2018

Africa Cyber Security Report - Uganda

SERIANU

Cyber Security Skills G ap

United States International University-Africa

ISACA
Trust in, and value from, information systems

Serianu Cyber-Threat Command Centre
SC3
Anticipate • Detect • Respond • Contain

Africa Cyber Immersion Centre
acic
Engage | Educate | Empower

CYBOTA INTEL
Africa's Cyber Threat Sharing Platform

Milima Technologies

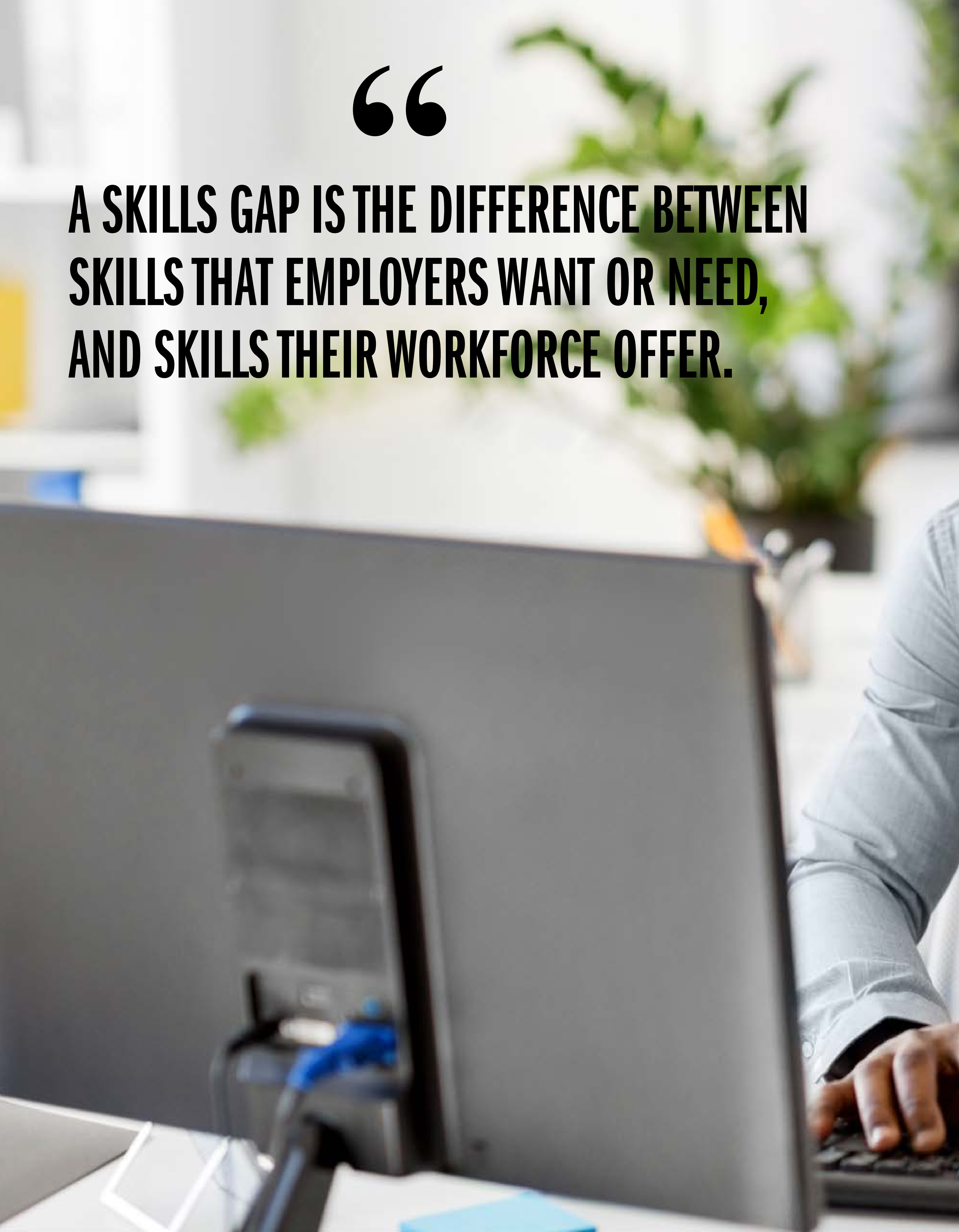
SERIANU

2018

Africa Cyber Security Report - Uganda

Cyber Security Skills Gap

“A SKILLS GAP IS THE DIFFERENCE BETWEEN SKILLS THAT EMPLOYERS WANT OR NEED, AND SKILLS THEIR WORKFORCE OFFER.



IN THIS REPORT

EDITOR'S NOTE AND ACKNOWLEDGEMENT

Brencil Kaimba
Editor-in-chief and Cyber Security Consultant,
Serianu Limited

We are extremely pleased to publish the 2nd Edition of Uganda 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 and Cyber security skills gap. Over the last 6 years, we have consistently strived to demystify the state of Cyber security in Africa. In this edition themed Africa's Cyber Security Skills Gap, we take a deeper look at the limited technical skills, and financial limitations impacting many Ugandan organisations. Our research is broken down into the following key areas:

Top Trends: We analysed incidents that occurred in 2018 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.

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

Survey Analysis: This section analyses the responses we received from over 1000 organisations surveyed across Africa. It measures the challenges facing Ugandan organisations, including low Cyber security budgets and inadequate security impact awareness that eventually translates to limited capabilities to anticipate, detect, respond and contain threats.

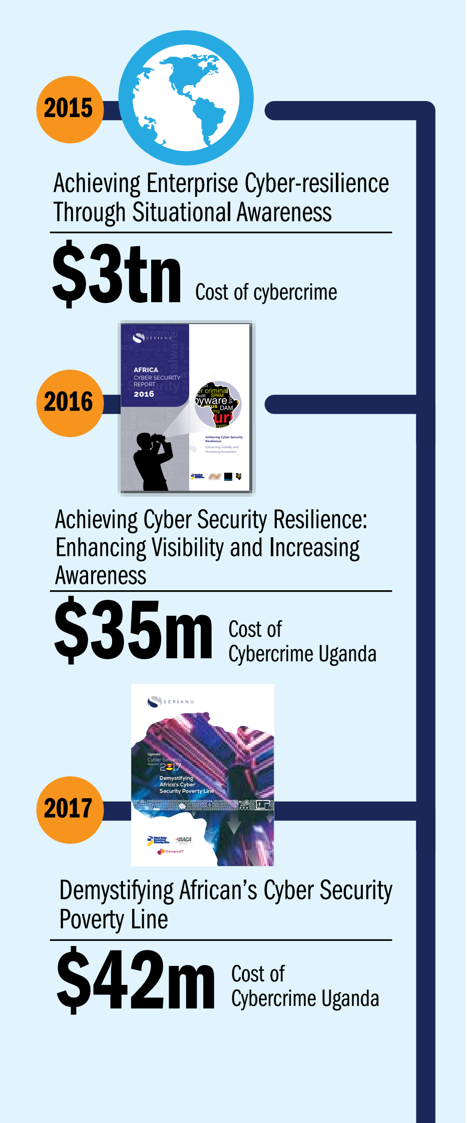
Skills Gap Analysis: This section analyses the key skills gap challenges within Ugandan organisations such as, top challenges faced when recruiting skilled cybersecurity professionals, length of time it takes to fill a cybersecurity role, the importance and relevance of certifications etc. We analyzed responses from HR executives, CIOs and training managers.

Gender Gap Analysis: This section analyses the gender gap challenge issues within Cybersecurity. Key question being, is Cybersecurity failing to attract women. Another concept discussed on the technical capabilities of women to handle tech roles. Are women more "Around" tech than "in" tech?

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

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

Cyber-risk Visibility and Exposure Quantification Framework (CVEQ Framework): Organisations are now required to quantify their Cyber risk and articulate their Cybersecurity exposures. In this section, we highlights metrics that organisations need to focus on in order to fully quantity, monitor and track their Cybersecurity posture and performance.


2015
Achieving Enterprise Cyber-resilience Through Situational Awareness
$3tn Cost of cybercrime
2016
AFRICA CYBER SECURITY REPORT 2016
Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness
$35m Cost of Cybercrime Uganda
2017
SERIANU
Demystifying Africa's Cyber Security Poverty Line
Demystifying African's Cyber Security Poverty Line
$42m Cost of Cybercrime Uganda

WHAT CAN WE LEARN FROM BREACHES/NEW THREATS THAT HAVE EMERGED?

Going by our 2018 observations, it is clear that African threats are unique to African organisations. Incidences that were widely reported such as malware samples, attack vectors including mobile money compromise and SIM Swap frauds, are unique to the continent. It is important to note that, since most of the attacks are replicated from one organisation to the other, it is important for executives in charge of cyber security to share information.

EXPECTATIONS FOR 2019

For as long as the attack tactics remain effective, we anticipate that 2018 trends will continue in 2019. This is both in-terms of cyber-attacks and cyber defense tactics. Organisations will continue to focus on training their users, enhancing in-house technical capabilities for Anticipating, Detecting, Responding and Containing cyber threats.

- Board members will become more proactive and there will be a need to streamline Cyber risk reporting and quantification.
- Vendors will be expected to communicate and show value for their services in a quantifiable manner.
- Attackers will continue to engineer unique malware
- Regulators will develop stronger cybersecurity policies
- Third party firms, such as vendors and vulnerable systems, will be weak links, forming a primary access compromise point that needs to be checked thoroughly.
- Malware attacks are expected to rise, especially locally developed or re-engineered viruses.
- We also anticipate other industries will rise to the occasion and develop their own specific cyber security guidelines, just as the financial services sector has done.
- Since the skills gap is yet to narrow, outsourcing will continue.

01

DID YOU KNOW?

AS TECHNOLOGY CONTINUES TO EVOLVE SO ALSO DO THE OPPORTUNITIES AND CHALLENGES IT PROVIDES. WE ARE AT A CROSSROADS AS WE MOVE FROM A SOCIETY ALREADY ENTWINED WITH THE INTERNET TO THE COMING AGE OF AUTOMATION, BIG DATA, AND THE INTERNET OF THINGS (IOT).

ACKNOWLEDGEMENT

In developing the Africa Cyber Security Report 2018 - Uganda Edition, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;

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

The ISACA-Kampala 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-Kampala chapter members.

We partnered with Milima Technologies, an Information Security company focused on offering innovative and holistic top-down trainings and audits for organisations. Milima Technologies provided immense support through research and provision of statistics, survey responses, local intelligence on top issues and trends highlighted in the report.

The Serianu CyberThreat Intelligence Team

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

CO-AUTHORS

Barbara Munyendo - Researcher, Cyber Intelligence
Margaret Ndungu - Researcher and Editor
Nabihah Rishad - Researcher, Framework
Salome Njoki - Researcher, Trends
Brilliant Grant - Researcher, Trends
Ayub Mwangi - Data Analyst
Collins Mwangi - Data Analyst
Daniel Kabucho - Data Analyst
David Ochieng' - Data Analyst
Joseph Gitonga - Data Analyst
Sheila Nyambura - Data Analyst
Vionna Muriithi - Data Analyst

OTHER CONTRIBUTORS

Kevin Kimani
Martin Mwangi
Jeff Karanja
Daniel Ndegwa
Jackie Madowo
Bonface Shisakha
Samuel Momanyi

Samuel Keige
Stephen Wanjuki
George Kiio
Morris Kamethu
Jerome Okot
Joy Naeku

USIU TEAM

Onyibe Shalom Osemeke
Zamzam Abdi Hassan
Jamilla Kuta
Bryan Mutethia Nturibi
Khushi Gupta
Adegbemle Folarin Adefemi
Peter Kamande Numi

COMMENTARIES

William Makatiani
CEO, Serianu Limited

International Data Corporation (IDC)

Emmanuel A. Chagara
CEO, Milima Technologies | Milima Cyber Academy

Arnold R. Mangeni
Director of Information Security, NITA

Noah Balesanvu
National Information Security Advisory Group, NISAG

Kenneth Muhangi
Partner, KTA Advocates

Christine Masika
Digital Forensic Analyst, Applied Principal Consulting

Joseph Mathenge
Chief Operations Officer, Serianu Limited

Nabihah Rishad
Sr. Risk Consultant, Serianu Limited

Building Data Partnerships

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

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

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

Design, Layout and Production: Tonn Kriation

Disclaimer

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

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

For more information contact:

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

FOREWORD

In the wake of the fast evolving cyber-threat landscape, the looming cybersecurity skills gap has become an industry crisis. With little capacity to match the massive losses being recorded across all tiers of the economy, efforts to close the skills gap should be collaborative and intentional. However we can not address a problem whose magnitude we can't fully comprehend; This is why Milima Technologies Uganda partnered with Serianu Kenya to bring to light the depth of cybersecurity skills gap in Uganda in this 6th edition of the Africa Cybersecurity Report – Uganda Edition.

Uganda has continued to witness increasing cases of cyber-crime and in this report, you will get to appreciate selected cases that came to light. There are many more that go unreported. The truth is many organisations are struggling to keep up with new attack techniques, free and available hacking tools that don't require special hacking acumen. Financial institutions continue to be top targets followed by government institutions. The incapacity of these organisations through ill-equipped personnel to detect, assess, contain and respond to attacks continues to be a major bottleneck. Some of the notable reasons for the mismatch are;

Preference for certifications over practicality. Due to the job market demand, the few experts who are being put incharge of systems are more inclined towards accumulating certification papers as opposed to developing practical and dependable cybersecurity skills. In the event of an attack, these experts are barely able to respond or contain the crisis. Over-dependence on tools; More organisations are dealing with pressures to beef up security on their infrastructure and the best way they know how is through deployment of more and more security solutions. Whereas this has many benefits, no vendor will tell you the down-side of their system. These solutions are in-turn providing a false sense of security which unfortunately many organisations have fallen for. These are the same organisations that have continued to experience growing incidents. Poor research culture; A poor research culture will always catch up with a professional. This is being witnessed across many organisations who have put little emphasis on staff development and research. Lack of research means staying in the shadows as a zero-day exploit is being released for your most critical assets; It means having no knowledge of released patches for your most valuable systems. Without research we stand no chance against the bad actors.

Shortage of Training Centers; Lack of training centers has been a major cause for the looming cybersecurity skills gap. This also explains why at Milima Technologies we had to launch a cybersecurity training arm, Milima Cyber Academy, to support in bridging the wide skills gap. More institutions and training centers will need to be setup if we are to match the fast growing demand for cybersecurity experts.

As more and more business go online, more data, more digital footprints and henceforth more sophisticated cyber-attacks will unravel. It's only wise that we brace ourselves for the long haul. We have a big job ahead of us and we need every hand we can get to build resilience across all tiers of our economy.

“

THE TRUTH IS MANY ORGANISATIONS ARE STRUGGLING TO KEEP UP WITH NEW ATTACK TECHNIQUES, FREE AND AVAILABLE HACKING TOOLS THAT DON'T REQUIRE SPECIAL HACKING ACUMEN. FINANCIAL INSTITUTIONS CONTINUE TO BE TOP TARGETS FOLLOWED BY GOVERNMENT INSTITUTIONS. THE INCAPACITY OF THESE ORGANISATIONS THROUGH ILL-EQUIPPED PERSONNEL TO DETECT, ASSESS, CONTAIN AND RESPOND TO ATTACKS CONTINUES TO BE A MAJOR BOTTLENECK.

Emmanuel A. Chagara
C.E.O, Milima Technologies |
Milima Cyber Academy

EXECUTIVE SUMMARY

Welcome to the 2nd edition of the Cyber Security Report. Each year, we tackle key themes that capture the spirit of core matters that the industry needs to address to make progress. This time, we are highlighting the need to raise our collective level of training, upgrade certification and even more crucial, build the new talent pipeline by actively skilling high school and technical institution students.

Just as the sun will rise from the east and set in the west daily, the demand for cyber security professionals will continue to grow, largely driven by the degree with which both the public and private sectors have continued to embrace the use of information and communication technology (ICT). Even though ICT is evolving rapidly and organisational leadership is raising the priority given to cyber security risk, a lot more still needs to be done to empower professionals.

Our take, is that there is a higher focus on certification than skills acquisition. The first is theoretical; the second is gained by practice. While certification is highly encouraged for formal employment, we need to build a pool of professionals that have a balance with skill in order to strengthen the overall capability to deal with emerging cyber security threats. This report shows that cyber security losses have been mounting annually, over the past six years.

We estimate that today, Uganda needs at least 3,000 cyber security professionals to keep abreast with the number of organisations in need of this critical skill, yet we have observed that each year, just about 50 new personnel join the market. In another five years, going by the current rate of technology uptake, we anticipate that the country will need at least 30,000 cyber security professionals.

To refine their capability further, Serianu has summarized the skill needs in three broad categories i.e. understanding, attribution and deterrence.

Understanding refers to the need to have a broader perspective of the events that are happening and tools being used, while attribution covers pin pointing the perpetrators. It is only then that can deterrence take place, because by now the perpetrators are known. Backed by the law, it is then easier to enforce regulations. A structured approach to assessing and addressing the cyber security landscape shows us our collective primary areas of focus.

This way we will begin to actively narrow the cyber security skills gap, a factor that we have established plays an enormous role in the whole industry's need to strengthen organisational cyber security. Fortunately, the solutions are now available locally, integrating modern, state- of -the -art facilities for on job practical training manned by a pool of highly experienced trainers.

3 CRITICAL ISSUES ORGANISATIONS ARE GRAPPLING WITH

CYBER UNDERSTANDING

IS THE PROCESS OF CONTINUOUSLY MONITORING AND DETECTING NETWORK ACTIVITIES TO BETTER UNDERSTAND ACTIVE THREATS IN THE ENVIRONMENT.

CYBER ATTRIBUTION

IS THE PROCESS OF EXAMINING FORENSIC EVIDENCE AND IDENTIFYING THE ACTUAL/REAL PERPETRATORS OF AN CYBER CRIMINAL ACTIVITY.

CYBER DETERRENCE

REFERS TO THE PROCESS OF DISCOURAGING CYBER CRIMINALS FROM CARRYING OUR CYBER ATTACKS THROUGH INSTILLING DOUBT OR FEAR OF THE CONSEQUENCES.

William Makatiani
CEO, Serianu Limited

2018 HIGHLIGHTS

400 Cyber Security Skilled Professionals in Uganda

Skills shortage at senior management and mid management levels

70% of Companies to face talent shortage of Cybersecurity professionals in 2019

Constraint when recruiting Cybersecurity professionals

1. Lack of solid experience
2. High remuneration rates

Increase in organisational spend in cybersecurity in 2017 to 2018

25% of respondents spend above $10000

$52M cost of cybercrime in Uganda in 2018

15% ↑ reported Cyber crime incidents to the police

5% ↑ successfully prosecuted Cyber crimes

Locally engineered malwares are on the rise ↑

↑ Increased targeted ATM attacks

↑ Increased Targeted Phishing Attacks

50% ↑ Increased involvement of Board members on matters cybersecurity

TOP TRENDS FOR 2018

Over 2018 the Serianu Cyber Intelligence team has seen a number of trends develop which may impact your organisation's operations and exposure to cyber risk as summarized below:

MALWARE ATTACKS

Malware keeps going from worse to worse. In 2018 we encountered dangerous malware such as Emotet also dubbed (Payments.xls), Trickbot, and Zeus Panda. Our research team identified unique variants of these malwares. Criminals are increasingly tweaking malwares and banking trojans to better target organisations. Global malwares such NSA malware and shadow brokers are now being deployed in Africa.

A close relative of banking malware is crypto mining malware. The rise of Bitcoin and other cryptocurrencies such as Neo, Etheurium etc. took Ugandans by storm. Hackers are placing crypto mining software on devices, networks, and websites at an alarming rate. The impact of these attacks being:

- Financial Impact - drives up the electric bill.
- Performance Impact: slows down machines.
- Maintenance Impact: Detrimental to the hardware as the machines can burn out or run more slowly.

From our survey, crypto miners are targeting popular Ugandan manufacturing, educational and financial institutions, installing these crypto miners on core servers and user endpoints.

In order to prevent such exploitation it is critical that enterprises employ a multi-layered cybersecurity strategy that protects against both established malware cyber-attacks and brand new threats.

CYBER SECURITY SKILL GAP

One of the major trends pointed out last year was the lack of local cybersecurity skillsets in Ugandan organisations. With the cost of cybercrime increasing every year across Uganda, this is still a challenge to the nation.

From our analysis, we identified this skill gap comes from two major sources. Few skillsets in the nation and an inability for companies to have a proper cybersecurity team and strategy. With the number of SMEs and large organisations in the country facing cyber security threats, compared to the number of certified security professionals in Uganda - 400 it is clear that businesses are an easy target for both local and international hackers. Some companies in Uganda who hire security skillsets fail to understand the strength of the skillsets hence confer all roles to an individual. For example, an IT administrator with little or no training on security is conferred the role of the security engineer in an application development company.

01

DID YOU KNOW?

EMOTET IS

- A BANKING TROJAN
- EVADES TYPICAL SIGNATURE-BASED DETECTION
- SPREADS THROUGH EMAILS OR LINKS

EMOTET INFECTIONS HAVE COST STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS UP TO $1 MILLION PER INCIDENT TO REMEDIATE.

US-CERT

400

Cyber Security Skilled Professionals in Uganda

02

DID YOU KNOW?

3RD PARTY API INTEGRATION SERVICE PROVIDERS ARE A LUCRATIVE TARGET FOR HACKERS DUE TO THE VAST AMOUNT OF TRANSACTION AND DATA THEY PROCESS.

> WHEN A COMPANY GIVES 3RD PARTIES ACCESS TO ITS DATA AND SENSITIVE INFORMATION, THE COMPANY IS STILL RESPONSIBLE AND LEGALLY LIABLE FOR THAT INFORMATION.
>
> MARGARET NDUNGU, RISK CONSULTANT

Our analysis also discovered that Ugandan companies are reluctant to develop the skillsets of their security team through frequent trainings and certifications. This is due to the fact that information security is information security is still seen as an expense rather than a return on investment. This is where organisations fail to understand that their team's posture should be proactive against constant and evolving new threats.

Third Party Exposure

Outsourcing enables organisations to focus on their core business. However, this relationship is often based on Service Level Agreements and TRUST. However, that third party trust must be earned. Examples of third party vulnerabilities include:

- Compromise of vendor accounts through key loggers
- Collusion of vendor staff and malicious hackers
- Intentional system compromise by vendors (deletion of database, turning off CCTV, firewall misconfiguration etc)

How to reduce exposure?

- Maintain primary control over who has access, and at what level, to network systems (especially production systems).
- Monitor vendor access (especially remote access) within the network 24/7.
- Get your own house in order by ensuring that physical, internal and operational security controls are in place to secure data that may be accessed by external vendors.

SIM SWAP

SIM swap has become a lucrative enterprise in Uganda particularly because of the increased adoption of mobile money services and mobile number based authentication.

Attackers gather enough information on a target such as ID details and Pin numbers etc through confidence tricks they create a false identity. Using this information, the attackers then contact the service provider and request for a SIM card replacement and thereafter start transacting using your phone number. With the rise of internet and mobile banking attackers can easily access your bank account and transfer money to parallel malicious accounts that they have created. The attacker can can empty your mobile money and bank funds and transfer all your bonga points!

That said, there are number of ways to combat SIM fraud:

- Introducing additional checks for SIM reissuing such as voice recognition and security questions.
- Introducing User behavioral analysis (UBA) especially for financial institutions to monitor for key indicators of compromise and alert the customers.
- Adopting the IMSI (International Mobile Subscriber Identity) — a unique number associated with a specific GSM phone — to ensure one-time use codes are sent only to legitimate subscribers.
- Mobile phone users can check whether their SIM card number and IMSI are the same. If there is a discrepancy, your bank could contact you by email or landline to check.

- Users should also exercise due diligence whereby they check-in with their ISP regularly to validate if any SIM cards have been issued without their knowledge.

POVERTY AND UNEMPLOYMENT RATES

Uganda has a high unemployment rate amongst the youth aged 24 to 30. This acts as a driver for professionals out of work to look for other income streams that are illegal.

Additionally disgruntled employees are the biggest threat in cybersecurity.

BRING YOUR OWN DEVICES (BYOD)

With the changing trends in the use of technology, most people are always online. Devices such as personal mobile phones, tablets and laptops inevitably find themselves connected to the an organisation's network. These devices have become the weakest link and one such infected device, could spread malware across the organisation's internal network, cause losses worth millions in finances and data.

FAKE NEWS

The near instantaneous spread of digital information means that some of the costs of misinformation may be hard to reverse and difficult to respond to, especially when confidence and trust are undermined. WhatsApp is seen as the most used platform to disseminate fake news.

INSTANCES OF FAKE NEWS

1

During the Ebola outbreak in Congo, it was also reported that there was a similar outbreak in Uganda whereas there was only one reported case in Kasese, located in the country's west.

2

After the terrorist attack at Dusit d2 Hotel along 14 riverside Drive in Westlands, Nairobi, reports were made on social media of an impending terrorist attack in Uganda in the coming days which of course were falsified.

