEY SYSTEMS



Firewall



Antivirus



Active Directory



ATTACK STAGES



RECONNAISSANCE



GAINING ACCESS

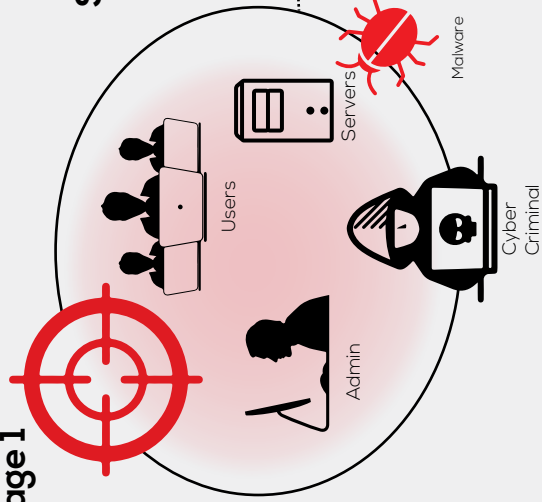


ATTACK



HIDE TRACKS

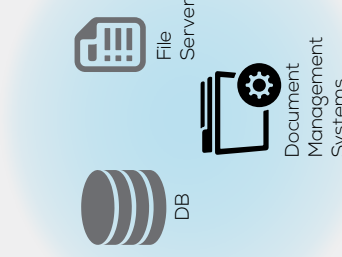
Stage 1



Stage 2

Gaining Access

- Admin credentials
- Customer account



Stage 3

Attack

Social Engineering and Identity Theft



Stage 4

Hide Tracks

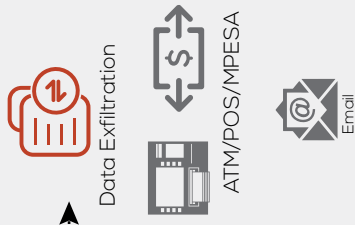
Erasing logs to remove evidence



Clean PC



Sending money to multiple recipients



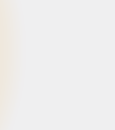
Malicious DB Manipulation



Server



Web Defacement



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.

Domains of the Africa Cyber Security Framework



Ministry of Finance website hacked, again

MINISTRY OF ICT AND NATIONAL GUIDANCE | REPUBLIC OF UGANDA
UGANDA MEDIA CENTRE

30 March 2017 Uganda Business News

Equity Bank Uganda Ponzi scheme

FRIDAY JUNE 16 2017

Uganda still regarded a high-risk nation for Cyber-attacks

Cyber Attack: Uganda Ranked 7th Highest Risk Country Globally

Business Focus Reporter June 27, 2017

Museveni to make presentation on impact of 'fake news on national security

FAKE NEWS national security MEDIA COVERAGE & NATIONAL SECURITY

438,692,102 Articles • 2,718,449 Readers

parts of the country were left in tears after being robbed of their hard-earned money in a fake electronic fraud scam by businessman Ronald Muramuzi. However, latest info reaching us has it that there is a new Brazilian company owned by an investor only identified as Sergio has joined the Ugandan electronic business market and is ... (continue reading)

Foreign hackers expand frontiers as fake News on the Rise in Uganda's Mainstream Media!

English En Français

BY ALLAFRICA

Uganda: Two Arrested for Hacking Into Centenary Bank Accounts

Uganda: All Not So Quiet On the Business Crime Slowly Takes Shape

Bank of Uganda warns of Cyber-attacks on commercial Banks

Makerere system hacked, 50 students deleted from 2017 graduation list

The expensive lifestyle of the Ugandan hacker who was arrested for attempting to hack into MPesa and IEBC computer systems (Photos)

Countries Topics Development BizTech Entertainment Sport Africa/World Governance

Uganda: All Not So Quiet On the Business Crime Slowly Takes Shape

Tagged: Business • East Africa • ICT • Legal Affairs • Uganda

FRIDAY APRIL 7 2017

Cyber Attack: Uganda Ranked 7th Highest Risk Country Globally

Business Focus Reporter June 27, 2017

Uganda still regarded a high-risk nation for Cyber-attacks

By Admin Added 23rd November 2017 02:03 PM

DFCU Banking System Hacked

By Our Reporter Posted on October 26, 2017

WORLD NEWS REPORT

Breaking News

Brazilian Investor Operates Cyber Scam In Uganda

A few years ago, Ugandans in Kampala and other parts of the country were left in tears after being robbed of their hard-earned money in a fake electronic fraud scam by businessman Ronald Muramuzi. However, latest info reaching us has it that there is a new Brazilian company owned by an investor only identified as Sergio has joined the Ugandan electronic business market and is ... (continue reading)

Uganda still regarded a high-risk nation for Cyber-attacks

By Admin Added 23rd November 2017 02:03 PM

Bank of Uganda warns of Cyber-attacks on commercial Banks

Uganda: Two Arrested for Hacking Into Centenary Bank Accounts

News on the Rise in Uganda's Mainstream Media!