The real impact of the growing interest in fake news has been the realization that the public might not be well-equipped to tell the difference between true and fake information.

Modern technology gives fraudsters the fuel and platforms to instantly access millions of people.

The tech industry can and must do better to ensure the internet meets its potential to support individuals' wellbeing and social good. It should use its intelligent algorithms and human expertise to glean and clean out such information as it is uploaded.

03

DID YOU KNOW?

IN 2018, AT LEAST 17 COUNTRIES APPROVED OR PROPOSED LAWS THAT WOULD RESTRICT ONLINE MEDIA IN THE NAME OF FIGHTING "FAKE NEWS" AND ONLINE MANIPULATION.

FREEDOMHOUSE.ORG

> TARGETED AND CALCULATED NEGATIVE REPORTING ABOUT THE BANKING SECTOR HAS THE POTENTIAL OF UNDERMINING CONFIDENCE IN THE INDUSTRY AND RISKS TRIGGERING UNDESIRED PANIC WITH UNINTENDED ADVERSE CONSEQUENCES FOR THE ECONOMY

STATEMENT BY UGANDA BANKERS ASSOCIATION

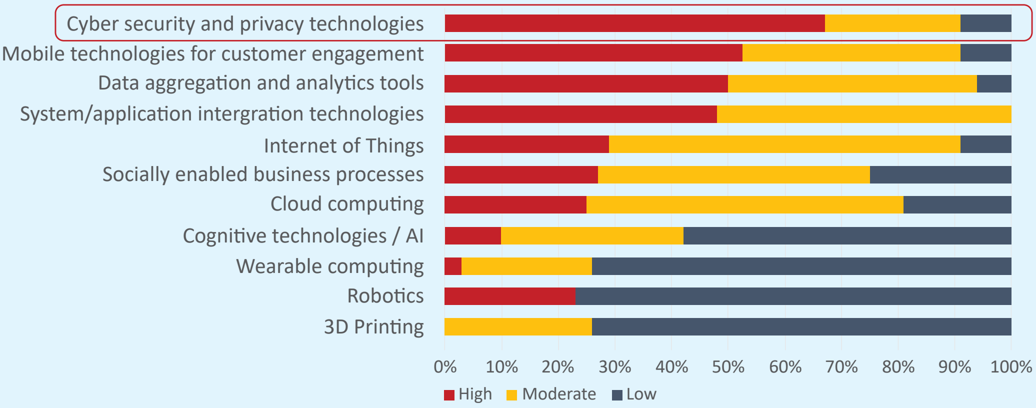
INDUSTRY PLAYER PERSPECTIVE

SUB SAHARAN AFRICA IT SECURITY LANDSCAPE AND TRENDS 2018-2019

SECURITY OUTLOOK 2019

- Breaches will continue to outpace spend.
- Threats will evolve faster than enterprise security.
- Security spending will be frequently misaligned with business needs and unrealistic risk mitigation
- Security awareness and skills remain a significant challenge across all organisations
- Increased adoption of cloud based security solutions and security managed services
- Emerging technologies will be disproportionately vulnerable and targeted
- Early uptake of advanced security solutions such as artificial intelligence security tools for behavioral analytics

CIO PERSPECTIVES OF IT SPENDING AND FOCUS



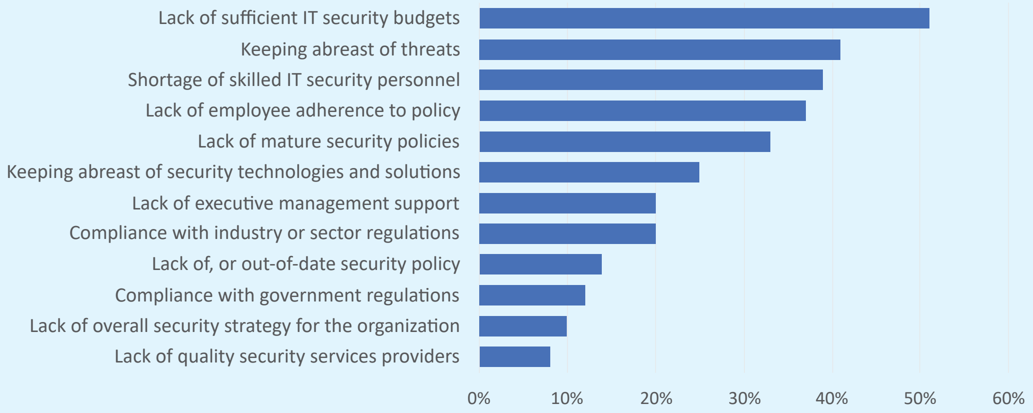
SOURCE 1: IDC

According to IDC's annual CIO Survey 2018, cyber security and privacy technologies rank the highest in importance for organisations looking at digital transformation.

Various Dx technologies are hotspots for (in) security:

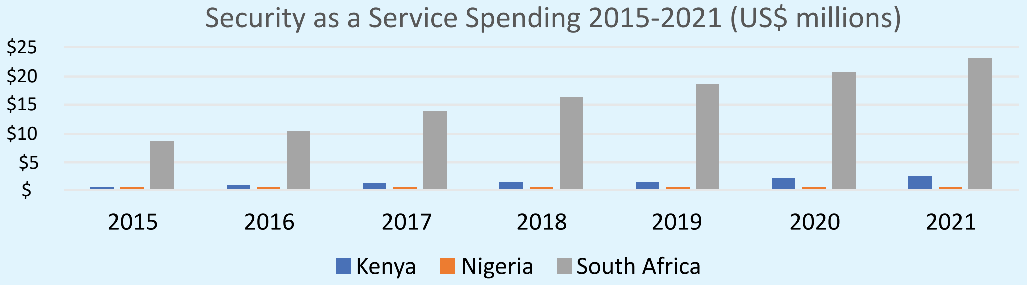
- Cloud (Spectre/Meltdown)
- IoT (auth/poisoning/DoS)
- AI/cognitive (subversion/DoS)
- Shadow IT (leakage/authentication/BC)

CHALLENGES IN MANAGING SECURITY



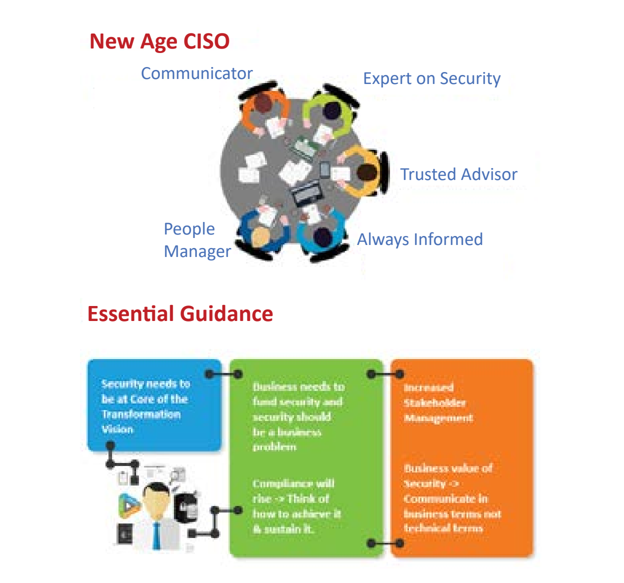
SOURCE 2: IDC

SECURITY AS A SERVICE SPENDING



SOURCE 3: IDC

- Uganda has a growing service-oriented view of IT management, from outsourcing to contract support, and security is now an established part of that. Still some way to go to acceptance and maturity, but the market is picking up.
- In Nigeria, it's mainly continuity-based (backup, DR, BC) except for large enterprises, where there's a more holistic security view, especially in MNCs. Endpoint security as a service is making decent progress too.
- RSA has a mature security-as-a-service market, plenty of service providers including some exporting skills internationally. Still heavily skewed towards the top organisations though, especially in BFSI and healthcare - for the mid-market and down it's still a grudge or post-incident engagement.
- In all these markets, there's a fairly clear sense that end-user organisations can't effectively keep up with cutting edge security. You either do the basics and hope the worst doesn't happen, or you outsource some of it. So the TAM ceiling for security as a service is really about awareness, not need.



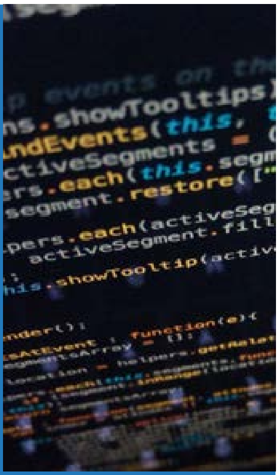
Security needs to be at Core of the Transformation Vision

Business needs to fund security and security should be a business problem

Compliance will rise -> Think of how to achieve it & sustain it.

Increased Stakeholder Management

Business value of Security -> Communicate in business terms not technical terms



IDC | ANALYZE THE FUTURE

ABOUT IDC

INTERNATIONAL DATA CORPORATION (IDC) IS THE PREMIER GLOBAL PROVIDER OF MARKET INTELLIGENCE, ADVISORY SERVICES, AND EVENTS FOR THE INFORMATION TECHNOLOGY, TELECOMMUNICATIONS, AND CONSUMER TECHNOLOGY MARKETS. WITH MORE THAN 1,100 ANALYSTS WORLDWIDE, IDC OFFERS GLOBAL, REGIONAL, AND LOCAL EXPERTISE ON TECHNOLOGY AND INDUSTRY OPPORTUNITIES AND TRENDS IN OVER 110 COUNTRIES.

IDC HAS BEEN PRESENT IN AFRICA SINCE 1999 AND SERVES THE CONTINENT THROUGH A NETWORK OF OFFICES IN JOHANNESBURG, NAIROBI, LAGOS, AND CAIRO, COMBINING LOCAL INSIGHTS WITH INTERNATIONAL PERSPECTIVES TO PROVIDE IT VENDORS, CHANNEL PARTNERS, TELCOS, AND END-USER ORGANISATIONS WITH A COMPREHENSIVE UNDERSTANDING OF THE DYNAMIC MARKETS THAT MAKE UP THIS DIVERSE REGION.

GIVEN IDC'S RESPECTED STANDING IN THE MARKET, WE HAVE ALSO ESTABLISHED CLOSE WORKING RELATIONSHIPS WITH GOVERNMENTS THROUGHOUT AFRICA, PROVIDING THEM WITH IN-DEPTH CONSULTANCY SERVICES DESIGNED TO INFORM A NEW GENERATION OF TECHNOLOGY POLICIES, STRATEGIES, AND REGULATIONS FOR THE DIGITAL ERA.

AS AFRICA'S DIGITAL TRANSFORMATION NARRATIVE CONTINUES TO EVOLVE, IDC IS PERFECTLY POSITIONED TO HELP IT VENDORS, SERVICE PROVIDERS, AND CHANNEL PARTNERS BUILD LONG-TERM PARTNERSHIPS, DELIVER LASTING BUSINESS VALUE, AND PROVIDE THE LOCAL CONTEXT REQUIRED TO ENABLE SUCCESS.

YOU CAN FOLLOW IDC SUB-SAHARAN AFRICA ON TWITTER AT @IDC_SSA.

SURVEY ANALYSIS

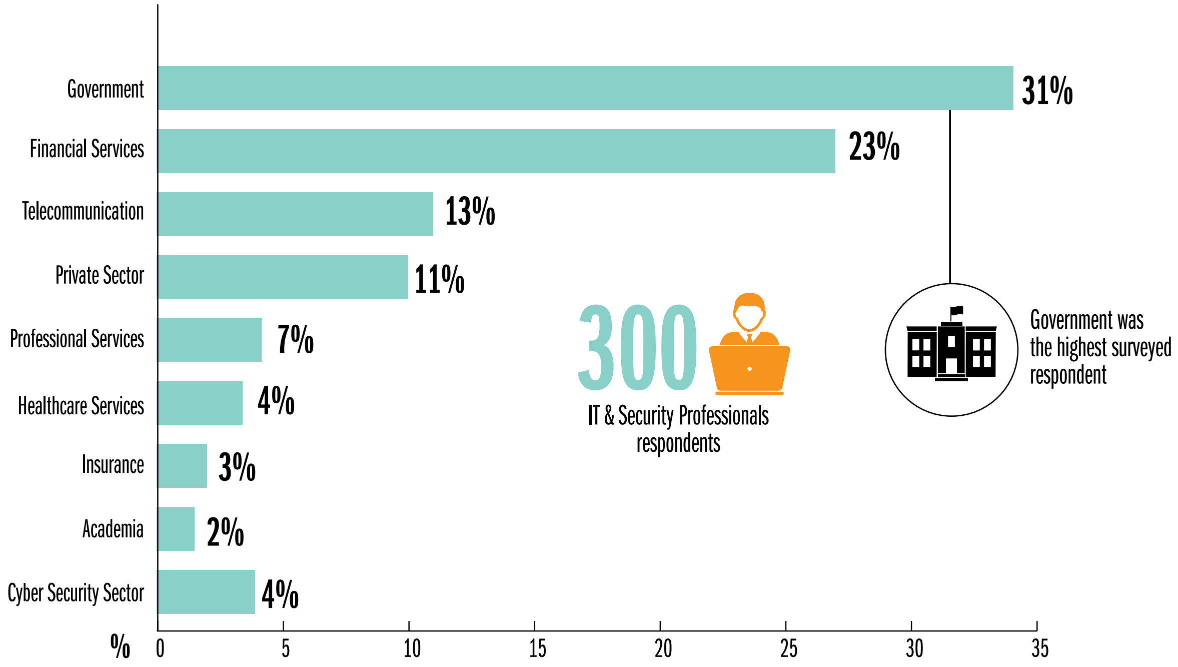
The 2018 Cybersecurity Survey provides insight into what Ugandan organizations are doing to protect their information and assets, in light of increasing cyber-attacks and compromises impacting them.

Based on the feedback from over 150 IT and security professionals we interviewed, an analysis of the findings yielded a few notable themes, which are explored in greater detail in this report and highlights are summarized below:

RESPONDENTS PROFILE

INDUSTRIES SURVEYED

To ensure that the results of our survey and research provide a nationwide representation of the state of



GRAPH 1: INDUSTRIES SURVEYED.

BYOD, CLOUD AND IOT

Getting more for less and saving costs are just few of the key motivators and driving forces for Ugandan businesses. The Bring Your Own Device, Cloud computing and IoT era has redefined this notion within modern corporate landscape.

We asked our respondents whether or not they utilize these systems:

CHART 1: BYOD USAGE.

Does your organisation allow the use of Bring Your Own Devices (BYODs)?

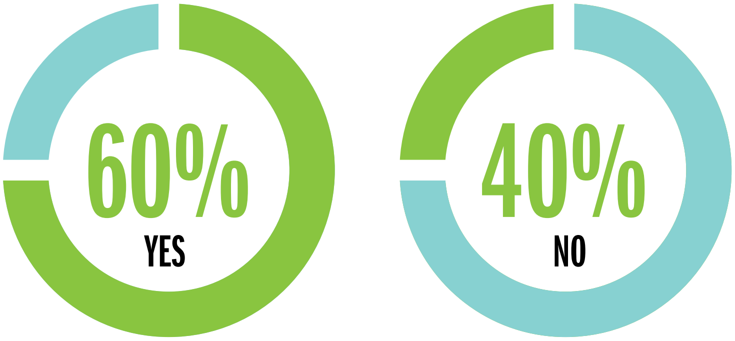
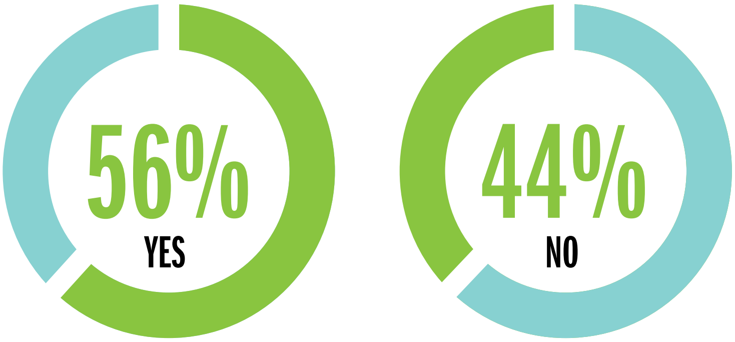


CHART 2: CLOUD SERVICES/ IOT USAGE.

Does your organization allow/utilize Cloud Services or Internet of Things Tech



> THE GLOBAL CLOUD COMPUTING MARKET IS EXPECTED TO CROSS $1 TRILLION BY 2024.
>
> MARKET RESEARCH MEDIA

The global BYOD and Enterprise Mobility market is expected to double from $35bn in 2016 to $73bn in 2021 according to Miranex research, while the global cloud computing market is expected to cross $1 Trillion by 2024, according to Market Research Media. There are more people working on laptops and mobile devices such as tablets and smartphones the main reasons for this adoption are:

- IT managers value the increased personal productivity that comes with BYOD
- General users:- with remote working becoming increasingly popular, more workers require the flexibility of working outside the office and outside of the normal working hours.

BYOD, CLOUD POLICIES

Organisations may be quick to use devices such as tablets, IPads and smart mobile phones as attractive perks or even transfer some of the device costs to their employees. However, the management of these devices has still not been prioritized. We asked our respondents whether or not they have a policy or framework to guide on usage of these technologies:

CHART 3: BYOD POLICY

Does your organisation have a best practice policy for BYOD?

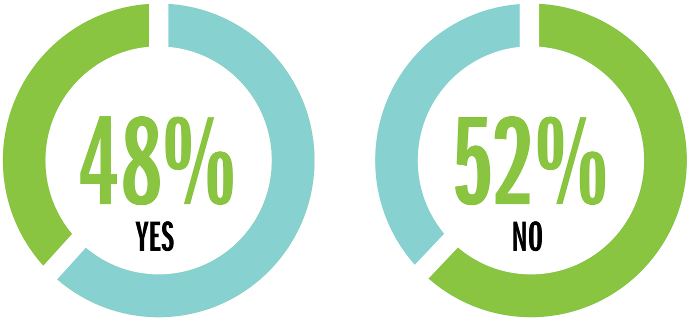
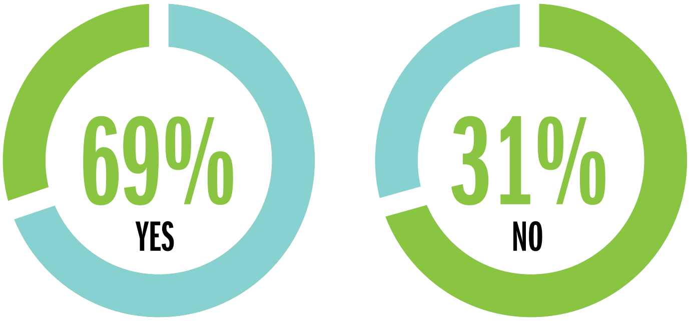


CHART 4: IOT AND CLOUD SERVICES BEST PRACTICE

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



BYOD/IoT present the following challenges:

- Widespread adoption of BYOD reduced standardization and increased complexity
- Integration concerns particularly with existing infrastructures, device support, and increased exposure to a variety of information security hazards

Key challenges in integrating data sources

- Limited capabilities for real-time data integration
- Ever-growing volume of data
- Increasing data complexity and formats
- Changing security requirements

Without a proper framework to provide guidance on the use of these technologies, organisations run the risk of Cyberattacks.

RECOMMENDATIONS

- Mission critical devices that rely on a standard PC platform should not be attached to a WAN unless absolutely necessary and need to be safeguarded from access by non-critical personnel.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities.

04

DID YOU KNOW?

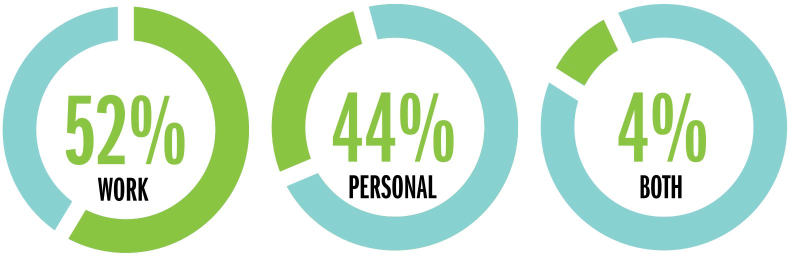
ATTACKERS ARE TAKING ADVANTAGE OF THE INCREASED USE AND LACK OF MONITORING OF PERSONAL DEVICES WITHIN ORGANISATIONS TO INTRODUCE ROGUE DEVICES THAT ARE THEN USED TO COMPROMISE THE NETWORK.

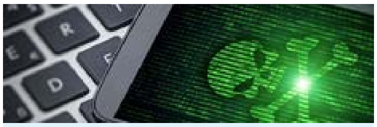
CYBER CRIME

The explosion of online fraud and cyber-crime affected almost 58% of all our respondents, mostly because of the roles they play in their organisations. This means majority of attackers are targeting organisations and people working for these organisations.

HAVE YOU BEEN A VICTIM OF ANY CYBERCRIMINAL ACTIVITY IN THE LAST 5 YEARS?

In what capacity, have you been a victim of cybercrime?





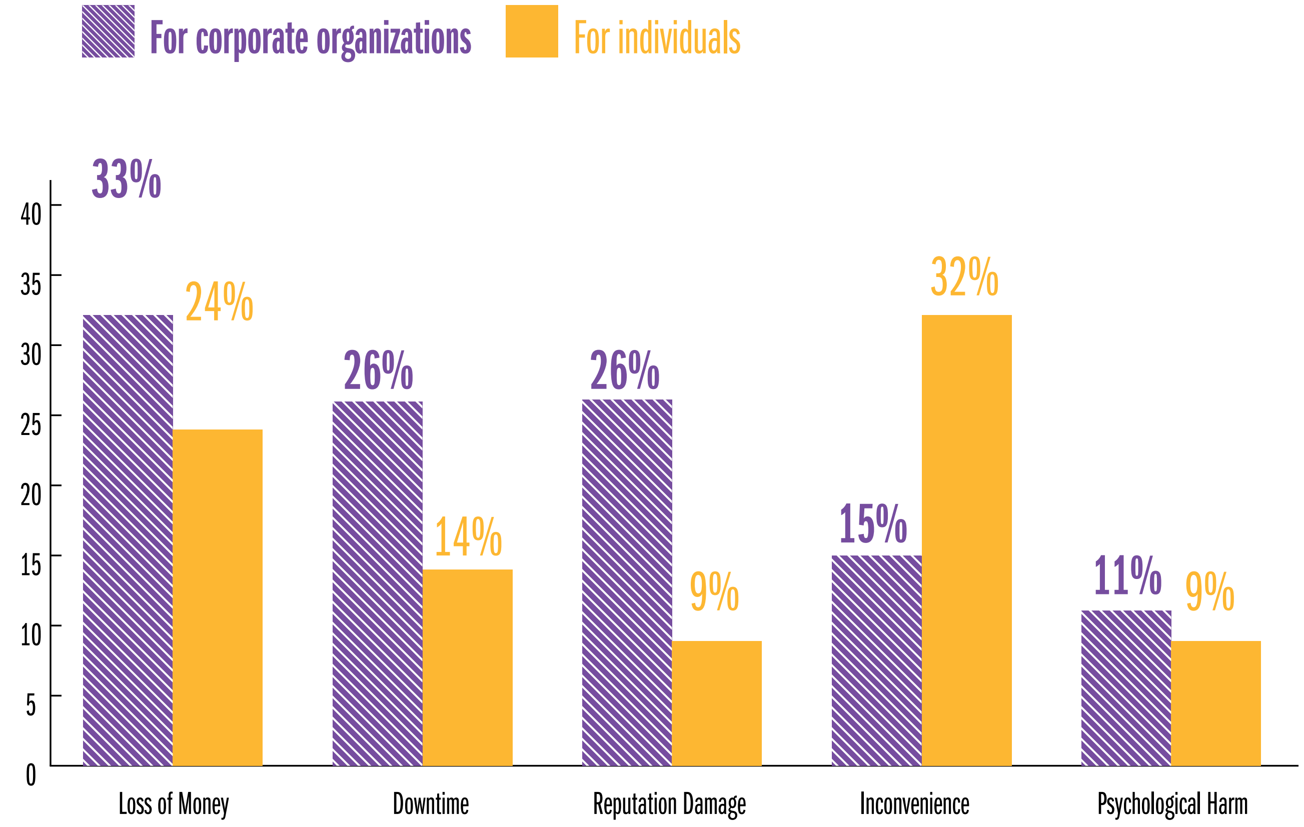
> ON AVERAGE, ORGANISATIONS VICTIMIZED BY CEO FRAUD ATTACKS LOSE BETWEEN $25,000 AND $75,000.
>
> FBI ALERT 2016

WHY YOU ARE A TARGET

Who	Why	How
HR Managers	Have direct access to payroll systems and information	Social Engineering
Board	Have access to sensitive information such company strategy, bank approvals and audit reports	Phishing e-mails
System Administrators	Custodians of credentials to critical infrastructure	Use of Keyloggers Network sniffing
Finance Executives	Have authority to process payments	Phishing e-mails

IMPACT OF CYBER CRIME

We asked the respondents to state the impacts experienced after the cyber attack. The biggest impact affecting both corporates and individuals was loss of money. It was interesting to note that inconvenience and psychological harm had a greater impact on individuals.



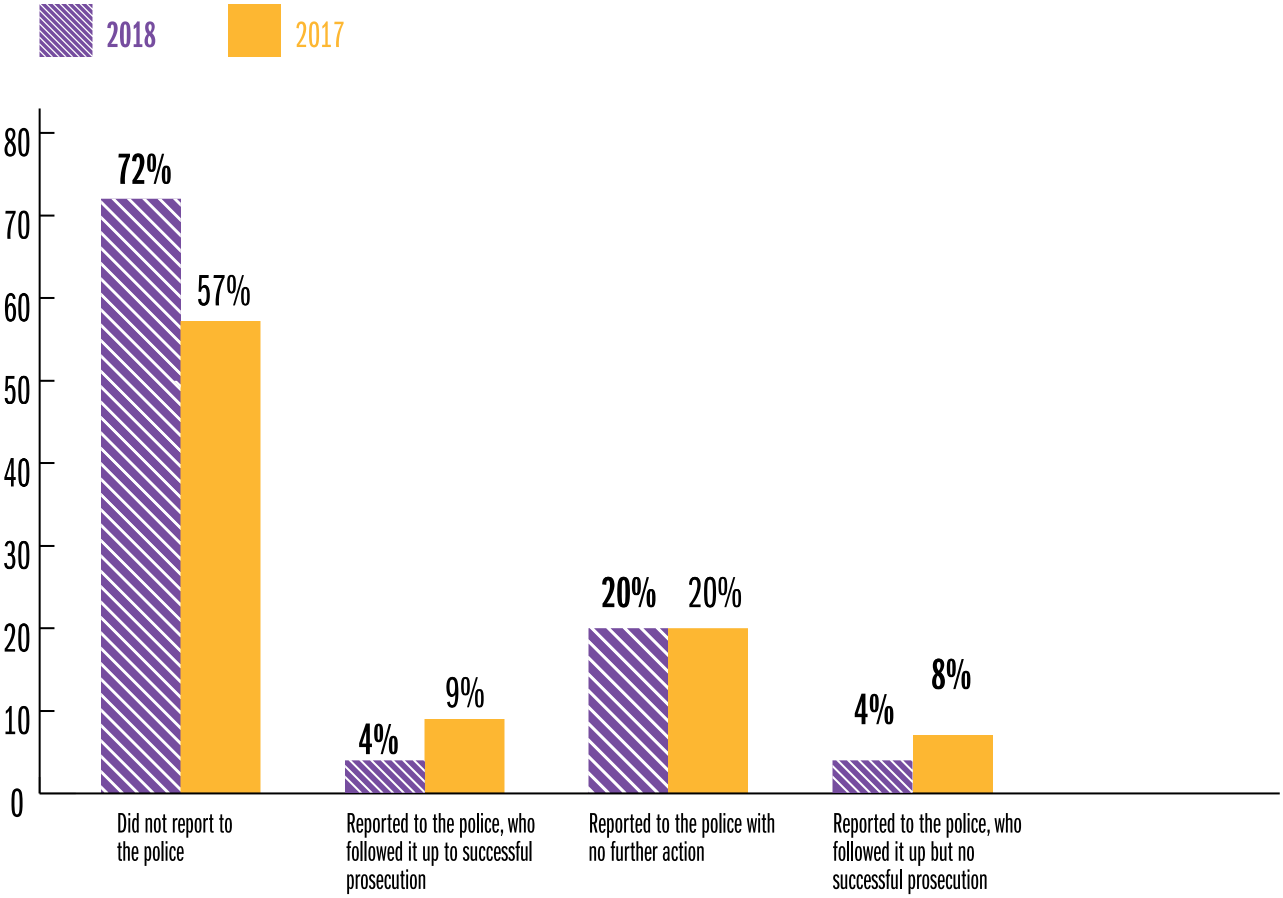
GRAPH 2: IMPACTS OF CYBERCRIME: CORPORATE VS INDIVIDUALS.

This presents one conclusion that majority of attacks in Africa are motivated by financial gain – suggesting reasons why financial institutions, Saccos and organisations that deal primarily with transaction processing are primary targets for the Cyber-attacks.

REPORTING OF CYBER CRIME

Internet-related crime, like any other crime, should be reported to appropriate law enforcement or investigative authorities. Citizens who are aware of cyber crimes should report them to local offices of cyber law enforcement.

IF YOU HAVE BEEN A VICTIM OF CYBERCRIME, WHAT ACTION FOLLOWED?



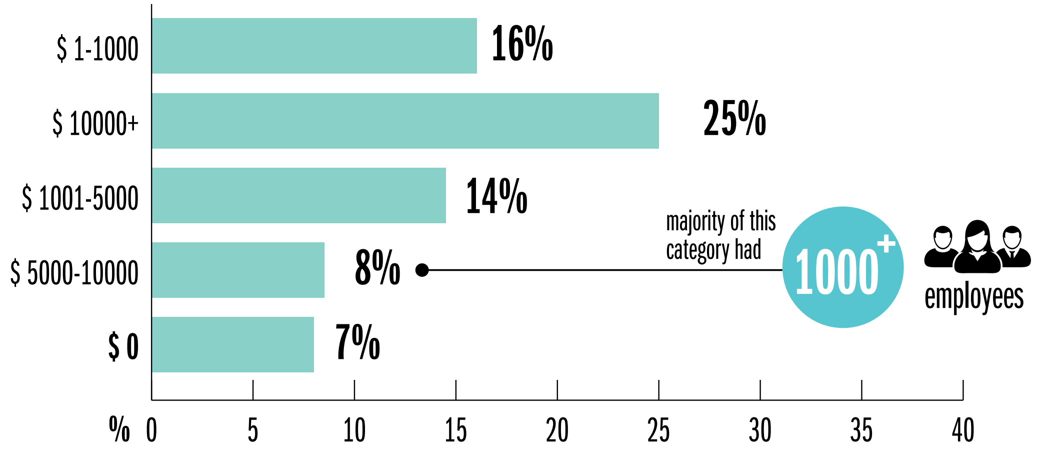
GRAPH 3: REPORTING OF CYBERCRIME .

- 2018 saw an 15% increase in the number of people who reported Cyber crime incidents to the police.
- 8% increase in the number of successfully prosecuted Cybersecurity incidents.
- However, we also witnessed an increase in the number of incidents that were not acted upon by the law enforcement.

CYBER SECURITY SPENDING

Organisations are now investing more to achieve cybersecurity resilience. From our analysis in 2016, 95% of respondents invested less than $5,000 on cyber security during the year. In 2018, 25% of respondents spend above $10,000. Further analysis also revealed that majority of organisations which spend USD 10,000+ are from the Banking and Financial sectors. This is not surprising since these industries are the most targeted.

Most of companies that invested more than $5000 had 1000+ employees.

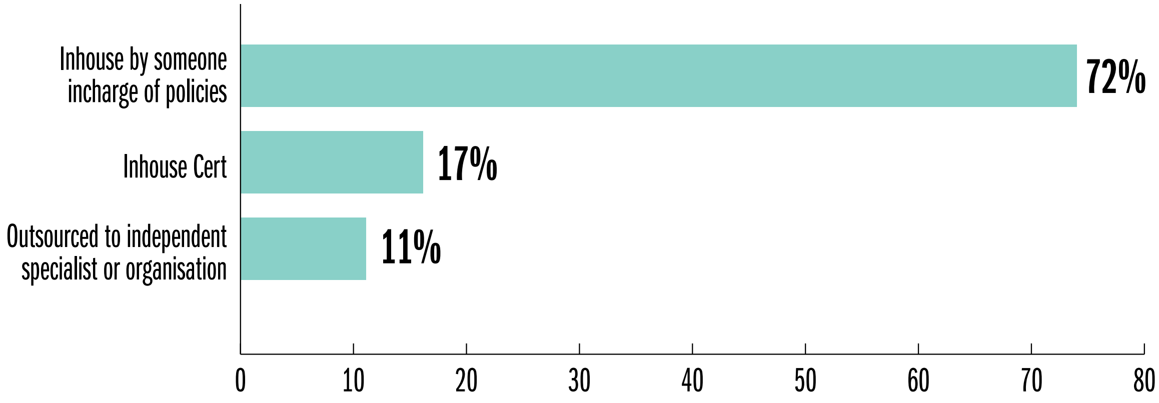


GRAPH 4: CYBERSECURITY SPEND.

MANAGING CYBER SECURITY

89% of organisations manage their cyber security inhouse while 11% have oursourced these services to an external party (MSSP or ISP). More companies are now developing inhouse capabilities to manage cyber security, this is the case with Banking, Saccos and financial institutions.

HOW IS YOUR ORGANISATION'S CYBER SECURITY MANAGED?

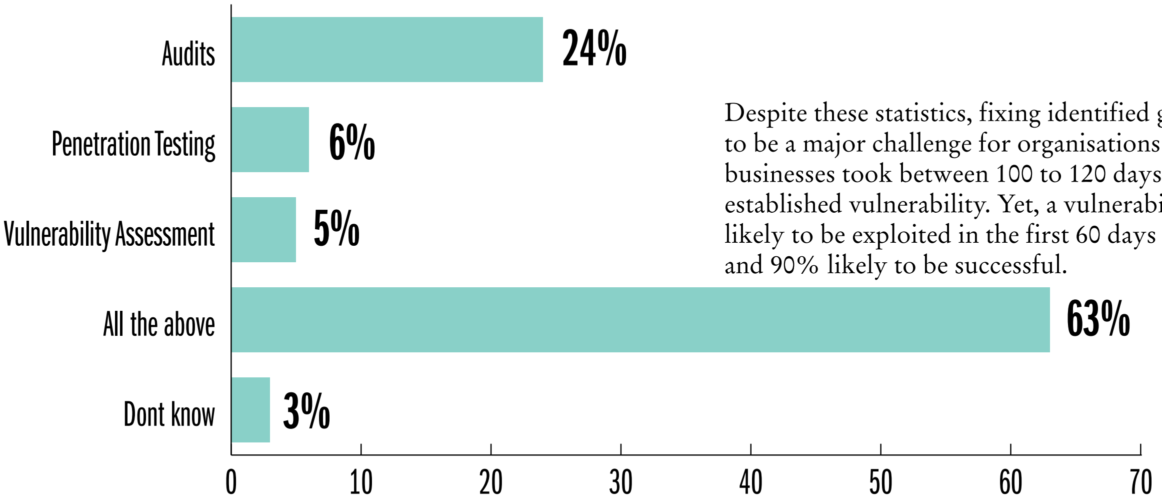


GRAPH 5: CYBERSECURITY MANAGEMENT.

CYBER SECURITY TESTING TECHNIQUES

Security testing is a process that is performed with the intention of revealing flaws in security mechanisms and finding the vulnerabilities or weaknesses in the environment. Recent security breaches of systems underscore the importance of ensuring that your security testing efforts are up to date. From the survey, 63% of respondents perform a combination of vulnerability assessments, penetration testing and audits. 6% perform penetration testing while 24% perfrom audits. All these testing techniques work best when applied concurrently.

WHICH OF THE FOLLOWING SECURITY TESTING TECHNIQUES DOES YOUR ORGANISATION USE?



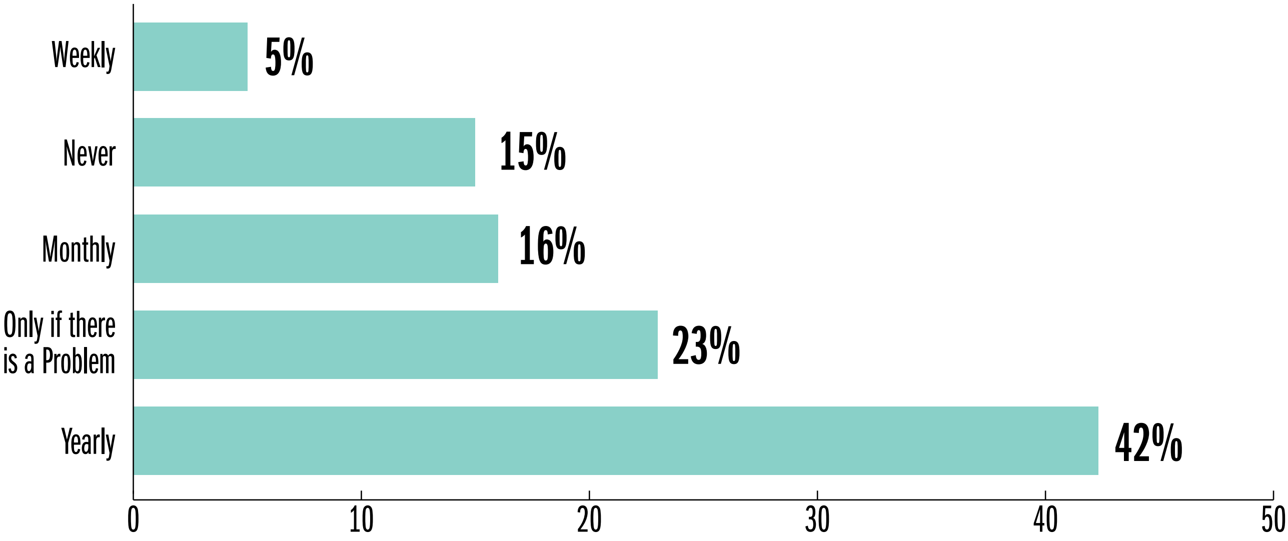
Despite these statistics, fixing identified gaps was found to be a major challenge for organisations. On average, businesses took between 100 to 120 days to fix an established vulnerability. Yet, a vulnerability is most likely to be exploited in the first 60 days of its release — and 90% likely to be successful.

GRAPH 6: SECURITY TESTING TECHNIQUES.

CYBER SECURITY AWARENESS

The level of cybersecurity awareness in Uganda is still low with 15% of organisations not having an established cyber security training program.Most organisations (23%) are also still very reactive when it comes to cyber security training, these organisations train their staff only when there is an incident or problem. This is worrying considering 54% of all cyber attacks reported in the survey was through work. Having said that, important to point out that 63% of respondents reported to have a regular training program in place. This is a 7% increase from 2017. The importance of having regular security training for employees cannot be over emphasised.

HOW OFTEN ARE STAFF TRAINED ON CYBERSECURITY RISKS?



GRAPH 7: STAFF TRAINING.

> THE SLOW RESPONSE PARTICULARLY BY THE IT TEAMS DUE TO LARGE VOLUME OF VULNERABILITIES AND LIMITED CYBERSECURITY SKILLS LEAVES A LOT OF ORGANISATIONS VULNERABLE TO CYBER ATTACKS.

INDUSTRY PLAYER PERSPECTIVE

ARNOLD R. MANGENI

Director of Information Security, NITA

IS THERE COHERENT GOVERNMENT STRATEGY ON CYBER SEC FROM THE NITA PERSPECTIVE AND WHAT DOES IT SAY?

Yes. We use the National cyber security strategy which was developed in partnership with the CTO. They did extensive stakeholder engagement to come up with the strategy which put together helps realize the country's cyber space. The key areas identified include the need to address capacity to fill the skills gap which was a key challenge. We are in progress to try and implement initiatives in the strategy.

ARE THERE ANY NEW DIGITAL INITIATIVES THAT HAVE DEVELOPED IN THE GOVERNMENT SECTOR WITHIN THE PAST FIVE YEARS?

We have a number of them such as the current devolvement of the payment gateway and other efforts like the e-government procurement project which is supposed to go live on 1st July 2019.We have a system integration project about to start. We are concluding the evaluation and the objective of that is to try and create mechanisms which the government can share data across the board to adopt the mode of collect once use always. For instance, when the national identification and registration authority(NIRA) captures your details during ID registration when applying for a passport they don't ask you your details.

DIGITIZATION IN GOVERNMENT PRESENTS MAJOR RISKS TO THE GOVERNMENT PARTICULARLY DATA LEAKAGE AND FRAUD. WHAT IS BEING DONE TO MITIGATE THIS?

In February this year we had the re-enactment of the data protection and privacy act. This act is both for the public sector and the private sector. There are a number of mechanisms expected to be upheld by entities that host information about people to provide assurance that they safeguard the information.

There is also the national information security framework that provides minimum security requirements for various government institutions, their supply chain and critical national infrastructure operators. When all this is implemented it benefits the country's security posture.

DOES THE GOVERNMENT ENGAGE THE PRIVATE SECTOR IN CYBER SECURITY PROJECTS AND HOW EFFECTIVE ARE THOSE PARTNERSHIPS?

It does and the partnerships yield a lot of value.

There is the national information security advisory group(NISAG) which is a fusion of both public and public system players who discuss cyber security issues that affect the country at a national level. This helps create the national risk register which highlights various risks government systems face that helps in installation of controls to improve security. This is one of the most valuable things we get from the mix of government and private sector because the private sector is advanced on two fronts that is the resource front and the research and development of cyber security.

The Nisag also has members from the academia. We tap into the research they have done that could be affecting our use if Technology. Nisag is brings everyone onboard.

ARE THERE ANY COMPETENCES YOU SEE THAT ARE LACKING IN THE GOVERNMENT SECTOR?

The key one is threat intelligence. It's interesting that we rely on signature based systems that probably are picking all their threat intelligence on things that have already been discovered and nothing new. If there is a zero-day attack the chances of hitting are higher due to lack of intelligence. Emphasis has not been given to threats and their motivations, capabilities etc.

THE PUBLIC SECTOR DOES NOT ATTRACT YOUNG PEOPLE. WHAT IS YOUR PICK ON THIS?

It does but there are so many things that people are interested in when it comes to employment. One of them is pay and it is known the government does not pay as well as the private sector. Government trains unconditionally in comparison to the private sector based and those that have stayed within the government have benefited from these trainings.

WHAT CAN BE DONE TO ENSURE WE ATTRACT YOUNG PEOPLE WITHIN GOVERNMENT?

Try and make our education relevant to the industry. Train on different areas to avoid overemphasis on one sector as it is going to be overburdened by a lot of graduates and the industry won't be able to take them all. But there are some that are deficient. I.e. Oil and gas whereas ICT is overwhelmed. We need to tailor our education to be relevant to the industry.

HOW DO YOU THINK THE GOVERNMENT IS SUPPORTING THIS PROCESS WHEN IT COMES TO SECURITY?

Makerere university offers a major in security. There is a masters and a bachelor in security.

IS THERE ANY WAY NITA IS TRYING TO SUPPORT THIS?

We work with a number of universities. To try and expose the youths to what the industry demands and that is how Makerere University has tailored their programs. We have a challenge to customize existing resources to suit industry needs. There is need for professional devolvement and we have not have had people come to set up shop. We have no providers of specific courses such as forensics within the country. Realigning the industry will take time because it requires resources but it will come over time.

DO YOU HAVE A ROUGH ESTIMATE ON HOW MANY PROFESSIONAL ACADEMIES ARE AVAILABLE?

No. I don't have an exact number. A couple include: Summit consultants and Milima.

There are quite a number but I am unaware of the exact number.

IN TERMS OF PROFESSIONALS, DO YOU KNOW HOW MANY PROFESSIONALS ARE IN THE COUNTRY?

There are a number of professional courses apart from those offered in the country. It is difficult to give a number. A rough estimate would be 200-300 security professionals both certified and not certified.

Cybercrime is increasing and it takes more time to resolve. Cyber-attacks are evolving from the perspective of what they target, how they affect organizations, and the changing methods of attack,

As cybercrime continues to evolve, organizations are facing an expanding threat landscape that includes malicious nation-states, indirect supply chain attacks, and information threats. At the same time, they are deploying new technologies faster than they can be secured.

INDUSTRY PLAYER PERSPECTIVE

NOAH BALESANVU

National Information Security Advisory Group, NISAG

IS A THERE A COHERENT GOVERNMENT STRATEGY ON CYBER SECURITY AND WHAT DOES IT SAY?

The government has octets of cyber security experts within different organs: Within the security sector there are organs are well equipped to handle cyber security threats. On the government side NITA does cyber security well. In the private sector it is handled by the regulator and then associations within the private sector. i.e. Uganda Bank association. ERA (Electricity regulatory authority). UIA and IRA for the insurance sector. In terms of where we see high automation in the utilities there are UMEME UATC etc. They have either dedicated cyber security resources in terms of humans or they have equipped their IT operations with cyber sec expertise. We noticed the interplay of different efforts presented parts hence formation of NISAG. NISAG gets its mandate from the national information security framework and strategy and so it brings together all critical infrastructure players under one roof where they co-ordinate specifically on infrastructure because it was the biggest gap, once infrastructure is covered then periphery can be handled by other organizations.

WHAT DIGITAL INITIATIVES HAVE DEVELOPED IN THE GOVERNMENT HAVE DEVELOPED IN THE LAST FIVE YEARS?

NITA has been growing rapidly, they just had the e-government week. We have over 80 systems in government that are online and being integrated and the list keeps growing. VISA, passport and Immigration system are fully automated. The SCADA system for utilities are automated. Other areas such as service delivery are automated too such as E-TAX, NSSA. The question now is which systems are not automated. The move right now is to consolidate these systems so that we have information sharing securely to improve service delivery.

DIGITIZATION IN GOVERNMENT PRESENTS MAJOR RISKS TO THE GOVERNMENT PARTICULARLY DATA LEAKAGE AND FRAUD. WHAT IS BEING DONE TO MITIGATE THIS?

One of the tasks NISAG handles is to ensure the integrations are done securely and so we hold member organizations at high standards of security with regards to protecting this data. One of the things we do is data classification. This is empowered by our different existing laws. Within the financial sector we have BAU regulating this. We have ERA doing this for the energy sector and then we have the regulators playing an active role in ensuring cyber security is kept at a high standard. In telecommunication we have UCC. From a policy standpoint we have the laws and regulators have power to enforce the laws. From a technology standpoint it will come over time for example with the current integration it will come with visibility over multiple systems which also gives the risk exposure and give decision makers tools to make decisions. We have new laws getting better. i.e. the data protection law which forces compliance on data. One of the challenges is massive freedom which presents security risks.

HOW IS THE REGULATION OF THE DGPR LAW COMING ALONG?

The regulation is being worked on but the law is already definitive in several areas. Different acts are already being implemented. Companies here are already prepared to be DGPR compliant.

DOES THE GOVERNMENT ENGAGE THE PRIVATE SECTOR IN CYBER SECURITY PROJECTS AND HOW EFFECTIVE ARE THOSE PARTNERSHIPS?

It does.

NISAG engages the private sector very actively.

Academia not as much as we should but we recently added them as a key member.

ARE THERE ANY CYBER SECURITY COMPETENCES YOU SEE THAT ARE LACKING IN THE GOVERNMENT SECTOR?

We are certificate hunters. The evolution of the technology industry in Uganda you find that many people are self-taught. It is only recently that we are seeing Makerere training cyber security courses. We have heavy dependent on tools we stop being professionals. We also lack cyber security leadership. We don't have a commissioner level leadership in cyber security.

THE PUBLIC SECTOR DOES NOT ATTRACT YOUNG PEOPLE. WHAT IS YOUR PICK ON THIS?

The government is very active in engaging young people. Organizations like NSSF and URA hire young people. BOU has campus outreach that hires people from university. We have very many graduates every year and the government can't hire them all but it can create opportunities for young people.

WHAT NEEDS TO BE DONE SO THE GOVERNMENT ATTRACTS NEW TALENT?

Embracing innovation. Uganda is one of the most entrepreneurial countries in the world and the youth have the idea and the drive. The government has committed 30B shillings to spark innovations in this financial year.

HOW MANY DOORS ARE BEING PUSHED OUT BY UGANDAN STARTUPS?

Not many but there is representation for instance the Academic management information system(AMIS). Entities like NSSF builds most of its applications in house. We have to up our game so as to tip the scales which will allow us to compete with others.

COST OF CYBERCRIME

2018 analysis of Cost of Cybercrime is based on our assessments, focusing on reported annual cybersecurity budgets, incidents of cybercrime, our insider knowledge when handling cases of cybercrime and estimates.