FRIDAY JUNE 16 2017

Equity Bank Uganda freezes Ponzi scheme's account

Uganda: All Not So Quiet On the Business Crime Slowly Takes Shape

Tagged: Business • East Africa • ICT • Legal Affairs • Uganda

FRIDAY APRIL 7 2017

Detectives link Ugandan Ronnie Nsale to IEBC hacking

Uganda: All Not So Quiet On the Business Crime Slowly Takes Shape

Tagged: Business • East Africa • ICT • Legal Affairs • Uganda

FRIDAY APRIL 7 2017

Cyber Attack: Uganda Ranked 7th Highest Risk Country Globally

Business Focus Reporter June 27, 2017

Uganda still regarded a high-risk nation for Cyber-attacks

By Admin Added 23rd November 2017 02:03 PM

WORLD NEWS REPORT

Breaking News

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 Prof[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	Yes	Yes	Yes		Yes					
Navicat	Proprietary	Yes	Yes		Yes	Yes	Yes	Yes	Yes		Yes
Navicat Data Modeler	Proprietary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes
Oracle Enterprise Manager	Proprietary	Yes	No	Yes	Yes	Yes		Yes			
Oracle SQL Developer	Proprietary	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	
Orbada	GPL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
pgAdmin III	PostgreSQL License	Yes	Yes	Yes							
pgAdmin4	PostgreSQL License						Yes				
phpLiteAdmin	GPL	Yes	Yes	Yes	No	No	No	No	No	No	Yes
phpMyAdmin	GPL	Yes	Yes	Yes		Yes					
SQL Database Studio	Proprietary	Yes	No	No	No	No	No	Yes			
SQLyog	GPLv2	Yes				Yes					
Squirrel SQL	GPLv2 & LGPLv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TablePlus	Proprietary	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes
Toad	Proprietary	Yes	No	No	Yes	Yes		Yes	Yes		
Toad Data Modeler	Proprietary	Yes	No	No	Yes	Yes	Yes	Yes			
Tora	GPL	Yes	Yes	Yes	Yes	Yes	Yes				

Remote Access tools for Endpoints

Software	Protocols	License	Free for personal use	Free for commercial use
AetherPal	Proprietary	Proprietary	No	No
Ammy 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
Pliixo 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
Techniline	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
Uterius	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	Uterius (VNC)	BSD	Yes	Yes
x2x	X11	BSD	Yes	Yes
Software	Protocol	License	Free for personal use	Free for commercial use

List of Open Source Tools

Vulnerability Scanners

1. OpenVAS

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

2. Retina CS Community

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

3. Microsoft Baseline Security Analyzer (MBSA)

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

4. Nexpose Community Edition

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

5. SecureCheq

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

6. Qualys FreeScan

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

References

Top Attacks

- <http://theugandan.com.ug/makerere-system-hacked-50-students-deleted-from-2017-graduation-list/>
- <https://www.nita.go.ug/media/cyber-threat-horizon-uganda-2016>
- http://www.newvision.co.ug/new_vision/news/1328415/uganda-sets-unit-fight-cyber-crime
- http://world.einnews.com/article__detail/region/east-africa/392702819-brazilian-investor-operates-cyber-scam-in-uganda?vcode=Qg-r
- <http://mbararaneews.co.ug/bank-uganda-hacked-try-steal-sh2-45bn/>
- <https://www.databreaches.net/ug-key-data-stolen-from-main-government-registry/>
- <http://allafrica.com/stories/201609050130.html>
- <http://www.chimpreports.com/uganda-finance-ministry-website-hacked/>
- <http://blog.mondato.com/mobile-money-hack/>
- <http://theinsider.ug/index.php/2017/10/26/dfcu-banking-system-hacked/>

Cyber Intelligence

- <https://www.csoonline.com/article/3191531/network-security/securing-risky-network-ports.html>

Top Attacks in Uganda

- <https://www.nation.co.ke/news/-Ronnie-Nsale-to-Safaricom-and-iebc-hacking/1056-3880474-bp6l44z/index.html>
- https://www.newvision.co.ug/new_vision/news/1466266/uganda-regarded-risk-nation-cyber-attacks
- <http://ugbusiness.com/3035/ministry-of-finance-website-hacked-again>
- <https://www.pressreader.com/kenya/the-east-african/20170805/282170766236687>
- <http://allafrica.com/stories/201704140593.html>

<https://guru8.net/2017/05/bank-uganda-warns-cyber-attacks-commercial-banks/>

<https://www.pressreader.com/kenya/the-east-african/20170805/282170766236687>

<http://theugandan.com.ug/makerere-system-hacked-50-students-deleted-from-2017-graduation-list/>

http://world.einnews.com/article__detail/region/east-africa/392702819-brazilian-investor-operates-cyber-scam-in-uganda?vcode=Qg-r

<https://www.standardmedia.co.ke/article/2001261018/ugandan-editors-arrested-over-fake-news-on-alleged-uganda-rwanda-tension>

Risk Ranking

<http://www.theeastafrican.co.ke/business/Cyber-crime-hits-businesses/2560-3889460-fuhqw9z/index.html>

<https://cipesa.org/2017/04/recent-developments-in-telecoms-regulation-threaten-online-rights-in-uganda/>

<https://www.scmagazineuk.com/uganda-and-malawi-sign-pact-to-fight-cybercrime-and-build-capabilities/article/638441/>

Appendix

Open Source tools: <https://www.networkworld.com/article/2176429/security/security-6-free-network-vulnerability-scanners.html>