$52m
estimated cost of cybercrime

→ **Direct Cost:** $17m

← **Indirect Costs:** $35m

MOST AFFECTED INDUSTRIES

1. Banking
2. Financial Services Intergrators
3. Microfinance
4. Financial Institutions and Service Providers
5. Government

REPORTED AND NON-REPORTED COST OF CYBERCRIME

Over 90% of Cybercrime cases go unreported. As such, we undertook to provide an approximate value of the overall cost of Cybercrime. This analysis decomposes the cost based on these 2 categories:

DIRECT COSTS

- Costs as a consequence of cybercrime, such as direct loss of money and confidential records
- Costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies;

INDIRECT COSTS

- Costs in anticipation of cybercrime, such as antivirus software, insurance and compliance;
- Costs as a consequence of cybercrime 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. indirect costs such as weakened competitiveness as a result of intellectual property compromise;

INDIRECT COSTS	Estimated Indirect Cost (USD)	Technologies	Process	People
Financial Services (Banking, Insurance, Saccos and MFI)	10,906,779.66	• SIEM • Network Access Controls • IPS/IDS • Active Directory • Vulnerability Management • Solutions • PAM • Antivirus • HIDS • Proxy • WAF • Load Balancer	• Penetration testing • Audit • Forensic Investigations • Risk Assessment • Compliance Review • Post-Implementation • Review • BCP/DR Testing and • Review	• General Awareness • Training • Technical Training • Board Training • Business Managers • Training
Government and Public Sector	10,110,169.49			
Service Providers (Telcos, Fin-tech, Betting, Financial apps)	8,135,593.22			
Manufacturing, Healthcare, Hospitality and Retail	1,186,440.68			
Others	4,661,016.95			
Total Indirect Loss: $35,000,000.00				

DIRECT COSTS	Estimated Direct Cost (USD)	Activities
Financial Services (Banking, Insurance, Saccos and MFI)	5,378,531.07	• Data hijacking (ransomware attack) • Money lost • Fines from regulators • Law suits • Claims and Cyber Insurance • Forensic Investigations
Government and Public Sector	4,898,305.08	
Service Providers (Telcos, Fin-tech, Betting, Financial apps)	3,841,807.91	
Healthcare, Hospitality and Retail	576,271.19	
Others	2,305,084.75	
Total Direct Loss: $17,000,000.00		

INDUSTRY PLAYER PERSPECTIVE

KENNETH MUHANGI

Partner, KTA Advocates

TO WHAT EXTENT DOES DATA PROTECTION AND PRIVACY REGULATION REFLECT THE CHALLENGES OF THE DIGITAL AGE?

We have an act, we don't have regulations that enforce what was gazetted as far as I am aware. We have a data protection and privacy act, It's not yet operationalized because in Uganda in order for you to have a law that is operationalized you need to have the act which is the primary source of the rules which then basically give an overview or a step by step guide on how the act is supposed to be enforced.

The fact that the law was passed and the fact that many African countries that have a data protection late on a stand-alone one act that shows the seriousness of cyber security of data breaches which am happy that our government is taking seriously and yes, that shows a big reflection that we have a law that governs data protection and privacy.

HOW COHERENT IS THE APPROACH TO CYBER REGULATION ACROSS DIFFERENT SECTORS OF THE ECONOMY AND THE WIDER INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN? WHAT ADVICE DOES THE GOVERNMENT GIVE?

I think overall there is a lot of laxity when it comes to cyber security and data protection. I think even the act that I just mentioned, although it is in force I'm sure there are only just a handful of companies are preparing because there are very stringent requirements for companies to follow. They are supposed to be compliant with the law because the act mentions or puts in force a data protection agency or authority in this case NITA. There are very few organizations which take cyber security seriously. The ones that do it is probably a facade which is a sad thing. Most people will take cyber security seriously when there is a hack or breach. But In terms of government, I think the government is very switched on. The ministry of ICT has really taken a lead in 1, ensuring we have adequate legislations, we have a computer misuse act which is very clear and criminalizes any cyber breaches or hacking. Of course the data protection and privacy act that I mentioned. And myriads of other legislations: electronic transactions acts etc. So I think in terms of the law, we are good. In terms of policies as well, perhaps where I'll say we still have a long way to go is ensuring even the government itself is compliant in regards to making sure that they have appropriate security measures and they have appropriate software and the like. But at least I know that a number of government agencies are moving with the digital age. The Judiciary for example is in the process of creating an ECMIS which is supposed to ensure or ease service and filing of court documents. So that's a very big deal. I saw the tender, the requirements were stringent in regards to cyber security and several other entities in the ministry of ICT itself through NIISP it's a project by the ministry of ICT to support and to give money to innovators to basically support the innovations cost systems. Most of the meetings we've had, most of the policies that make sure that the innovators that come through are finding solutions to problems and one of those problems is cyber security.

DOES THE CRIMINAL LAW ADEQUATELY ADDRESS OFFENCES COMMITTED?

Yes it does. But the nature of cyber-crime is that it's always changing in the sense for example, the time the computer misuse act was passed, there was hardly any tool of crypto currency. It existed but it wasn't as popular as it is now. And most of the hacks now that have happened some of them have involved crypto currency or people holding people at ransom and asking them to pay in crypto currency. So those are laws that provide an enabling framework in the sense that if you tamper with any computer or any device without authorization then you have an offense; that is adequate. But in terms of covering exact offenses, I would say no and that is impossible. That's the problem happening everywhere in the world. But in terms of having good enough legislation to cover that yeah I think we are okay. We could do better and I think the law also needs to keep changing with the time but overall I think it is good enough.

HOW CLOSELY HAVE POLICIES AND REGULATIONS BEEN DEVELOPED IN PARTNERSHIP WITH THE PUBLIC SECTOR OPERATORS WHO WILL BE IMPACTED?

There are a handful of laws that have been enacted with input from the public sector. One of those is the data protection act, I think they were called for people in the private sector to be able to give views on that. As to whether the views were implemented or not is another issue. But at least in regards with consultation of the public sector yes, we've had a number of businesses that have been consulted before this laws and policies come in to place. We have moving from tech to intellectual property which merges with tech, we have a national IP policy, we have a national ICT policy but I'm not sure if it covers or is adequate enough to cover every single area size. I think it's still a work in progress, we still need to have a lot of engagement between the private sector and the government.

WHICH AGENCY/AGENCIES HAVE THE RESPONSIBILITY FOR INVESTIGATIONS OF CYBER-ATTACKS AND ONLINE CRIME? WHAT CAPABILITIES AND CAPACITIES DO THIS AGENCIES HAVE?

Currently the police has a cyber-crime unit and again like everything, I don't think it is adequately stocked or it has adequate techniques to be able to prosecute and investigate crimes. So that's the body that I'd say is overall supposed to investigate. If it's financial crimes that involve money laundering or such, we also have the financial intelligence authority that works with the police to prosecute any such related offences that related to crimes like financial crimes. And then the prosecution is done by the directory of public prosecution. And we have other bodies that are in charge of compliance which NITA . I know for a fact that IT providers, we have IT certifications act, so NITA is in charge of ensuring that every person that deals with IT or ICT equipment in terms of selling or installation has to get a license from them. In some cases also comes in not sure exactly how but the act gives them a lot of power to be able to put whatever they want. The key institutions that deal with cyber security are the police, DPP and maybe NITA.

YOU SAID THE FIA IS UNDER THE POLICE?

No, FIA is an independent body but it works hand in hand with the police. Its job is to investigate and work with the prosecution. They handle crimes like money laundering and other financial crimes.

DOES THE GOVERNMENT COLLABORATE WITH OTHER GOVERNMENT TO PREVENT AND INVESTIGATE CYBER-CRIME?

Yes. To investigate especially if there is a cyber-breach that perhaps has originated from another country. We have had cases where there has been interaction between our agencies and foreign entities to try and get to the bottom of it and I think any government should be able to collaborate because usually the crimes usually happen in the space and most people will mask their IP addresses. So it's good for agencies to do that and yes I know that Uganda does collaborate with other countries to investigate and prosecute cyber-crime.

OTHER THAN THAT, IS THERE ANY OTHER COMMENT YOU'D LIKE TO GIVE IN REGARDS TO THE SKILLS GAP IN THE LEGAL DEPARTMENT

Definitely in terms of prosecution I conducted a training with the judicial system of the office of the DPP and you could tell that a number of them weren't aware of some of the development that have happened especially in investigating and prosecuting. Some do but I think the most important thing is the zeal to want to skill their staff so I think in terms of the skills gap we have a very big skills deficit in regards to having the officers who understand cyber security and ICT law. But that is changing slowly especially with the younger generation. ICT laws have been introduced to schools and universities not only secondary even primary. In a few years that gap will be bridged. A the moment there is a very big skills gap on both sides and also being able to use adequate techniques and people keep finding more sophisticated techniques to hack.

CYBER SECURITY SKILLS GAP

Uganda not only has a shortage of highly technically skilled people, but also an even more desperate shortage of technicians who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to Anticipate, Detect, Respond and Contain Cyber threats.

We interviewed a number of certifying bodies in Uganda to determine the approximate number of skilled professionals within the country.

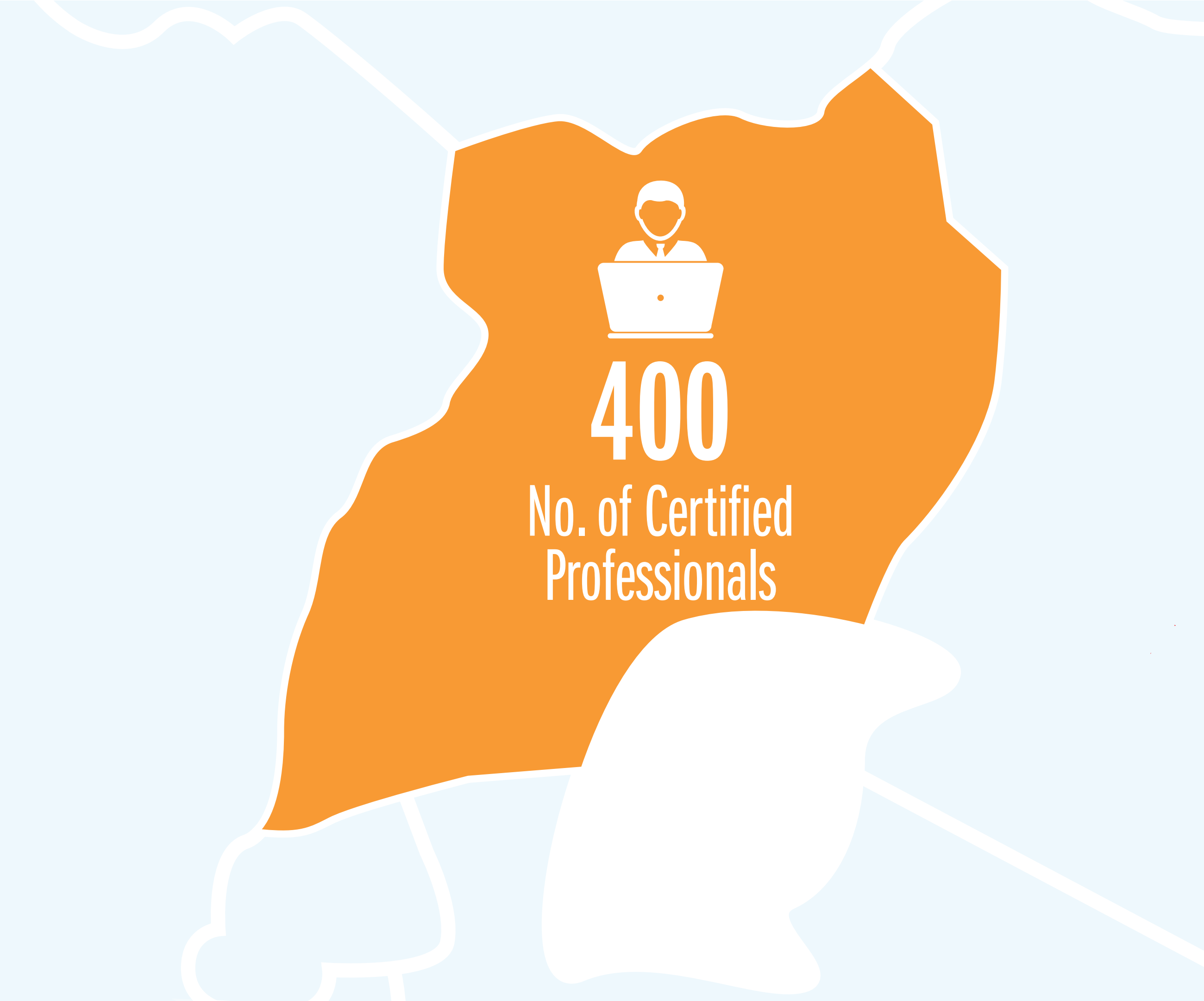


FIGURE 1: NUMBER OF CERTIFIED PROFESSIONALS IN UGANDA.

No. of Skilled Professionals in 2018

		Sub-Saharan	Global
ISACA Trust in, and value from, information systems	CISA Certified Information Systems Auditor An ISACA Certification	3795	84,484
	CRISC Certified in Risk and Information Systems Control An ISACA Certification	646	19,163
	CISM Certified Information Security Manager An ISACA Certification	945	32,233
	CGEIT Certified in the Governance of Enterprise IT An ISACA Certification +Others	324	5749
(ISC)²	CISSP Certified Information Systems Security Professional	844	*
C|EH Certified Ethical Hacker	OTHERS	6554	*
	TOTAL	**13,500**	*

Source: https://www.isc2.org/About/Member-Counts, http://www.isaca.org/About-ISACA/Press-room/Pages/ISACA-Certifications-by-Region.aspx

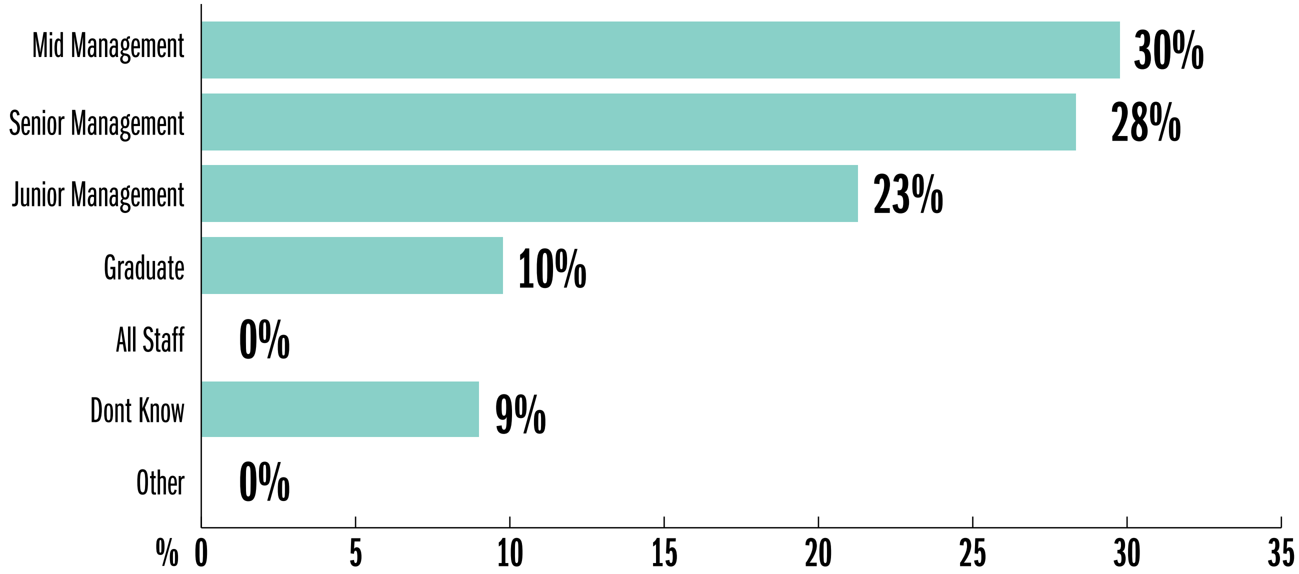
(ISC)² Member Counts.The above counts reflect the number of members per credential as of December 31, 2018..
Note: Member counts are updated bi-annually.
www.isc2.org

The above figures are estimates, for more accurate data, please confirm with the specific training institutions.

FIGURE 2: SKILLED PROFESSIONALS.

To determine where the pain points are, we asked over 150 professionals to provide more insights on the issues they faced. Below are the findings:

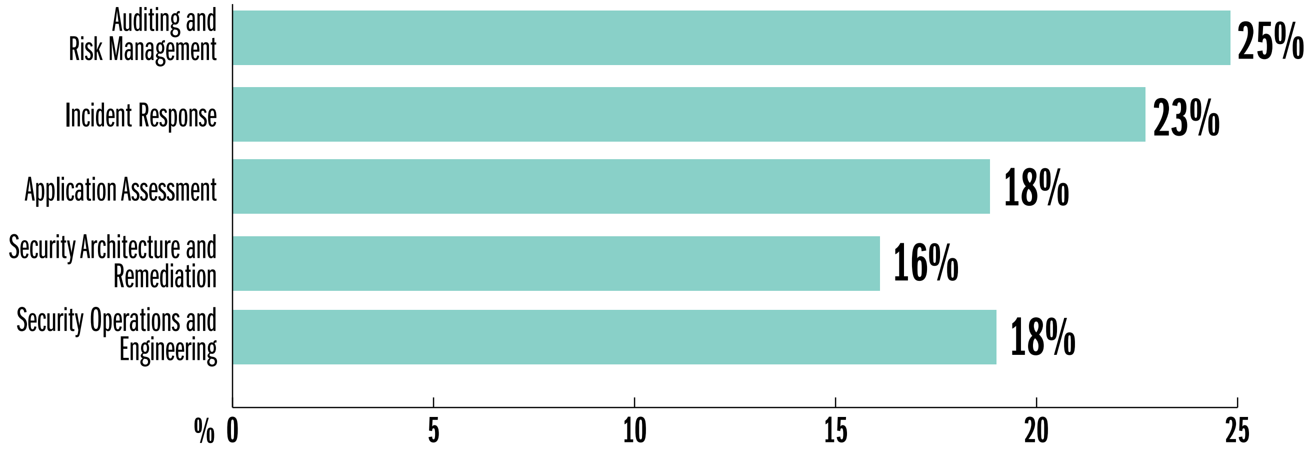
AT WHICH LEVEL DOES YOUR ORGANISATION FIND THE SKILLS SHORTAGE TO BE THE MOST ACUTE?



GRAPH 8: SKILLS SHORTAGE PAIN POINT.

All industries reviewed declared a challenge in finding top-tier professionals. About 70% of companies expect to face a huge talent short fall in 2019, all factors held constant. On the flip side, senior security managers are now in high demand, particularly in the financial services sector. Cross-company poaching is increasingly becoming a concern for organisations that can't keep up with competitive offers for their employees.

IN WHICH OF THE FOLLOWING AREAS IS THE CYBERSECURITY SKILLS GAP MOST APPARENT?



GRAPH 9: CYBERSECURITY SKILLS GAP.

05

DID YOU KNOW?

Secure Network Architecture and Design is the foundation of a secure business. Without a well-designed network and business process, an organisation cannot derive value from its cybersecurity investments.

Most respondents said that they faced a challenge in filling the role of audit, risk management and incident response. This is unsurprising given the numerous regulatory compliance requirements that came up in 2018.

Our analysis in 2017 highlighted the limited number of security architects and practitioners as one of the biggest problems facing the cybersecurity practice. This notion still stands in 2018.

Secure Network Architecture and Design is the foundation of a secure business. Without a well-designed network and business process, an organisation cannot derive value from its cybersecurity investments.

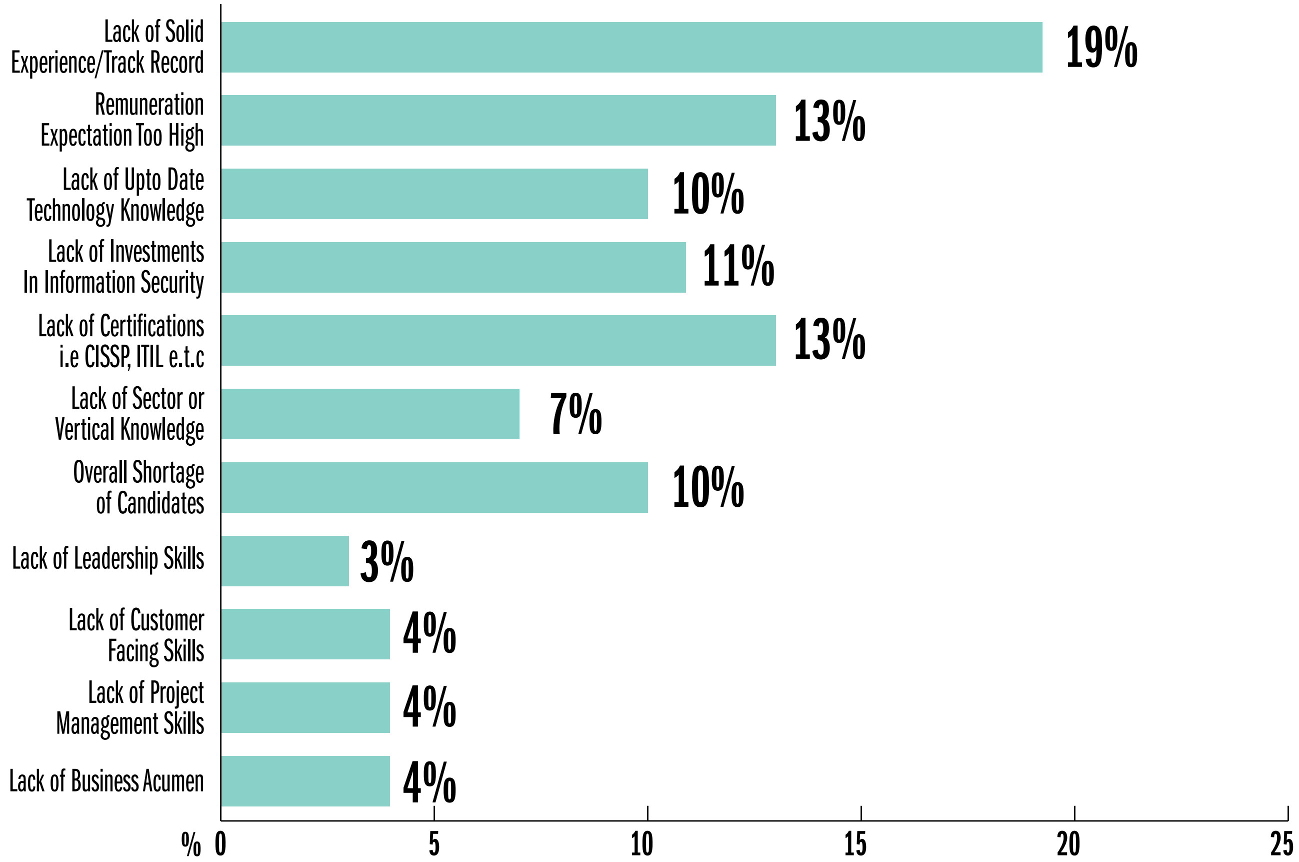
- A top notch cybersecurity manager will not be efficient if the organisation structure limits his mandate by having him report to e.g. finance.
- Investing in a SIEM will not add value if the network has not been properly segmented and baseline of activities (determining what's normal) established.

Security Architecture and Engineering allows an organisation to start with the very basics. Build a strong foundation upon which security technologies and processes can be build.

Security Architects would typically start by looking at the business, its goals and build the risks and threats that may arise. For example:

- **A bank** relies on the availability of their channels, security of their customer data and proper dispensation of monies occurring on a 24/7/365 basis to meet demand and generate revenue. System downtime or malicious transactions costs the organisation. With this understanding, the architect designs the network to be able to identify and withstand any threats and attacks that may lead to the successful exploitation of these dearly.
- **Legal firms** handle confidential information that could cost organisations millions of dollars, or even cost people their lives if in the wrong hands, a case in point being the panama papers. The conversations between legal partners and their clients are confidential. The fact that a third party could intercept these conversations could be the biggest threat a law firm faces. A security architect understands these threats and models a network that has proper segregation of access, data loss prevention and anti-tampering.
- **A biomedical company** focuses all of its effort on researching new pharmaceuticals. The data generated from this research is the nest egg of the organisation, and represents the combined results of the money provided by their investors. Should a competitor gain access to the information, it could potentially cause the entire organisation to fail. The possibility of theft of intellectual property could be the biggest threat faced by this biomedical company.

WHAT CONSTRAINTS DO YOU ENCOUNTER AS AN ORGANISATION WHEN RECRUITING EXPERIENCED CYBERSECURITY PROFESSIONALS?



GRAPH 10: RECRUITING CONSTRAINTS.

> IF YOU HAVE AN EDUCATION AND NO EXPERIENCE, YOU'RE GOING TO BE HARD-PRESSED TO FIND A CAREER IN THIS FIELD. YOU'VE GOT TO DO WHATEVER IT TAKES TO GET YOURSELF EXPERIENCE. THAT'S MORE IMPORTANT THAN ANYTHING.
>
> KEVIN HAWKINS, PROFESSOR OF IT AND DATABASE ADMINISTRATOR AT HUMANA HEALTH INSURANCE

Lack of solid experience is the leading constraint when recruiting Cybersecurity professionals. This was closely followed by high remuneration rates.

TALENT POACHING

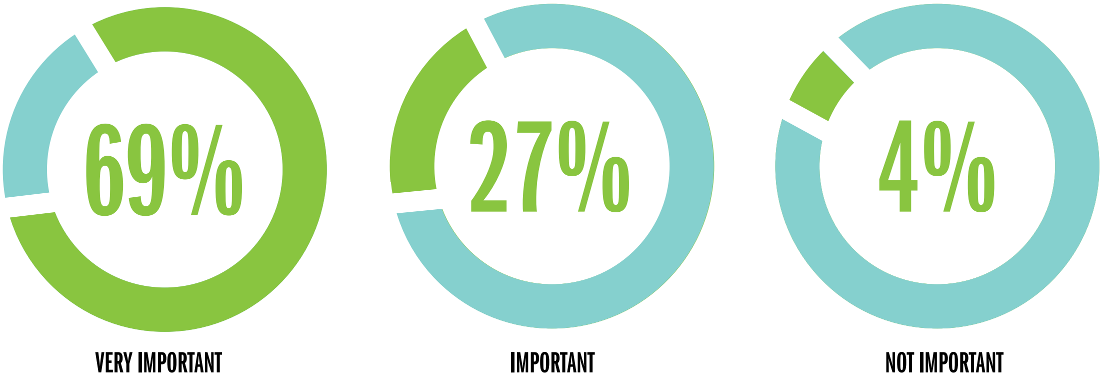
It is exceedingly difficult to hire new experienced professionals in an organisation. Why? Experienced cybersecurity professionals are in high demand, so organizations are engaged in a battle royale to coax them away from their present employers and outbid others for their services.

One fundamental fact that organisations should note however is: We should grow our own talent. Talent management is now a critical business strategy.

"Organisations spend large sums of money recruiting new employees rather than growing their own. The problem with this approach is that it causes frustration among existing employees who could have done the role just as effectively as a new recruit if they had been given training and a bit of encouragement."

WHAT IMPORTANCE DO YOU PLACE ON CERTIFICATIONS I.E. CISSP/CISA/CEH ETC?

CHART 9: IMPORTANCE OF CERTIFICATIONS.



Certifications are a crucial stepping stone for almost all careers. From our survey results, 98% of the respondents indicated that certificates are important. Clearly, certifications are resume worthy, but are they the end-all and be-all?

There is an obsession with high exam grades that has been promoted in the education system by most African countries. Consequently, even for employees and employers, more emphasis is placed on passing and gaining more certifications than actually understanding practical IT concepts.

CONCLUSIONS FROM THE SURVEY RESULTS.

- EMPLOYERS ARE LOOKING FOR CYBERSECURITY PROFESSIONALS AT SENIOR MANAGEMENT LEVELS.
- EMPLOYERS VALUE CERTIFICATIONS. (CEH, CISA, CISM, CISSP ETC)
- THE BIGGEST GAP THAT EMPLOYERS FACE WHEN HIRING IS LACK OF TECHNICAL EXPERIENCE CLOSELY FOLLOWED BY HIGH REMUNERATION DEMANDS.
- ORGANISATIONS ARE IN NEED OF NETWORK SECURITY ARCHITECTS WHO UNDERSTAND RISKS AND TECHNICAL CONTROLS NEED TO BE IMPLEMENTED.
- IT IS BETTER FOR AN ORGANISATION TO GROW ITS OWN TALENT THAN TO POACH.

INDUSTRY PLAYER PERSPECTIVE

MASIKA CHRISTINE

Digital Forensic Analyst, Applied Principal Consulting

TO WHAT EXTENT IS THE CYBER SECURITY KNOWLEDGE AND SKILL BEING DISPENSED IN YOUR VIEW?

The skills gap is huge. However, the government through the ministry of innovation and technology and NITA-U through their security department are training different departments between government ministry and agencies.

HOW WOULD YOU ASSESS THE NEED FORM THE PRIVATE SECTOR?

The private sector in the past two years have come to the realization that they need cyber security experts. 70% of the companies are conducting audits and trainings as a compliance requirement and not about as a means of closing actual gaps. Most banks rush to get Penetration tests done out of compliance as opposed to understanding their loopholes in their system. They are more reactive than proactive.

WHAT KEY CYBER SECURITY COMPETENCES ARE LACKING?

Hands on technical skills for Cyber Defence and Offense. Most companies are relying on tools and don't put much investment in equipping their employees with the relevant skills to operate these tools. Teams lack skills to Anticipate, Detect and Respond to cyber attacks.

DO YOU HAVE TOOLS THAT HELP YOU IN DELIVERING CYBER SECURITY CONTENT?

Yes.

We work with core impact when it comes to information security. Acunetix, Splunk.

With regards to digital forensics we are partners with Magnet forensics which delivers Axiom.

We also work with Cellebrite and NKS.

IS THERE A COHERENCE CROSS-INSTITUTIONAL STRATEGY IN CYBER SECURITY?

We have the National information security framework under NITAU. They have the mandate to implement cyber security from the public sector to the private sector. There is the National cyber security advisory group which is under NITAU. They tap into the private sector's knowledge.

WHAT NEW DIGITAL INITIATIVES HAVE INFLUENCED THE CYBER SPACE AND HOW HAS THIS IMPACTED BUSINESS GENERALLY?

E-commerce. Buying and selling through various online platforms. People use visa cards to pay for this which calls for stronger cyber security controls on the e-commerce sites.

Hotels use free Wi-Fi hence need for securing their network from rogue users.

DO YOU KNOW OF ANY CYBER-ATTACKS IN UGANDA?

There are cyber-attacks especially in the banking industries and the government. The challenge is we are not open about these attacks due to fear of brand reputation.

ANY ATTACKS YOU HAVE GOTTEN WIND OF?

ATM fraud. Direct attack on core banking systems and banks losing money.

THE MOST PROMINENT ATTACK YOU KNOW OF?

Direct attack on core banking systems.

WHAT'S YOUR VIEW ON CYBER SEC EMPLOYMENT OPPORTUNITIES FOR YOUNG PEOPLE?

Opportunities are there but employers are very reluctant to take on young talent because this means a lot of training and they want to jump right to someone who knows what they are doing.

Employers need to motivate young people to join their organizations.

WHAT CAN BE DONE TO ENSURE WE ATTRACT YOUNG TALENT?

Organizations need to be more open about taking their cyber security policies and cyber operations and hire people who are passionate within that field.

INDUSTRY PLAYER PERSPECTIVE

ADDRESSING CYBER SECURITY SKILLS GAP IN THE ENTERPRISE ENVIRONMENT

JOSEPH MATHENGE

Chief Operations Officer, Serianu Limited

“WHEN YOU WERE MADE A LEADER, YOU WEREN’T GIVEN A CROWN, YOU WERE GIVEN THE RESPONSIBILITY TO BRING OUT THE BEST IN OTHERS.” – JACK WELCH

The challenge to attract and retain skilled talent is arguably an age-old problem. One that probably has hundreds of books written about it as well as countless hours in formal training or conference sessions to understand. In stating so, it is therefore apparent that this is not a new challenge and there is no single perfect solution to resolve it.

That there is no single solution therefore presents the best chance to effectively manage it. In that there are probably several suggestions and recommendations that one can employ in finding what best works for your organisation.

Addressing the skills gap in cyber security in our region will require certain key fundamentals.

- Attract and hire the right candidate.
- Provide a challenging and interesting environment to keep them engaged and performing at a high level – Retention.
- Willingness and ability to let go when the moment is right for separation.

I will discuss these concepts in brief.

1. Attract the right candidate.

This is a fundamental step that requires some critical thinking in developing the Job Description used to advertise and hire as well as measure the fulfilment of the position.

a. What is the critical function of the role? What should the incumbent do on a daily, weekly and monthly basis. What is most important function that will be addressed in it? Is it technical e.g. configuring a firewall or an IDS or will the person need to lead in policy design and implementation.

b. Temperament of the ideal candidate. This seeks to understand what attitude and personality that would deliver effectively on the role. A technical person would need to show a desire to constantly sharpen these skills to keep pace with the ever-changing technology. A risk manager on the other hand may require strong analytical as well as technical writing skills in order to effectively advice the business on emerging risks.

c. Interest and challenge for a prospective respondent. A technical job can be arduous and consume long hours. It’s imperative to show to a prospective candidate that the role will hold their interest as well as present new challenges that require unique and timely resolutions.

2. Total compensation and benefits package.

In any given job we all expect to get paid. The difference comes down to an understanding of what a candidate believes they deserve and how the organisation measures up to that standard. A few may be lucky to get paid more than they anticipated while some may feel disgruntled in receiving far lower than they expected. Salary pay at the end of the month should however only make up one component of the total compensation package. There a number of considerations here in attracting and retaining the right candidate.

a. Right pay as measured by industry standard. This can be hard to establish particularly in a unique field like cyber security. It is imperative however that organisation seeks to learn what other organisations like them are paying and ensure that the match or exceed it where possible.

b. Bonus and/or employee stock options. Bonuses and stock options offer an extension of the base pay. In it, an organisation provides additional payment dependent on the performance of both the individual and the company and as all do well additional monies can be paid out. I find this to be a motivator for an individual to not only do their job, but also gain an understanding of the business model being executed and how they contribute to it. Done well, the bonus pay-out as well as stock options endears the individual to the organisation.

c. Other financial compensation - health insurance, retirement planning. An organisation needs to show an interest and investment in the well-being of their people. The human body occasionally breaks down and may require medical attention to recover. A well-designed wellness program that includes medical insurance coverage including dental and vision goes a long way in showing this. Building in sick days separate from leave days that an individual can use during an illness shows this as well. As we get older and not able to work as well there needs to be a plan for retirement that is partial sponsored by employers.

3. Retain the talent.

Retention of Cyber Security skilled personnel is a skill on its own. It is a difficult task to find and train these skills and as such an organisation needs to invest in retaining them.

a. Recognize and reward performance. In the section above, we delved into financial compensation as a tool to attract candidates. In retaining them we take this further in finding non-monetary methods to recognize and reward performance. Everyone likes to be appreciated and it occurring at the work place is very rewarding. Organisations need to build in rewards such as discretionary leave days, a night out for dinner or to the movies or even company retreats to add avenues to reward performances.

b. b.Opportunity for career growth. We spend a significant time of our days at the work place. We must then be able to see a path of growth that creates a motivation beyond the financial benefits of a job. Skilled talent with opportunity and career growth path within the organisation will tend to remain steady as they work their way through the organisation structure. You must show a career growth path and also show how one can fairly work towards it and achieve it.

c. Technical training and conferences. Cyber security is a dynamic field. The most skilled individuals spend time and resources to keep up with the field. As an organisation, it is imperative that we participate in this upskilling in both encouraging individuals to seek it as well as promoting it by sponsoring some technical training and attendance of security conferences. In challenging individuals learn a new skill every year as well as encouraging them to attend conferences where they can meet and network with other professionals is key in retaining them.

4. Be willing to let go.

We have argued extensively about encouraging self-development and career growth. This can be a double edge sword as the more skilled an individual becomes the more attractive to others and risks the valuable employee in getting 'poached'. This is okay. Work very hard to both attract and retain the talent in offering a unique work environment but be able to let go. It's important that we allow the individual to explore and exploit their potential including pursuit of opportunities outside of the organisation.

In conclusion, managing skilled talent requires deliberate action. Finding the right candidate that possess the skills to perform the task at hand and ensuring that you do everything to retain them. But perhaps most importantly in all this is to inspire and create the environment that brings out the very best in them.

THE GENDER GAP

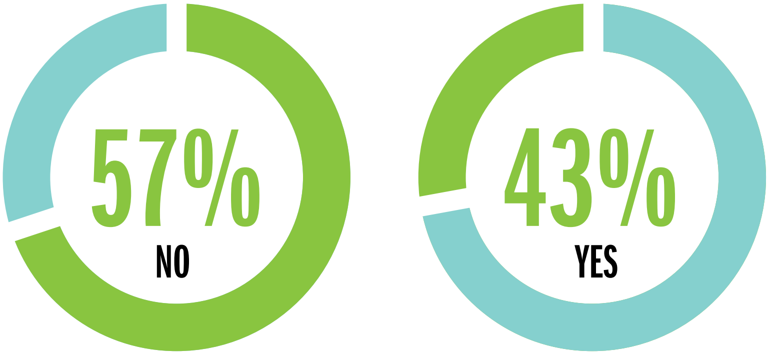
Jobs in Cybersecurity are exploding, but why aren't women in the picture? Research shows that women make up only 20% of the cybersecurity workforce globally according to Research firm Frost and Sullivan. In Africa, this figure is 10% as estimated by Serianu.

AS UGANDA DEVELOPS IT'S SILICON SAVANNA, ONE QUESTION STILL STANDS, WHERE ARE THE LADIES?

WE ASKED OUR RESPONDENTS TO PROVIDE THEIR VIEWS.

CYBERSECURITY INDUSTRY IS FAILING TO ATTRACT YOUNG TALENT AND WOMEN INTO THE PROFESSION. DO YOU AGREE WITH THIS STATEMENT

CHART 10: IS THE CYBERSECURITY INDUSTRY FAILING TO ATTRACT YOUNG TALENT AND WOMENT?.



Interestingly, majority of the respondents indicated that they did not agree with this statement. It's important to point out that majority of the respondents were male. However, the gender gap discussion is not really one of right versus wrong or men versus women but rather diversity.

Diversity is a good business strategy as different people present different technical, leadership and management skills.

GENDER GAP ISSUES

It is not so much as failing to attract women but a matter of retaining them. Arguments to be made here include;

- Women do not get promoted at the same rate as men are, and
- Women are not getting salary increases at the same rate as men are even though they are asking for and applying at the same rate.
- As a rule, women wait until they accrue required skills before applying for cybersecurity jobs, while men routinely bluff their way through. The men may have none of (the skills) and will still apply.

A number of non-profit groups and private companies have now come out to actively promote training to get younger girls involved in Information Security.

LIES WOMEN TELL THEMSELVES FOR NOT WORKING IN IT:

"I AM NOT GOOD ENOUGH."

"I AM WAITING TO GAIN THE RIGHT EXPERIENCE BEFORE I APPLY FOR THE JOB."

"THAT'S A MAN'S JOB."

"I AM OKAY WHERE I AM."

"BEING A SOFTWARE DEVELOPER DOES NOT BRING OUT MY UNIQUENESS AS A WOMAN."

"WHEN I YOUNG I WAS INTERESTED IN SCIENCE AND TECHNOLOGY"

"IT IS THE BOYS CLUB"

"THERE ARE TOO MANY MEN"

"THERE ARE TOO MANY WOMEN"

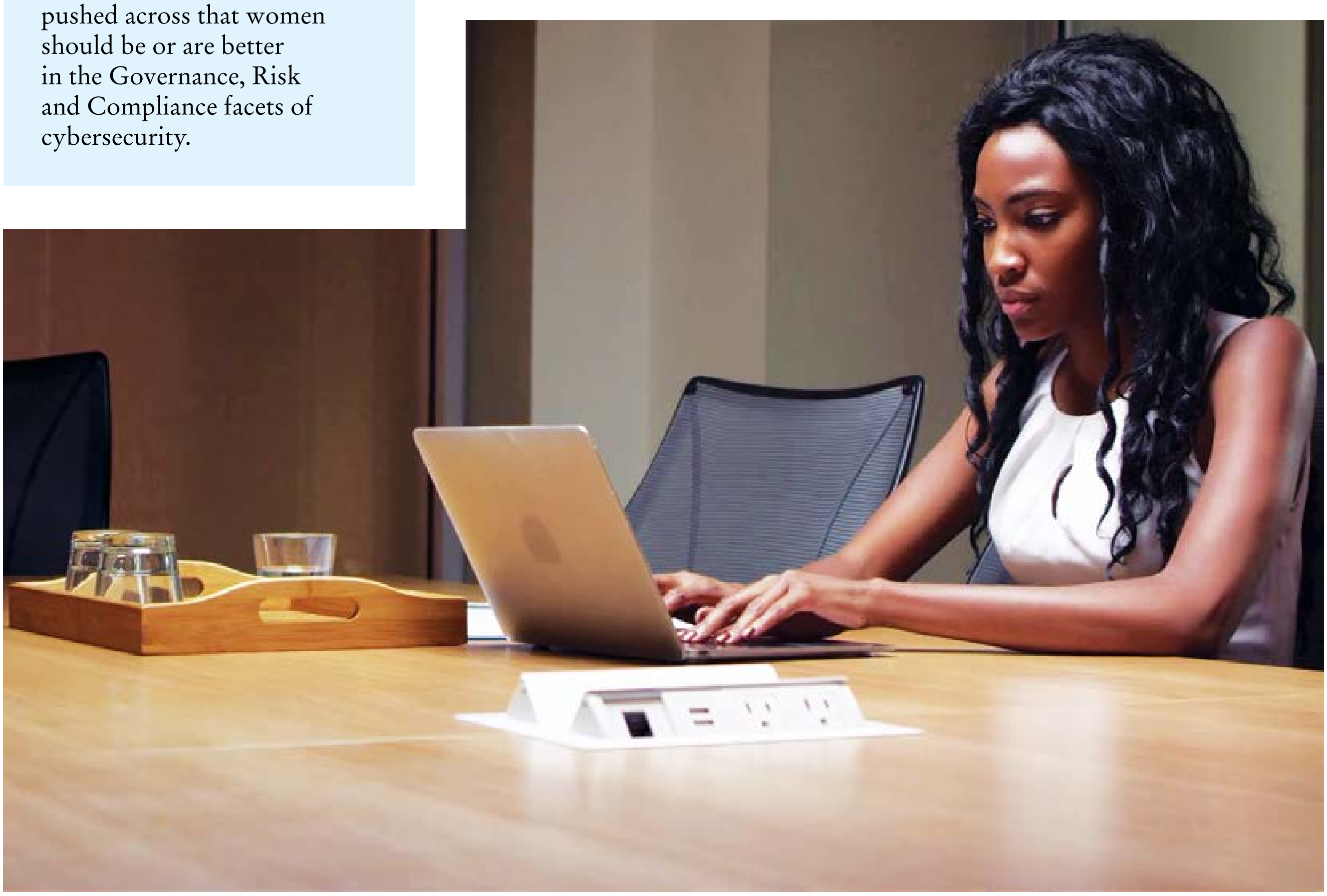
THE TECHNICAL SKILLS QUESTIONS?

Technical capabilities of women is always a contentious topic. We acknowledge the steady increase of women in cybersecurity due to all initiatives aimed at growing and retaining those numbers, and especially notable progress in Information Security; Governance Risk and Compliance. However, it would be imprudent not to acknowledge that the numbers specifically in the technical facets of cybersecurity are wanting. There is a notion pushed across that women should be or are better in the Governance, Risk and Compliance facets of cybersecurity.

Of course, there are some notable women who are in Governance, Risk and Compliance out of deep passion and not picking the "easy" way.

But if you look closely, an interesting fact emerges: Only about a third of the women pursue network engineering, penetration testing and coding. On the other hand, two-thirds of the men pursue the more technical roles such as penetration testing, coding and participate in hackathons.

None of the above paths is better than the other, however, mastering the core of the craft should be a priority for all genders. The fundamental blocks of cybersecurity come from possessing in-depth understanding of your working tools - Networks and Technologies. Majority of the women are seen to be "around tech" more than they are "in tech". Main difference being, one is able to utilize technical skills to compromise or defend the network.



SKILLS MISMATCH-ARE YOU HIRING THE RIGHT PERSON, FOR THE RIGHT JOB?

It is easier for organisations and all stakeholders within the Cybersecurity eco-system to squarely blame "skills shortage" as the key contributor to the skills gap problem.

However, a review of majority of our hiring processes reveals:

- Employers don't clearly define cybersecurity roles that need to be filled
- Applicants are desperate for jobs and apply for roles that they do not fully understand
- Students lack the hands-on expertise that most employers are looking for.
- Interviewers often use "instinct" to determine if a candidate would fit into the specific role.

ACIC's Competency matrix (derived from NICE framework and Mark Carney's Skills matrix) is a resource that matches roles to desired and necessary skills. This matrix is designed to aid better facilitation of hiring decisions for CISOs, hiring managers, and as a guide to students and educators.

The main users of the Matrix are recruiters, employers, HR managers, CIOs, trainers and academics.

COMPONENTS OF ACIC'S COMPETENCY MATRIX

There are 4 categories as borrowed from the CVEQ framework. These are Anticipate, Detect, Respond and Contain. All Cybersecurity roles have been mapped into one or more of these categories.

There are 4 specialty areas in the competency matrix. These are Risk Management, Vulnerability Management, Incident Response and Threat Intelligence. Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work.

There are 16 roles in the competency matrix. These are defined as the specific activities that a security professional is involved in. Employees can have more than one role.

Attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.

> “
>
> IF STUDENTS KNEW BETTER WHAT TO LEARN, EDUCATORS KNEW BETTER WHAT THEY NEEDED TO TEACH, AND HIRING AND TECH MANAGERS KNEW BETTER WHAT TO LOOK FOR WHEN HIRING, THEN BUSINESSES WILL BE BETTER PROTECTED AGAINST THREATS.
>
> MARK CARNEY

ACIC'S COMPETENCY MATRIX

		Cyber Visibility and Exposure Quantification (CVEQ™) Framework	ISO 27001 Clauses, Annex A Requirements	PCI DSS Requirements	NIST Requirements	COBIT Framework	Industry Specific Cybersecurity Guidelines	Networking Concepts (OSI Model, Protocols)	Windows Secure Configuration and Hardening Process and Tools	Linux Secure Configuration and Hardening Process and Tools	Windows OS Administration Concepts - AD Intergration Configurations	Virtual Environment Security Configurations	Network Devices Set Up, Configuration and Hardening, (Firewall, Loadbalancer, Switch, Router
ANTICIPATE	**Risk Management**												
	Risk Analyst	3	3	3	3	3	3	2	0	0	0	0	0
	Compliance Analyst	3	3	3	3	3	3	2	1	1	1	1	1
	IT Security Auditor	3	3	3	3	3	3	2	2	2	2	2	2
	Security Engineer	2	2	2	2	2	2	3	3	3	3	3	3
	Security Architect	2	2	2	2	2	2	3	3	3	3	3	3
DETECT	**Vulnerability Management**												
	Web Pentester	0	1	0	1	0	1	2	2	2	0	0	0
	Mobile Pentester	0	1	0	1	0	1	2	2	2	0	0	0
	Network Pentester	0	1	0	1	0	1	3	3	3	3	3	3
	Patching Analyst	0	1	0	1	0	1	2	2	2	2	2	2
RESPOND	**Incident Management**												
	Breach Scenario Analyst	2	1	1	1	1	1	2	2	2	2	2	2
	Soc Analyst	1	1	1	1	1	1	3	2	2	2	2	2
	Intel and Trending Analyst	1	1	1	1	1	1	1	1	1	1	1	1
	Malware Analyst	0	0	0	0	0	0	3	0	0	0	0	0
	Forensic Analyst	0	0	0	1	0	3	3	2	2	2	2	1
CONTAIN	**Threat Management**												
	Threat Hunting Analyst	1	0	0	0	0	1	3	2	2	2	2	2
	Remediation Specialist	2	0	0	0	0	2	3	3	3	3	3	3
	Development Specialist	1	1	1	1	0	3	3	2	2	2	2	2

TABLE 2: ACIC'S COMPETENCY MATRIX.

0 Not Applicable   1 General Knowledge

	Reporting Skills	Application Architecture (Client, Server and Database)	Web Protocols (Rest APIS, SOAP APIs, XML)	Owasp Top 10	Mobile Application Architecture (IOS, Android)	Code Reviews/Programming Languages	Presentation Skills	Network Exploitation Tools (Kali Linux)	Open Source Intelligence Tools	Intrusion Detection And Prevention Techniques	Understanding of Windows Event Logs	Understanding of Network Logs (Firewall and Antivirus)	Scripting and Parser Creation	Siem Management - (Setup, Rule Fine-Tuning and Device Intergration.)	Analytics and Graphical Representation Techniques (Excel, Kibana)	System Imaging Techniques	Data Recovery Techniques	Legal Procedures For Cybersecurity Prosecution
🟥																		
	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0
	2	1	1	1	1	1	1	2	2	2	1	1	0	1	1	0	0	0
	2	3	3	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1
	3	3	3	3	3	3	1	2	2	2	2	2	2	2	2	2	2	2
🟦																		
	2	3	3	3	3	3	0	0	0	0	0	0	2	0	1	0	0	0
	2	2	2	3	3	3	0	0	2	0	0	0	2	0	1	0	0	0
	2	1	1	1	1	1	0	3	3	3	2	0	2	0	1	0	0	0
	2	1	1	1	1	1	0	0	0	0	2	0	2	0	1	0	2	0
🟩																		
	3	2	2	2	2	2	3	2	2	2	2	2	2	2	1	2	2	0
	3	2	2	2	2	0	3	2	2	2	3	3	3	3	3	3	3	1
	3	1	1	1	1	1	3	1	1	1	2	2	2	2	3	1	0	0
	2	2	1	1	2	3	0	0	0	2	1	2	2	0	1	2	2	0
	3	1	1	1	1	1	3	1	1	1	3	3	2	1	3	3	3	3
🟧																		
	3	2	2	2	2	2	3	2	2	2	3	3	1	2	3	0	0	0
	2	2	2	3	2	0	0	0	2	0	0	1	2	0	1	3	3	0
	2	3	3	3	3	3	0	0	0	0	0	0	3	0	1	0	0	0

2 Good Understanding

3 Expert Understanding

AFRICA CYBER IMMERSION CENTRE

Africa Cyber Immersion Centre
acic
Engage | Educate | Empower

Bridging the Skills Gap

The Africa Cyber Immersion Centre (ACIC) 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.

PARENTAL CONTROL

Raising children in this interconnected era has become more challenging than ever. The internet can be a fantastic educational tool, but without parental control software and careful supervision it can be a dangerous place. Here are some of the critical concerns from parents:

TIPS FOR ENSURING MY KID'S ONLINE BEHAVIOR?

- Browser history (Chrome: Ctr+H).
- YouTube watch history and the list of suggested material.
- Check Cookies history.

Limitation: Kids have become very tech savvy and have found ways of hiding their online activity from parents by:

- Clearing their search history and/or cookies on their browser
- Using private browsing feature so their parents can't see the sites they've hit (Info provided by "Enough is enough")

So the most effective way is to use a parental control. It allows parents to monitor online activity (social media, sites) unpredictably for a kid and, if needed, block a private browsing feature.

WHAT PARENTAL SOFTWARE CAN I USE?

- OpenDNS FamilyShield: Block domains on your whole home network at router level
- KidLogger: A simple way to record your children's computing activity for your peace of mind
- Spyrix Free Keylogger: Find out what your kids are typing, and if they might be in trouble
- Kiddle: A kid-friendly search engine that's ideal for researching

YOU CAN CATCH UP WITH YOUR TECH-SAVVY KID IF YOU;

- Explore the different technologies together with your kids
- Provide suggestions to the type of games, apps or sites that your kids can use
- Subscribe to digital journals about cybersecurity and IT

Engage, Educate & Empower

MASTERING THE FOUNDATION

Cybersecurity is a wide field. Structuring a single university program around this can be impractical. We therefore need to build basic fundamental skills-sets such as networking, programming, database administration, computer architecture, cryptography and working with Linux systems. Inadequacy to incorporate practical learning in the above fundamentals adds to the skill-gap referenced by employers.

WAY-FORWARD

Following the findings on the skill-gap in Uganda and Africa in general, we point out some recommendations for the Government, Academia, and Employers.

GOVERNMENT

The Government should consider giving grants and or tax breaks to companies and organisations that train cybersecurity professionals.

The government should be alive to the realities of cyberwars.

ACADEMIA

Academic institutions need to incorporate cybersecurity courses in their curriculum with an emphasis on practical hands-on learning for ICT programs. This may require liaising with employers to get the actual necessary skills in the market. Hands-on learning can be furthered through internship and apprenticeship, hackathons, cyber-ranges and specific competitions, these can be carried out in liaison with potential employers.

EMPLOYERS

Organisations need to work with academic institutions to relay the necessary practical skills needed in the market. This will streamline education programs to fit market needs and benefit organisations with skilled personnel.

It is necessary to consider training current employees and progressively developing in house talent to match the cybersecurity needs of the company. It is generally considered more cost effective.

> “
>
> OUR EXPERIENCE IN CYBER SECURITY CAN BE SAID TO START MORE OR LESS FROM OUR CURRENT SYLLABUS WHICH ONLY GIVES US THE MOST BASIC INFORMATION AND MAKES US A BIT PRIVY ON WHAT CYBER SECURITY ENTAILS. ONE OF OUR SOURCES OF INFORMATION IS THE INTERNET WHICH HAS HELPED US TO ACQUIRE KNOWLEDGE ON THE DEVELOPMENT OF APPLICATIONS AND WAYS TO SAFEGUARD THEM AGAINST ATTACKS. ALTHOUGH THE INTERNET CONTAINS A VAST AMOUNT OF INFORMATION, GUIDANCE IN UNDERSTANDING AND MITIGATING THREATS WITHIN OUR ENVIRONMENT HAS BEEN A CHALLENGE. RECENTLY, WE WERE GRACED WITH THE OPPORTUNITY OF LEARNING MORE AND BEING EXPOSED TO THE VAST AREA OF CYBER SECURITY OFFERED BY THE AFRICA CYBER IMMERSION CLUB (ACIC) WHICH HAS ENABLED US TO GAIN MORE INSIGHT AND FOR WHICH WE ARE HUMBLED AND EXTEND OUR SINCERE ARM OF APPRECIATION AND GRATITUDE.
>
> **STUDENT, KAPSABET BOYS HIGH SCHOOL**

CHALLENGES FACING HIGH SCHOOL TEACHERS

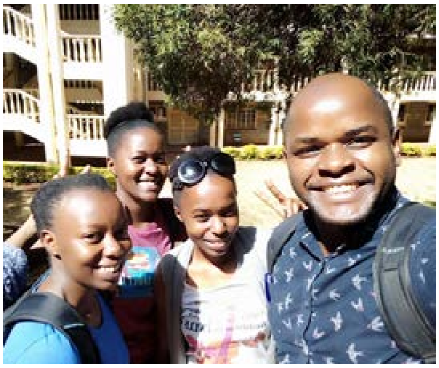
A large number of teachers are widely affected by cyber-attacks but do not have the skills to safeguard themselves against these attacks. There are no existing regulations that require teachers to acquire cyber security-based trainings yet they are mandated to safeguard their personal, school and student data with high priority and also answer intuitive questions from their students. The education system faces cyber threats from threat actors such as students, faculty and staff which has been observed through the years. The Academia sector requires a strategic cybersecurity approach as we continuously embrace technology in our schools.

Information sharing is also a challenge within the Academia sector. Teachers are sometimes reluctant to share cyber security-based issues that affect them due to a lack of knowledge or lack of access to industry specialists who can help advise on issues.

Another challenge exists within the full integration of ICT and cybersecurity skills in the school curriculum within the education system as a means of reducing the number of cybersecurity attacks targeting individuals. The government has supported the inclusion of ICT in the academia sector but has not invested in implementing regular awareness trainings on cyber based threats among teachers, students and citizens in general.

The creation of the ICT club has for some time has now served as a platform through which students (club members) acquire the relevant skills needed when dealing with cyber-related issues and the computer world in general but input is still required in order to keep up to date with vectors of attacks and how to safeguard ourselves.

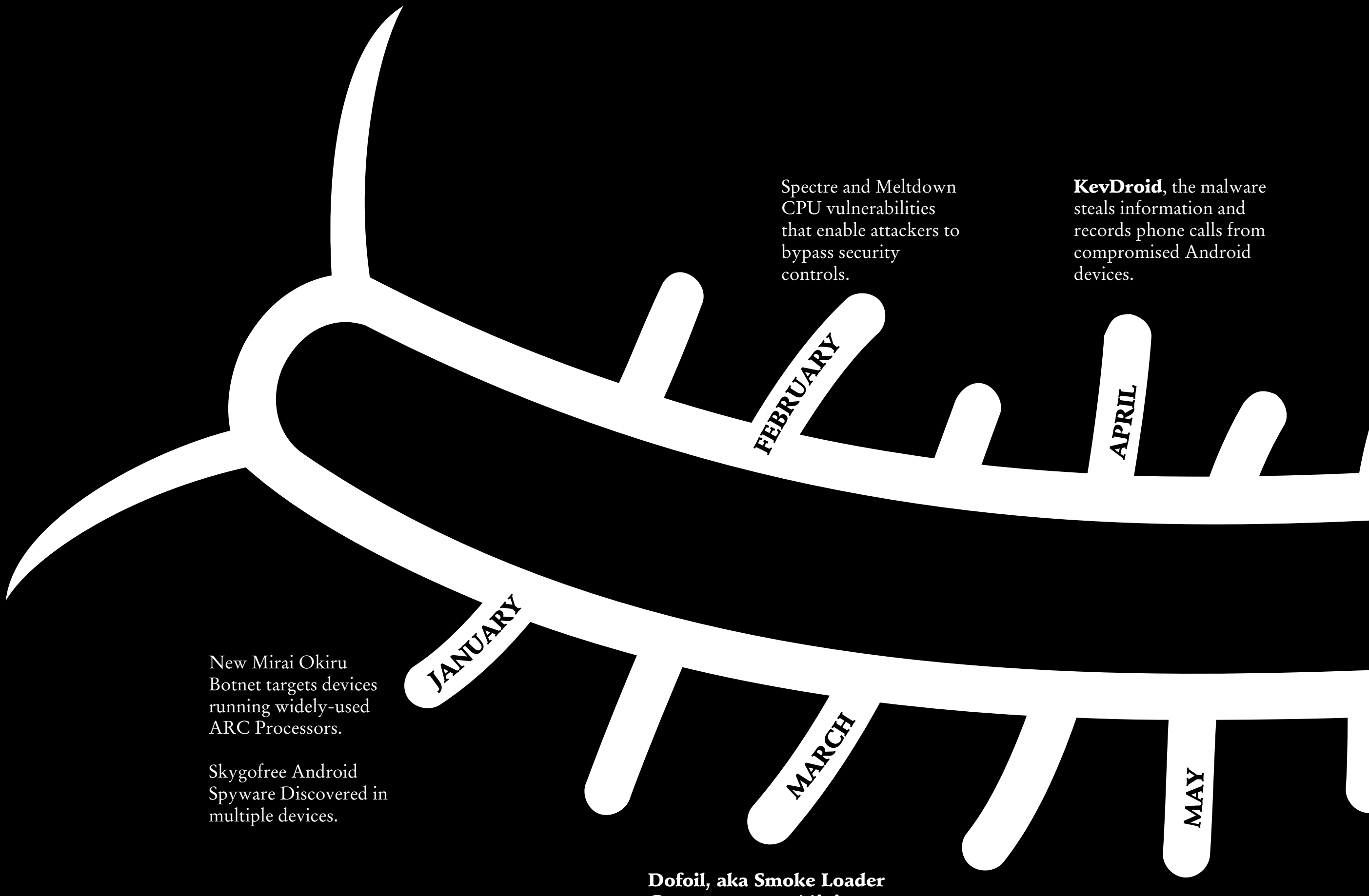
GEOFFREY OSORO, COMPUTER STUDIES TEACHER, KAPSABET HIGH SCHOOL



KAPSABET HIGH SCHOOL

CYBER INTELLIGENCE

LATEST MALWARE VIRUSES THAT WERE RELEASED AND CAPTURED IN 2018.



New Mirai Okiru Botnet targets devices running widely-used ARC Processors.

Skygofree Android Spyware Discovered in multiple devices.

Spectre and Meltdown CPU vulnerabilities that enable attackers to bypass security controls.

Dofoil, aka Smoke Loader Cryptocurrency Mining Malware Infected Over 500,000 PCs in just Few Hours.

Global ISPs inject **Cryptocurrency Mining Scripts** and spyware into users' Web Browsers.

KevDroid, the malware steals information and records phone calls from compromised Android devices.

Cryptomining Malware Digs into Nearly 40% of Organizations Globally.

Prowli Malware Infected Over 40,000 Servers, Modems, and IoT Devices.

MyloBot – Highly Sophisticated Botnet Shutdowns Windows Defender and windows update.

FakeSpy – Android Information Stealing Malware Attack to Steal Text Messages, Call Records & Contacts.

MysteryBot; a new Android banking Trojan for Android 7 and 8.

Dark Tequila – Banking Malware is designed to steal victim's financial information, as well as login credentials.

Triout is an Android Spyware Framework being used to turn legitimate apps into spyware.

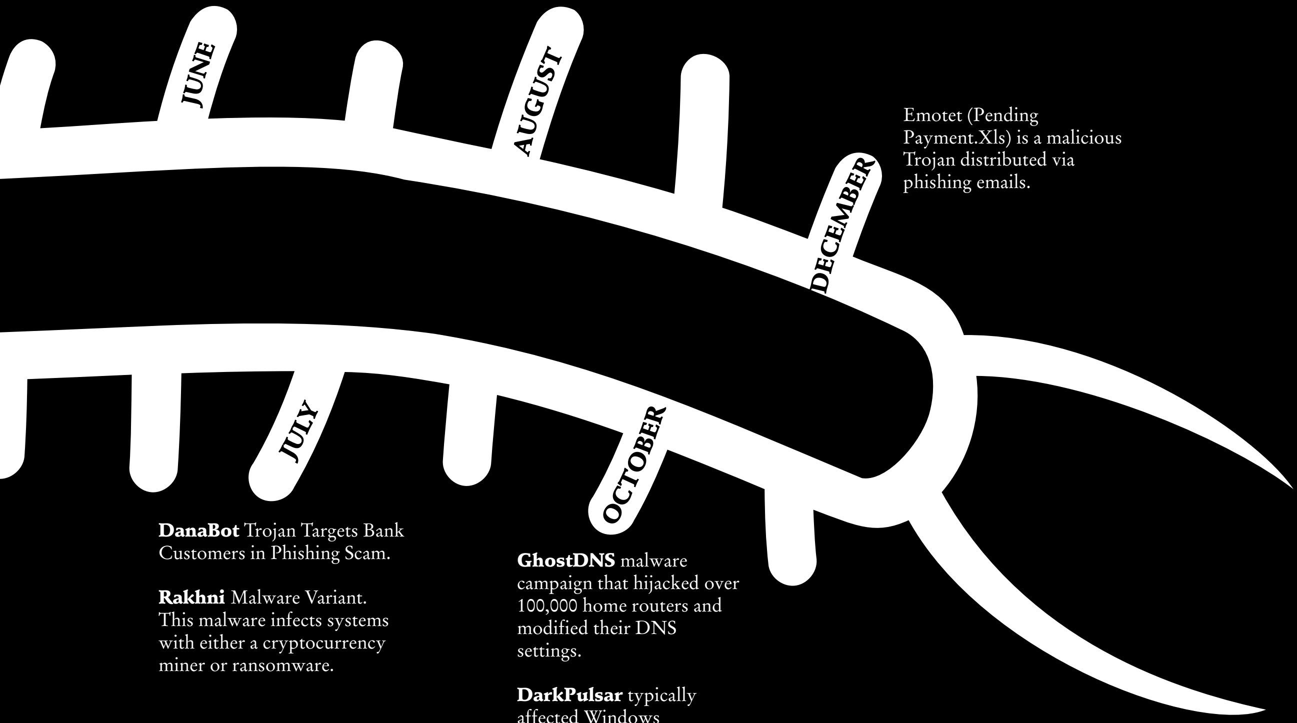
Locally re- engineered Malware discovered by the ACIC team;

Betaversion Malware
MD5 hash value: e86c626878a0c693d3727024d55ff882

Scr.exe Malware:
MD5 hash value: f05a31ae604e4ea844e8130e45d30f01

Taskrun Malware:
MD5 hash value: f2223193031768286296c5c70990d63d

Scvhost.exe Malware:
MD5 hash value: f2223193031768286296c5c70990d63d



Emotet (Pending Payment.Xls) is a malicious Trojan distributed via phishing emails.

DanaBot Trojan Targets Bank Customers in Phishing Scam.

Rakhni Malware Variant. This malware infects systems with either a cryptocurrency miner or ransomware.

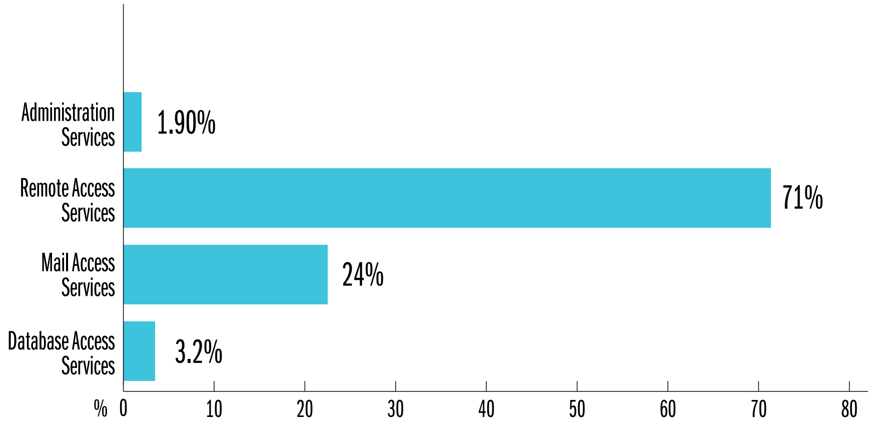
GhostDNS malware campaign that hijacked over 100,000 home routers and modified their DNS settings.

DarkPulsar typically affected Windows 2003/2008 servers. It runs malicious code

OPEN PORTS

Based on our analysis we identified that system administrators have been exposing critical services that should be limited to internal environments.

We classified them into the following categories::

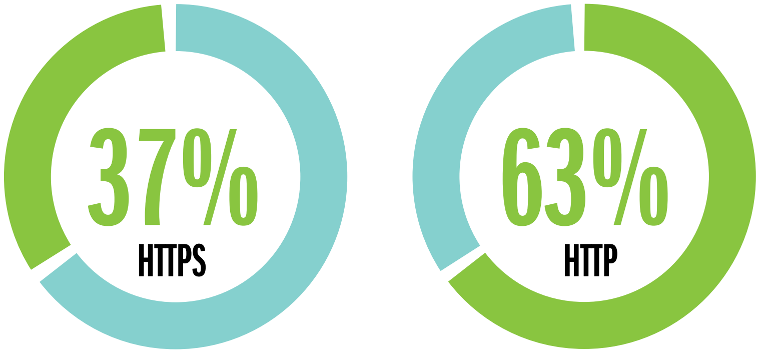


GRAPH 12: EXTERNALLY ACCESSIBLE SERVICES.

WEB SERVICES

Attackers are using web applications as a means of gaining access to critical services

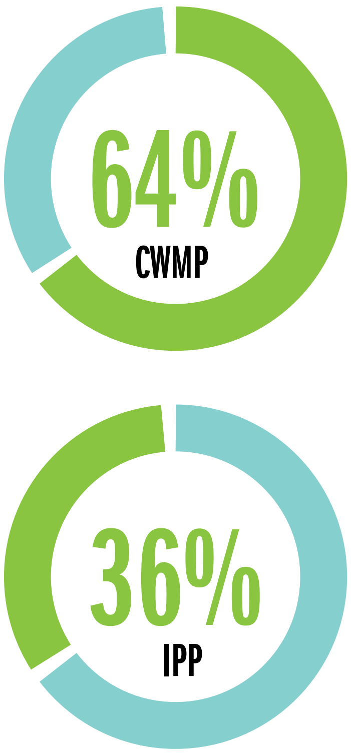
CHART 11: WEB SERVICES.



ADMINISTRATION SERVICES

These are protocols that allow system administrators to configure their devices. We noted that (1.90%) of the active ports hosted administrative services. In Uganda, the CPE WAN Management Protocol (CWMP) port (64%) used for remote router management by ISPs and (IPP) - Internet Printing Protocol (36%) were accessible under this category.

CHART 12: ADMINISTRATION SERVICES.



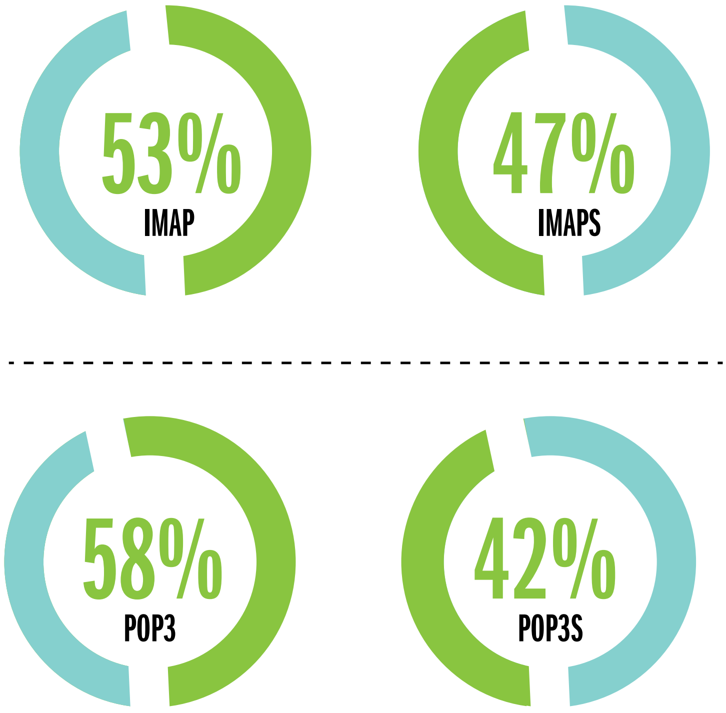
CUPS manages print jobs and queues and provides network printing while CWMP protocol enables devices to be remotely configured through the use of SOAP based Remote Procedure Calls (RPC).

- In 2016, port 7547 (CWMP) was a target of Mirai botnet due to a Remote Code Execution vulnerability.
- CUPS port is vulnerable to Denial of Service (DoS) attacks through CPU consumption.
- CUPS has a vast array of exploits that can be used to remotely execute code.

MAIL ACCESS SERVICES

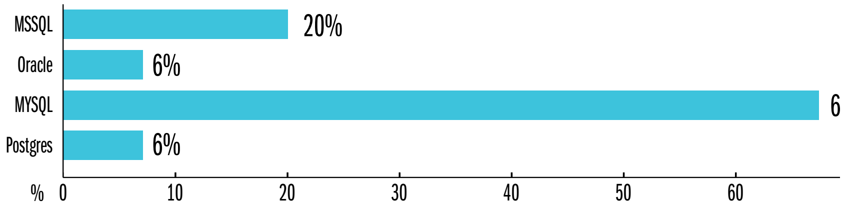
UGANDA

CHART 13: MAIL ACCESS SERVICES.



DATABASE ACCESS SERVICES

UGANDA



CRYPTO MINING

During our analysis we identified 12,975 African servers hosting Crypto Mining scripts that silently mine cryptocurrencies from users that access the webpage containing the embedded mining script.

The top (10) countries hosting the crypto mining scripts.

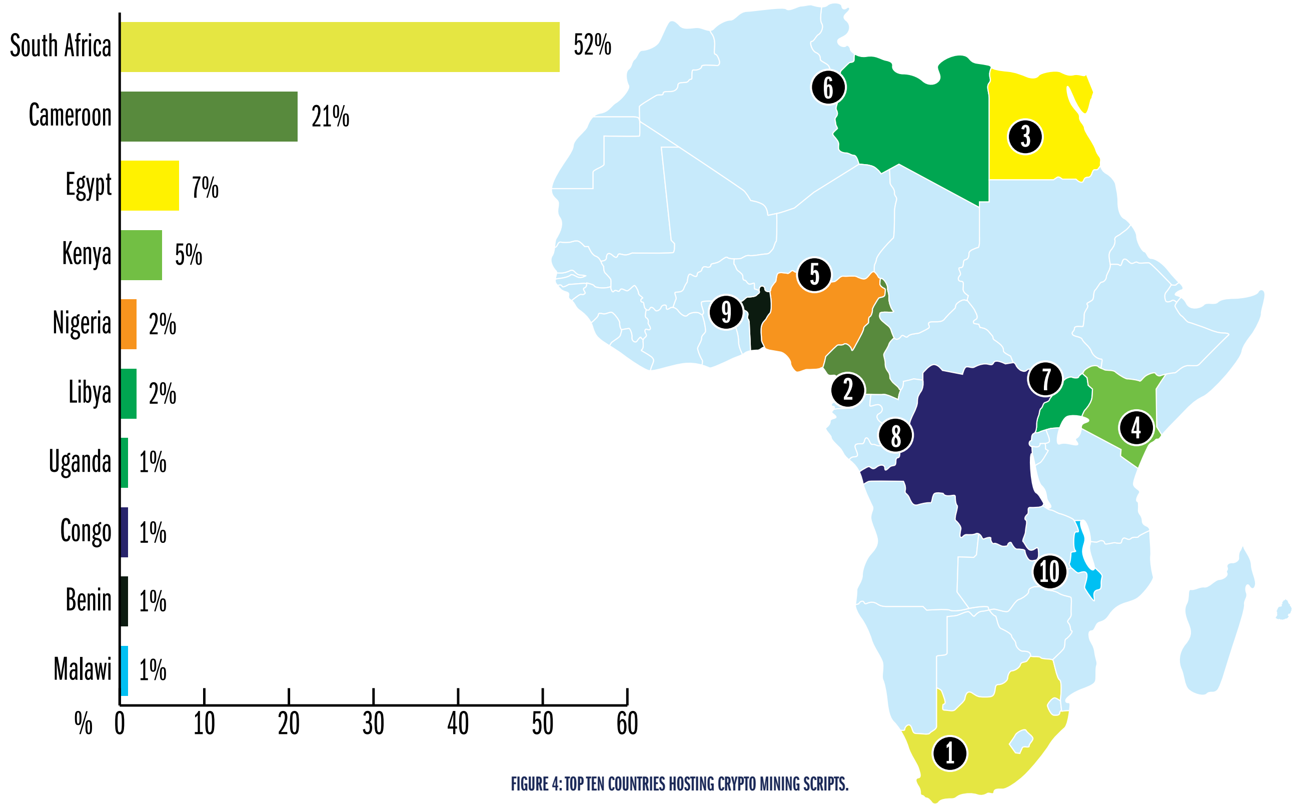


FIGURE 4: TOP TEN COUNTRIES HOSTING CRYPTO MINING SCRIPTS.

RASPBIAN ADOPTION

The technology growth is fueled by the need to automate and achieve deeper insight into existing data through analysis. With the use of IoT technology, people are now creating simple solutions to monitor or secure their existing infrastructure. IoT technology relies on the internet as a means of distribution of data or easy externa access.

Africa is currently embracing the same technology but have not implemented security controls to prevent access to the IoT based technology. Based on our analysis, we identified the following existing technology accessible online

RASPBERRY PI

Raspberry PI is an open source tiny and affordable computer mainly used in educating people on computing. It runs on a Raspbian operating system which is based on Debian. The device can be used as an IoT device and also be configured to run hacking software.

Based on our research, we were able to identify over 120 devices using the Raspbian operating system:

The top 10 countries using the Raspbian include: See Figure 5

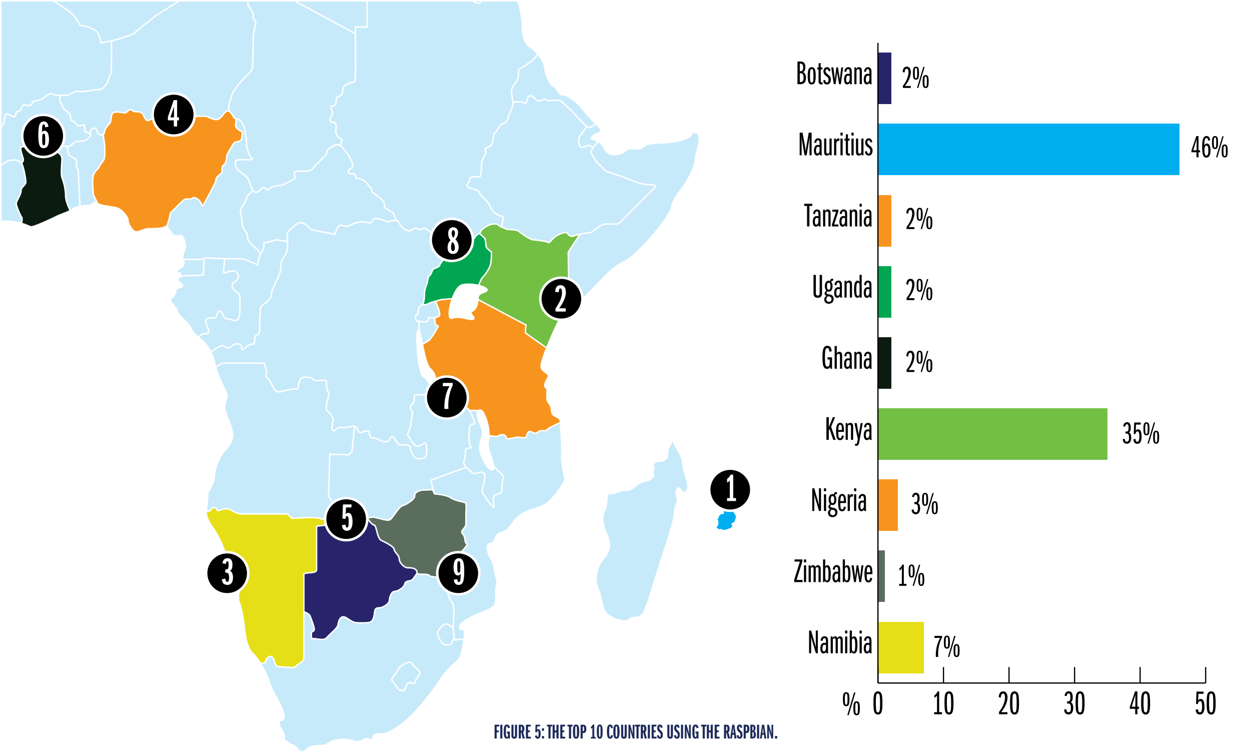
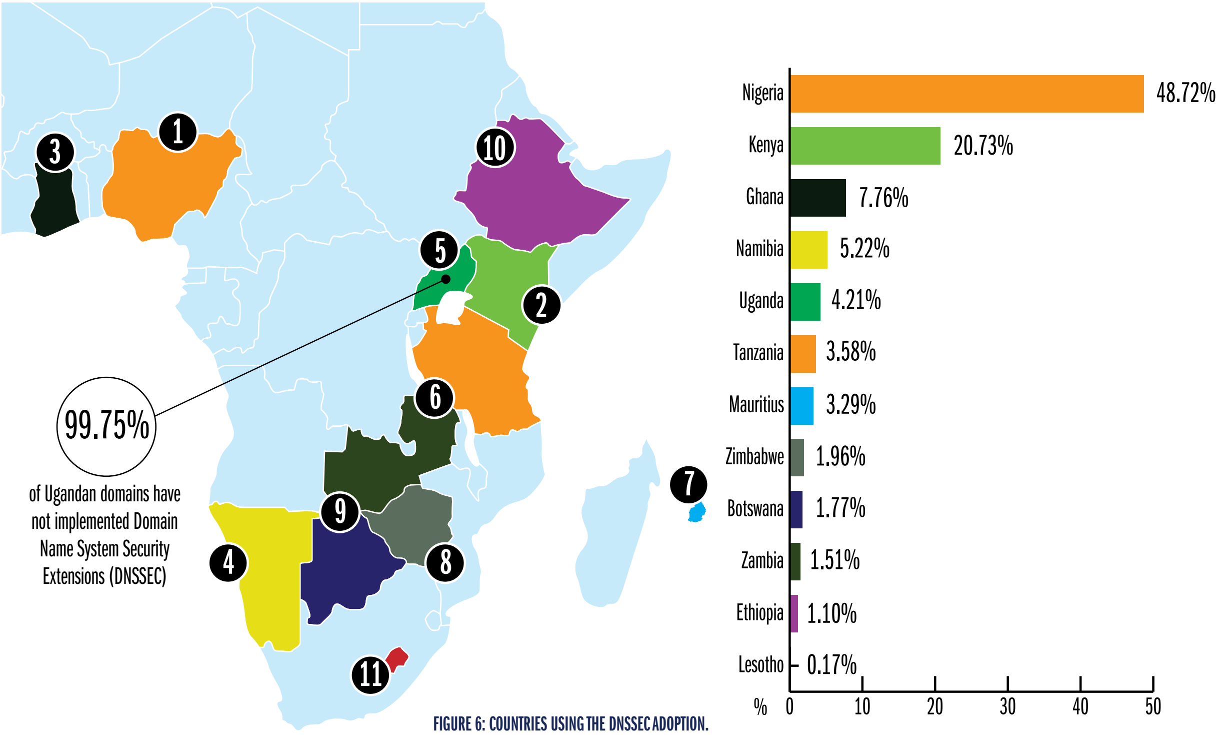


FIGURE 5: THE TOP 10 COUNTRIES USING THE RASPBIAN.

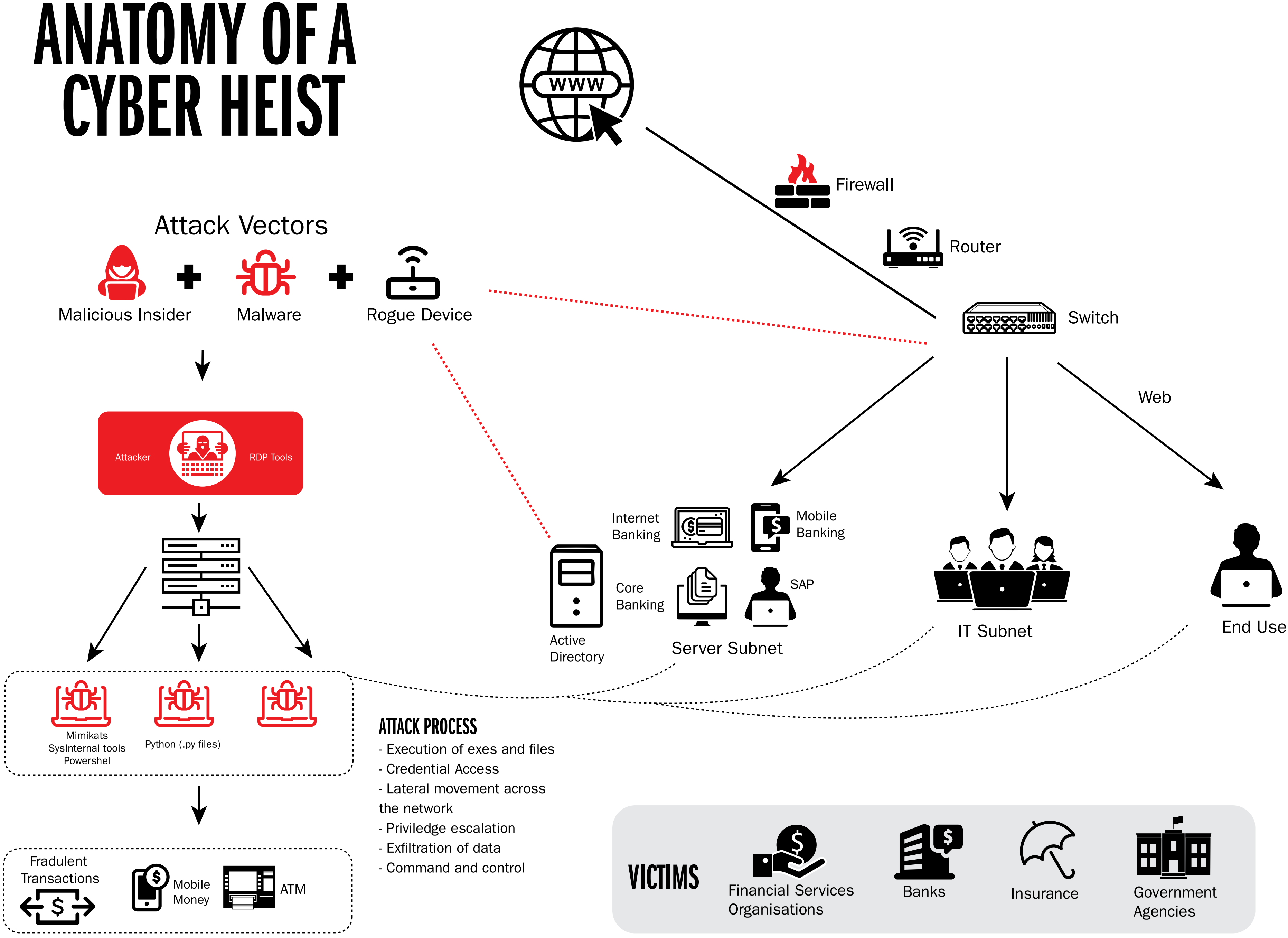
DNSSEC ADOPTION



99.75% of Ugandan domains have not implemented Domain Name System Security Extensions (DNSSEC)

FIGURE 6: COUNTRIES USING THE DNSSEC ADOPTION.

ANATOMY OF A CYBER HEIST



Attack Vectors

Malicious Insider + Malware + Rogue Device

ATTACK PROCESS

- Execution of exes and files
- Credential Access
- Lateral movement across the network
- Priviledge escalation
- Exfiltration of data
- Command and control

VICTIMS

Financial Services Organisations

Banks

Insurance

Government Agencies

INFORMATION SHARING GAP

As pointed out in the previous sections, the lack of information sharing across organisations has promoted the ease with which attacks are being replicated. Information sharing on cyber security threats is therefore highly critical, reinforcing the need for more cooperation across borders, individuals and organisations.

CYBOTA INTEL
Africa's Cyber Threat Sharing Platform

OBJECTIVES OF SERIANU'S INFORMATION SHARING PLATFORM

Early Detection: Through sharing of indicators of compromise, and malware samples.

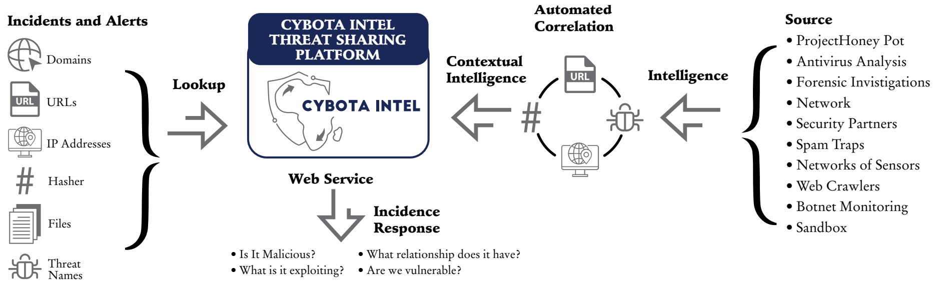
Rapid Response: Early detection leading to rapid incident response.

Prevention: Through applying of patches and fixes shared through the platform.

Improved Eco-system: Through information sharing.

Following this global and urgent need, Serianu has developed Serianu-Information Sharing Platform, a premier program that aims to enhance information sharing in between trusted members and communities in Africa.

HOW IT WORKS



WHY JOIN?

ORGANISATION

- Learn from others and the security issues they are facing or detecting.
- Collect the information to support your internal intelligence team.
- Find out if other organisations are already working on the same incident or similar ones.
- Ensure your security team is actively engaged in the analysis of security threats within Africa.
- Show your capabilities among the sharing community.
- Access to Serianu's pool of threat hunting experts.

SECURITY AND TECHNICAL TEAMS

- Gain access to a vast database of Indicators of Compromise (hashes, IPs, File samples etc.)
- Use the indicators from the system to protect your infrastructure.
- Learn from others and the security issues they are facing or detecting.
- Automatically create relations between malware and their attributes.
- Contribute to improve malware detection and reverse engineering efforts.
- Ensuring that your indicators can be peer reviewed in the information security community.

HOW TO JOIN?: Send an email to info@serianu.com to start your registration process.

INDUSTRY PLAYER PERSPECTIVE

NABIHAH RISHAD

Sr. Risk Consultant, Serianu Limited

Today, organizations are taking a keen interest in the impact of risky internet connectivity for their businesses, employees and customers. This is referred to collectively as cyber security- a structured way of using computer software and systems designed to monitor, detect and prevent unauthorized access to computerized information. In most cases this kind of access has turned out to be mischievous.

Yet, while we can safely say that the rise is commendable, it is still far too slow to make a real impact. Since most sensible companies have a business continuity plan as part of risk management, it is emerging that several are yet to stress-test their plans against emerging and evolving cyber security threats.

The Board of Directors is in a position to push for this actively, but unfortunately there is a severe low appreciation of the need to include cyber security risk as a key success factor for regular discussion. As a result, many business leaders, including Chief Executive Officers and Chief Information Officers, are unable to ramp up cyber security risk to the Directors, citing their low appreciation of the gravity of exposure to internet connectivity without a safety methodology that keeps criminals at bay.

Even though these issues may initially seem like those that the management can deal with, there is a well-developed school of thought that cyber security is no longer just that within the purvey of top management. The Board of Directors must be consciously aware of the organization's cyber risk profile at any given time. Directors need to possess a strong understanding about investment in systems, personnel and continuous knowledge about cyber security.

There is mounting evidence that cyber security is now more of a strategic issue for the organization. The degree of losses from cyber fraud and the scale of attacks are rising with every passing year. Indeed, available data shows that African organizations lost nearly USD 210 Million in 2017 alone to cyber criminals.

Granted, many of the Board matters are driven by regulators: from finance to insurance, human resources and even corporate governance. So where does cyber security come in?

It actually does on two fronts. The first is internal, the second external. Internal means that each Board has to finally find a way to measure and present cyber security risk exposure and its possible impact on the organization. Cyber security is a strategic matter for the board because in addition to financial losses, it is the source of major reputational risk.

Fortunately, there is already a growing wave of emerging regulation regarding cyber risk policies due to piling insurance claims lodged as a result of cyber security losses.

With a firm grasp of cyber security issues and the risk profiling of their respective organizations, directors are then able to focus on the impact- be it legal, regulatory or financial consequences - of cybercrime.

Is cyber security a complicated subject for directors? Probably so. But courses can easily be tailor – made with content simplified for their ease of understanding as they usually come from diverse back grounds. Other IT industry players have said that the issue is a lack of a methodology that gives directors a mechanism for evaluating and assigning a value to the cyber security risks. This was, the directors can possess a visibility on the effectiveness of various controls implemented to address cybersecurity within their organization.

The reality is that globally, board directors are increasingly required to include cyber security as a critical component of their overall role as a risk oversight body chaperoning the management. Since the Board of Directors typically owns the vision of the organization, it therefore follows that each member should have a depth of understanding and appreciation about cyber security.

It is the responsibility of the board to make sure that compliance requirements are met. Boards must proactively manage cybersecurity and drive the organization's attention to and readiness for cybersecurity risks. In order to understand and appreciate the state of their organization's risk profile, they must implement a policy that guides the frequency of evaluation, the shape and form of its valuation and adopt a reporting style that is in line with global best practice.

Fortunately, Uganda is seen as a pace setter on matters information technology; and cyber security is right up there. We look forward to more directors taking up the mantle of and using modern global best practice to show the way for their colleagues to follow. In any case, Uganda is ready to embrace this concept and the best way to do it is to have the board and senior management include this methodology when developing the ICT strategy.

CYBER LAWS IN UGANDA

06

DID YOU KNOW?

CYBER LAW IS THE AREA OF LAW THAT DEALS WITH THE INTERNET'S RELATIONSHIP TO TECHNOLOGICAL AND ELECTRONIC ELEMENTS, INCLUDING COMPUTERS, SOFTWARE, HARDWARE AND INFORMATION SYSTEMS (IS)?

WIKIPEDIA

DATA PROTECTION BILL, 2018

The law, which expands the mandate of the National Information Authority Uganda (NITA-U), will protect the privacy of the individual and of personal data by regulating the collection and processing of personal information.

The Data Protection and Privacy Law will deliver a number of objectives, namely:

- To protect the privacy of the individual and personal data;
- To regulate the collection and processing of personal information;
- To provide for the rights of the persons whose data is collected;
- To provide obligations of data collectors and data processers;
- To regulate the use or disclosure of personal information and for related matters

The law provides the much-needed protection for personal identifiable information which is key in this digital age. It provides important safeguards that will protect Ugandan citizens as they use online services

This law also provides many avenues to facilitate growth in the IT sector. A good example is the BPO industry where the law makes it possible for Ugandan players to comply with international standards, improving credibility and customer trust, which inevitably leads to more business.

The Data Protection and Privacy Bill, was on December 6th 2018 passed by the Parliament of Uganda and was awaiting be assented to by the President to become law. The bill will operationalize Article 27 (2) of the 1995 Constitution for the Republic of Uganda which protects the right to privacy.

COMPUTER MISUSE ACT, 2011 ACT NO.2 OF 2011

It started as the Computer Misuse Bill No.23 of 2008. It includes;Overall, the bill aims to boost security and Uganda's cyber health. No law in its inception is perfect and we will need to constantly adjust it until it fits into our moral and ethical fabric as a country.

- Unauthorized modification of the contents of computer material <section 14>
- Unauthorized use or interception of electronic communications <section 15>
- Unauthorized obstruction of the use of a computer <section 16>
- Unauthorized disclosure of access codes or passwords <section 17>
- Unauthorized disclosure of information <section 18>
- Electronic fraud <section 19>
- Child pornography through computers <section 23>
- Cyber harassment <section 24>
- Cyber stalking <section 26>
- Provision for preservation orders: searches and seizures <section 28>
- Provision for the use of electronic evidence in legal proceedings <section 29>

PART I OF THE ACT

Contains commencement information and interpretation of terms used in the Act.

PART II OF THE ACT: GENERAL PROVISIONS

Contains provisions that further explain the meanings assigned to key terms used in the Act, particularly those concerning how data is accessed or modified on a computer.

PART III OF THE ACT: INVESTIGATIONS AND PROCEDURES.

Provides 3 orders that can be issued by court in relation to data on computers:

- Preservation orders
- Disclosure of preservation order
- Production order

PART IV OF THE ACT: COMPUTER MISUSE OFFENSE

Puts in place penal measures to punish computer misuse.

PART V OF THE ACT: MISCELLANEOUS PROVISIONS OF THE ACT

Provisions on enactment of the Act; Power to courts to issue search and seizure orders, the evidential value of electronic information, the jurisdiction of the courts under the Act including extra-territorial jurisdiction, the power of the minister to amend the schedule to the Act.

ELECTRONIC TRANSACTION ACT, 2011 ACT NO. 8 OF 2011

Provides for the use of security facilitation and regulation of electronic communications and transactions; to encourage the use of e-government services and to provide for the related matters.

It addresses:

- Enforceability and form requirements for electronic contracts.
- Regulation of domain names which are a new form of digital property.
- Privacy protection for consumers and users of electronic media.
- Establishment of a regulatory framework that is compliant with the rapid technological changes.
- Determining the levels of responsibility in tort and contract attached to enhanced abilities of machines.
- Classification of trade in information products especially where the relationship between the producers and ultimate is consumer is remote.
- The object of the Act is to provide a legal and regulatory framework to:
- Enable and facilitate electronic communication and transactions;
- Remove and eliminate the legal and operational barriers to electronic transactions;
- Promote technology neutrality in applying legislation to electronic communications and transactions;
- Provide legal certainty and public confidence in the use of electronic communications and transactions;
- Promote e-Government services through electronic communications and transactions with the Government, public and statutory bodies;
- Ensure that electronic transactions in Uganda conform to the best practices by international standards;
- Encourage investment and innovation in information communications and technology to promote electronic transactions;
- Develops a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;
- Promote the development of electronic transactions that are responsive to the needs of users and consumers
- Foster economic and social prosperity.

ELECTRONIC SIGNATURE ACT, 2011 ACT NO. 7 OF 201

Provides for:

- Use of electronic signatures and regulations.
- Criminalization of unauthorized access and modification of electronic signatures.
- Determination of minimum requirements for the functional equivalence of electronic signatures.

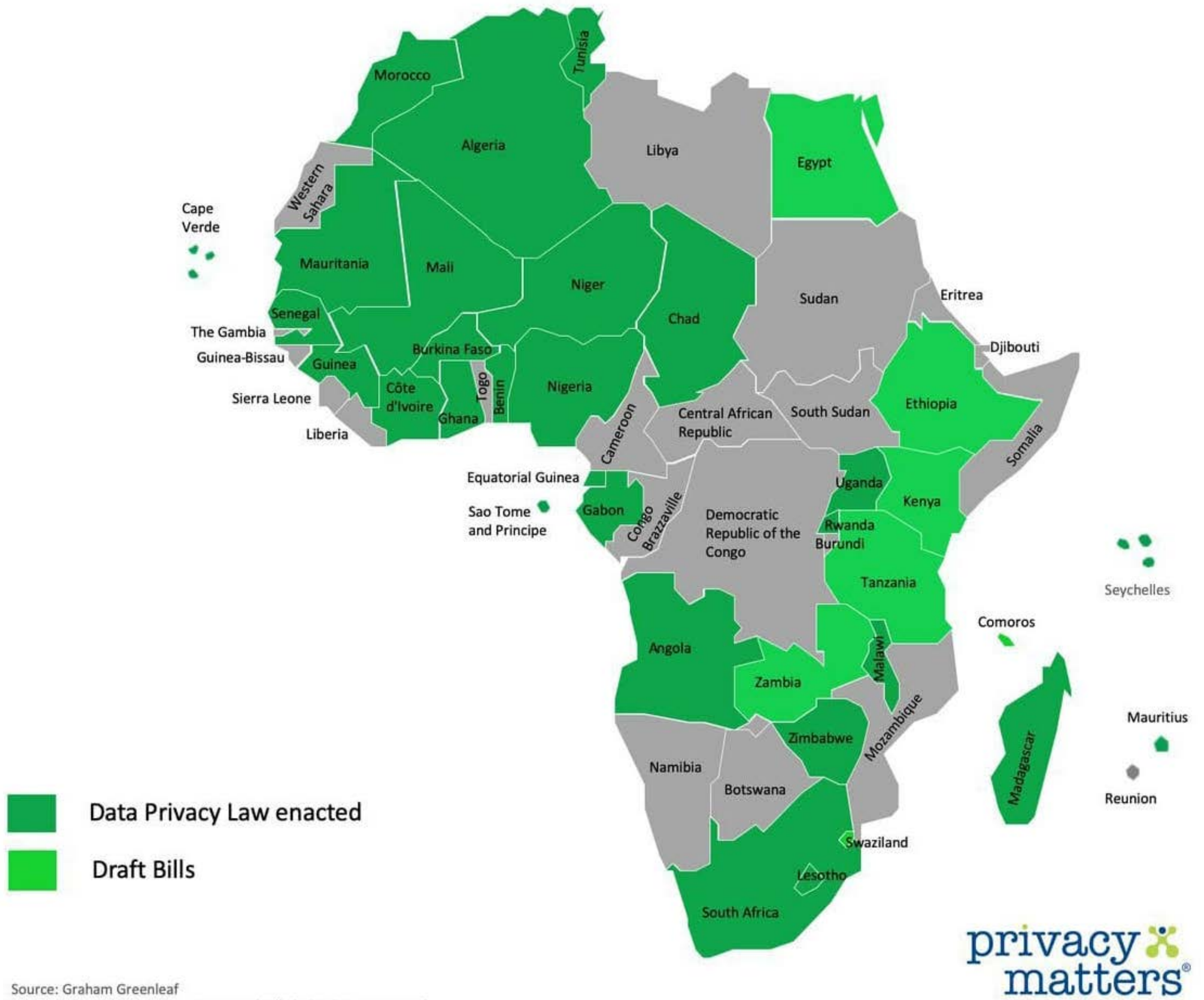
The object of the Act is to:

- Modernization and harmonization of the laws relating to computer generated evidence.
- Amendments of the current laws to provide for admissibility and evidential weight of electronic communications.

Other related matters;

- The Act makes provision for the use of electronic signatures in order to ensure that transactions are carried out in a secure environment.
- It establishes a public key infrastructure for authenticity and security of documents.
- Recognizes the different signature creating technologies.
- Provides effective administrative structures e.g. establishment of Certification Authorities.

Data Privacy Laws and Bills - Africa



Source: Graham Greenleaf
Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593

TOP TRENDS AND PRIORITIES FOR 2019

Looking into the crystal ball one thing is certain – cyber risk has become a board room issue. The responsibility for your organisation's cyber risk posture has escalated to senior executive and board members; understanding your position has never been more important and awareness of external factors more necessary.

> "THE BOARD IS NOW, MORE THAN EVER, FOCUSED ON UNDERSTANDING THE ORGANISATION'S CYBER SECURITY EXPOSURE IN QUANTIFIABLE METRICS.

The Serianu Cyber Intelligence team has seen a number of trends develop which may impact your organisation's operation and exposure to cyber risk in 2019 as summarized below:

GROWTH IN LETHAL AND TARGETED MALWARE

Malware attacks will continue to grow, particularly locally developed or re-engineered malware samples. In 2018, we identified over ten unique samples of locally developed or re-engineered malwares. We expect this trend to increase in 2019. Attackers will continue to evolve the malware samples in order to by-pass the traditional firewalls.

ATTACK-REPLICATION

Attackers will continue to utilize the same techniques and indicators of compromise to compromise multiple organisations. Information sharing and professional networking are therefore a critical measure in 2019 to limit the extent of damage.

INCREASED USE OF OUTSOURCED/ MANAGED SECURITY SERVICES

Increased cyber-attacks across organisations and limited staff skills will lead to an increase in the adoption rate of managed security services solutions. We anticipate that banking sector and Saccos will leverage on Managed Security Providers expertise to manage and secure their enterprise security.

USE OF THIRD PARTIES TO EXPLOIT TARGET ORGANISATIONS

Vendor vulnerabilities have led to devastating breaches in the past few years. Ranging from mobile application developers, core banking vendors or general supplies vendors. The most used attack vector is compromising vendor access to either system of premises. Rogue vendors can also collide with malicious attackers to compromise an internal system since they possess a good understanding of the processes involved.

CONTINUED ENGAGEMENT FROM BOARD AND SHAREHOLDERS

Now more than ever, these stakeholders are focused intensely on the importance of effective corporate oversight and are increasing scrutiny of oversight roles and responsibilities, including the accountability of these mechanisms for defending their interests. Such stakeholder scrutiny has prompted those with corporate oversight responsibility to critically review their own oversight roles and operations and has led to increased consideration of how to effectively measure the performance of controls within the organisation.

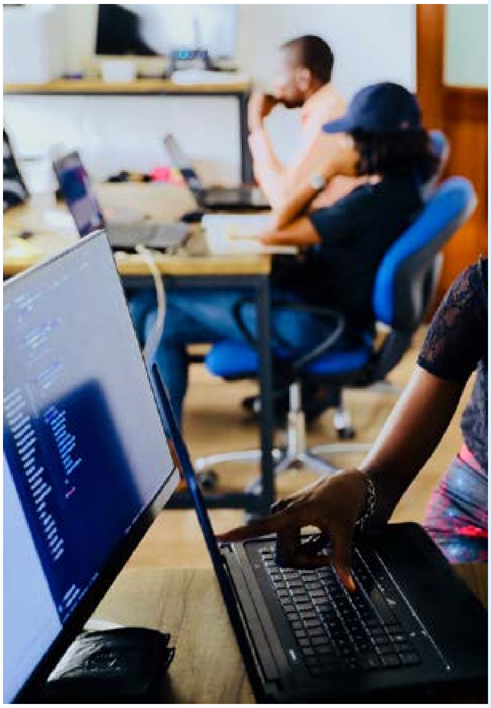
GROWTH IN CYBER INSURANCE OFFERINGS

The global cyber insurance market is expected to expand globally and projected to grow to $5bn in annual premiums by 2018 and at least $7.5bn by 2020. AoN one of the top insurance companies, launched Cyber Enterprise Solutions to help businesses thwart cyber-attack incidences that are potentially catastrophic in terms of data loss and corporate espionage. We anticipate that more players will join the market and more organisations will seek out Cyber Insurance Offerings.

As we embark on strengthening our Cyber resilience, it is critical that we identify what's priority. Below are key questions you need to answer going forward.

- What is my inherent risk profile? Do I know all my risks, threats and vulnerabilities?
- What controls have I implemented and are they adequate?
- What level of visibility do I have into the effectiveness and efficiency of the cyber risk controls?
- What is my organisations cyber security exposure? Should I purchase cyber insurance?

Cyber criminals are spending more time understanding the inner workings of their target organisations. Some of them are investing heavily in understanding the technologies and processes these organisations have deployed. It is no longer a question of when but of how and what? 2019 is the year of Cyber Risk Visibility, you need to take the first steps to improve your cyber risk resilience; measure your cyber visibility, benchmark your position against your peers start the journey of continuous improvement.



Top Priorities for 2019

➘**BREACH AND ATTACK SIMULATION:** RUN SIMULATED ATTACKS TO MEASURE THE EFFECTIVENESS OF A COMPANY'S PREVENTION, DETECTION AND MITIGATION CAPABILITIES.

➘**RISK QUANTIFICATION:** PROVIDING MEASUREABLE METRICS ON CYBERSECURITY POSTURE AND EXPOSURE VALUES FOR THE ORGANISATION.

➘**BOARD ENGAGEMENT:** PROACTIVE MONITORING AND TRACKING OF CYBERSECURITY METRICS.

➘**CYBERSECURITY AWARENESS:** ACQUIRE SKILLS FOR ANTICIPATING, DETECTING AND CONTAINING CYBER THREATS.

➘**3RD PARTY MANAGEMENT:** MONITORING AND TRACKING THIRD-PARTY ACCESS ON THE NETWORK.

➘**SECURITY ARCHITECTURE:** EFFECTIVE DESIGN AND CONFIGURATION OF NETWORK SYSTEMS FOR OPTIMAL SECURITY.

➘**THREAT SHARING:** KEEP ABREAST OF CYBERSECURITY THREATS, ATTACKS AND VULNERABILITIES WITHIN AFRICA.

➘**ENDPOINT SECURITY:** SECURING END-USER PCS FROM MALWARE, DATA EXFILTRATION AND VULNERABILITIES.

➘**PRIVILEGED USER MANAGEMENT:** MONITORING AND TRACKING PRIVILEGE USERS/ACCOUNTS FOR MALICIOUS ACTIVITIES.

➘**POLICY IMPLEMENTATION:** ENFORCING SPECIFIC ACTIONS DOCUMENTED WITHIN COMPANY POLICY.

FRAUD EXPOSURES

FRAUD EXPOSURES

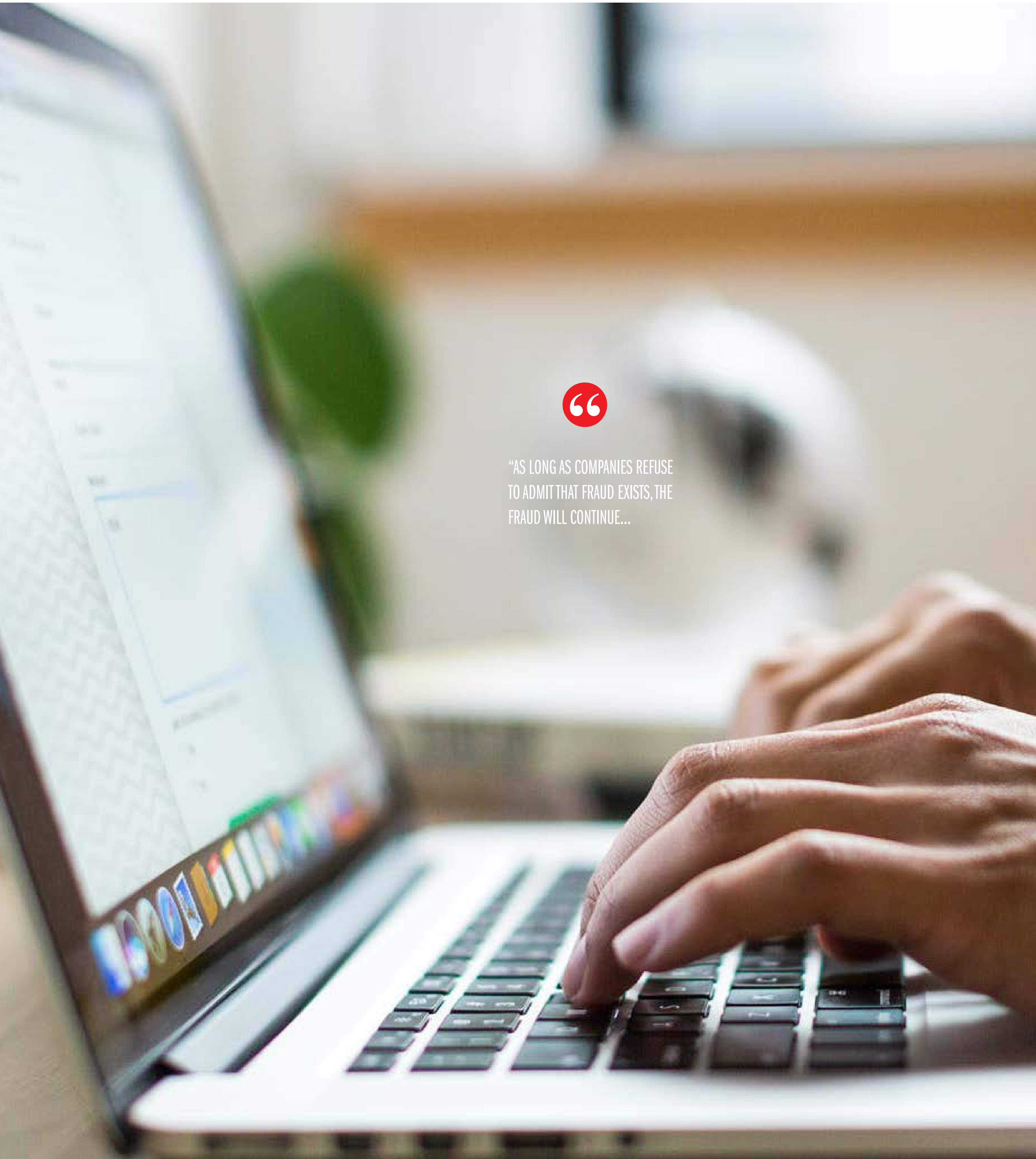
Mobile Fraud	Sim swaps, account takeovers,
Email Fraud	Spoofing, phishing, bogus offers and business email compromise.
Transfer Fraud	Unauthorized transfer of funds from one account to another in the same or different financial institution.
Online Fraud	Makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose tricking victims out of money, property, and inheritance

IP THEFT EXPOSURES

Data Breach	Malicious access, copying, transmission, viewing of sensitive, protected or confidential data.
Unauthorized Disclosures	Compromise of classified information by communication or physical transfer to an unauthorized recipient.
Cyber-forgery (counterfeit)	Unauthorized input, alteration or deletion of computer data resulting to inauthentic data.
Brand Theft (Domain)	Changing the registration of a domain name without the permission of its original registrant, or by abuse of privileges on domain hosting and registrar software systems.

SABOTAGE EXPOSURES

Data Hijacking	Uses malicious software aka ransomware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
System Tampering	Intentional modification of a system/technology in a way that would make them harmful to the system user.
Data Tampering	Deliberately modifying (destroying, manipulating or editing) data through unauthorized channels. Focus is on data at rest.
Cryptojacking	Unauthorized use of a computer or connected home device by cybercriminals to mine for cryptocurrency.
DDOS	A large-scale DoS attack where the perpetrator uses more than one unique IP address, often thousands of them



"AS LONG AS COMPANIES REFUSE TO ADMIT THAT FRAUD EXISTS, THE FRAUD WILL CONTINUE...

CYBER VISIBILITY AND EXPOSURE QUANTIFICATION (CVEQ™) FRAMEWORK

The Serianu Cyber-Risk Visibility and Exposure Quantification (CVEQ™) Framework is an innovative risk quantification approach that enables organisations to measure and quantify their cyber security risk.

Serianu CVEQ™ Framework

08

DID YOU KNOW?

CYBERSECURITY REQUIRES ORGANISATIONS TO DEFINE CLEAR METRICS FOR MEASURING AND MONITORING THE PERFORMANCE AND EFFECTIVENESS OF CYBER-SECURITY PROGRAM.

The Framework concepts are based on the globally accepted Credit Scoring Methodology - where a statistical analysis is performed by lenders and financial institutions to access an entity’s credit risk based on four key elements: Risk, Controls, Visibility and Exposure.

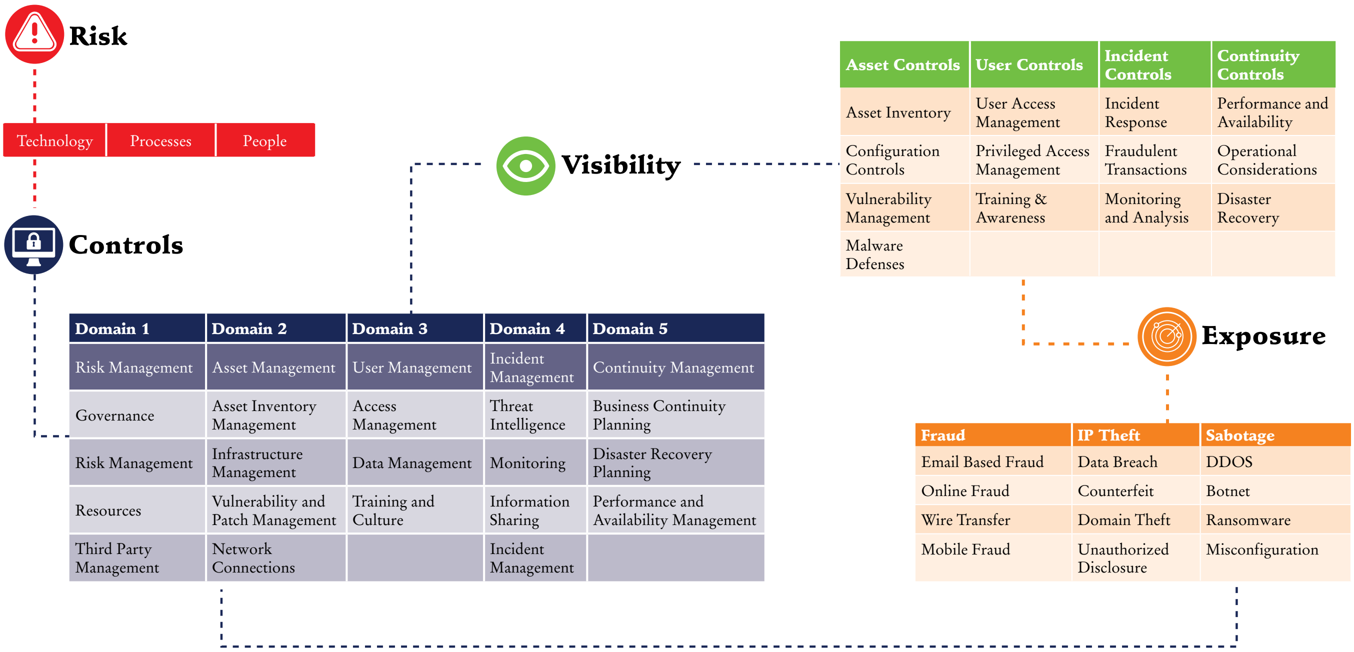
The Cyber Visibility Statements are an effective way to continuously measure your cyber security posture across a range of key security performance indicators. Measuring control effectiveness is a key element in any cyber security risk management process.

The statements include:

- Inherent Risk Statement
- Maturity Statement
- Visibility Statement
- Deficiency Statement
- Incident Monitoring Statement
- Exposure Statement

A Summary of the CVEQ™ Framework

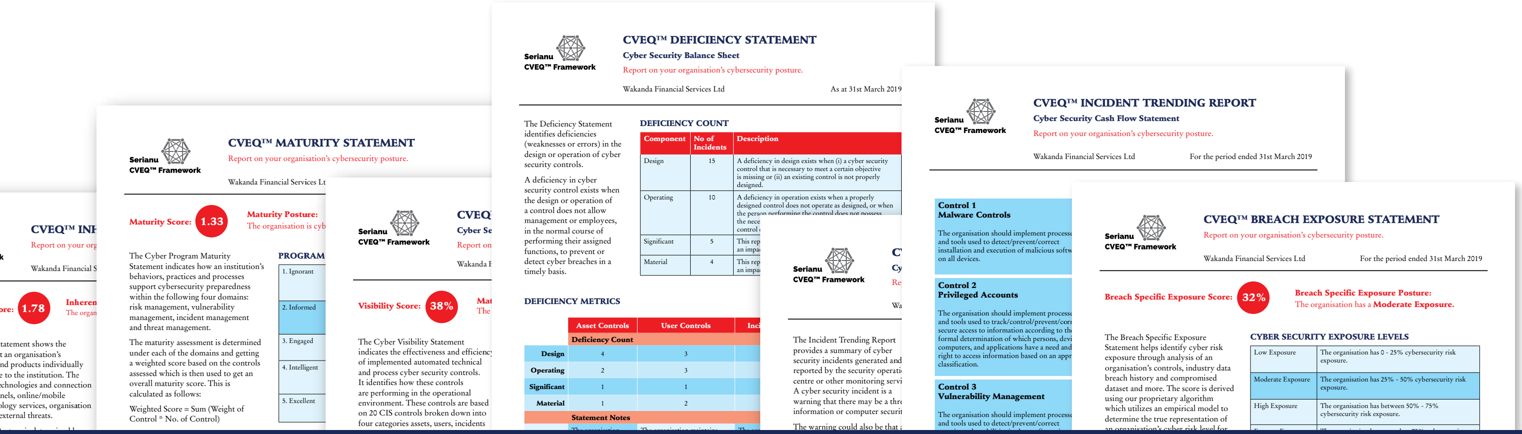
An organisations cyber risk exposure is assessed across **4 Dimensions** (Risk, Controls, Visibility and Exposure), **14 Distinct Drivers** and over **43 Quantifiable Levers.**



Asset Controls	User Controls	Incident Controls	Continuity Controls
Asset Inventory	User Access Management	Incident Response	Performance and Availability
Configuration Controls	Privileged Access Management	Fraudulent Transactions	Operational Considerations
Vulnerability Management	Training & Awareness	Monitoring and Analysis	Disaster Recovery
Malware Defenses			

Domain 1	Domain 2	Domain 3	Domain 4	Domain 5
Risk Management	Asset Management	User Management	Incident Management	Continuity Management
Governance	Asset Inventory Management	Access Management	Threat Intelligence	Business Continuity Planning
Risk Management	Infrastructure Management	Data Management	Monitoring	Disaster Recovery Planning
Resources	Vulnerability and Patch Management	Training and Culture	Information Sharing	Performance and Availability Management
Third Party Management	Network Connections		Incident Management	

Fraud	IP Theft	Sabotage
Email Based Fraud	Data Breach	DDOS
Online Fraud	Counterfeit	Botnet
Wire Transfer	Domain Theft	Ransomware
Mobile Fraud	Unauthorized Disclosure	Misconfiguration



Serianu CVEQ™ Framework

CVEQ™ INH
Report on your org
Wakanda Financial S
ore: 1.78 Inheren
The organ
tatement shows the t an organisation's nd products individually e to the institution. The echnologies and connection nels, online/mobile ology services, organisation external threats.

Serianu CVEQ™ Framework

CVEQ™ MATURITY STATEMENT
Report on your organisation's cybersecurity posture.
Wakanda Financial Services Lt

Maturity Score: 1.33
Maturity Posture:
The organisation is cyb

The Cyber Program Maturity Statement indicates how an institution's behaviors, practices and processes support cybersecurity preparedness within the following four domains: risk management, vulnerability management, incident management and threat management.

The maturity assessment is determined under each of the domains and getting a weighted score based on the controls assessed which is then used to get an overall maturity score. This is calculated as follows:

Weighted Score = Sum (Weight of Control * No. of Control)

PROGRAM
1. Ignorant
2. Informed
3. Engaged
4. Intelligent
5. Excellent

Serianu CVEQ™ Framework

CVEQ
Cyber Se
Report on
Wakanda F

Visibility Score: 38%
Mat
The

The Cyber Visibility Statement indicates the effectiveness and efficiency of implemented automated technical and process cyber security controls. It identifies how these controls are performing in the operational environment. These controls are based on 20 CIS controls broken down into four categories assets, users, incidents

Serianu CVEQ™ Framework

CVEQ™ DEFICIENCY STATEMENT
Cyber Security Balance Sheet
Report on your organisation's cybersecurity posture.
Wakanda Financial Services Ltd As at 31st March 2019

The Deficiency Statement identifies deficiencies (weaknesses or errors) in the design or operation of cyber security controls.

A deficiency in cyber security control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect cyber breaches in a timely basis.

DEFICIENCY COUNT

Component	No of Incidents	Description
Design	15	A deficiency in design exists when (i) a cyber security control that is necessary to meet a certain objective is missing or (ii) an existing control is not properly designed.
Operating	10	A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the nece control
Significant	5	This rep an impa
Material	4	This rep an impa

DEFICIENCY METRICS

	Asset Controls	User Controls	Inci
	Deficiency Count		
Design	4	3	
Operating	2	3	
Significant	1	1	
Material	1	2	
	Statement Notes		

Serianu CVEQ™ Framework

C
Cy
Re
Wa

The Incident Trending Report provides a summary of cyber security incidents generated and reported by the security operati centre or other monitoring servi A cyber security incident is a warning that there may be a thre information or computer securit

The warning could also be that a

Serianu CVEQ™ Framework

CVEQ™ INCIDENT TRENDING REPORT
Cyber Security Cash Flow Statement
Report on your organisation's cybersecurity posture.
Wakanda Financial Services Ltd For the period ended 31st March 2019

Control 1
Malware Controls
The organisation should implement processe and tools used to detect/prevent/correct installation and execution of malicious softw on all devices.

Control 2
Privileged Accounts
The organisation should implement processe and tools used to track/control/prevent/corr secure access to information according to the formal determination of which persons, devi computers, and applications have a need and right to access information based on an appr classification.

Control 3
Vulnerability Management
The organisation should implement processe and tools used to detect/prevent/correct

Serianu CVEQ™ Framework

CVEQ™ BREACH EXPOSURE STATEMENT
Report on your organisation's cybersecurity posture.
Wakanda Financial Services Ltd For the period ended 31st March 2019

Breach Specific Exposure Score: 32%
Breach Specific Exposure Posture:
The organisation has a **Moderate Exposure.**

The Breach Specific Exposure Statement helps identify cyber risk exposure through analysis of an organisation's controls, industry data breach history and compromised dataset and more. The score is derived using our proprietary algorithm which utilizes an empirical model to determine the true representation of

CYBER SECURITY EXPOSURE LEVELS

Low Exposure	The organisation has 0 - 25% cybersecurity risk exposure.
Moderate Exposure	The organisation has 25% - 50% cybersecurity risk exposure.
High Exposure	The organisation has between 50% - 75% cybersecurity risk exposure.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) VERSUS CYBER-RISK VISIBILITY AND EXPOSURE ASSESSMENT

Unlike the one-time penetration tests, the cyber resilience assessment enables simulation of various complex attack scenarios on your organisation. The assessment's key value is that as opposed to penetration testing and gap analysis services, the platform runs ongoing testing of your Cybersecurity resilience.

The approach enables you to assess the full scenario of a targeted attack against the entire organisation, evaluating the organisation's capability to identify and respond to an attack, with a clear measure of the organisation's cyber resilience maturity.

REFERENCES

https://www.marketresearchmedia.com/?p=839

https://www.peoplehr.com/blog/index.php/2016/06/17/grow-your-own-with-a-talent-plan/

https://www.raconteur.net/hr/grow-your-own-with-a-talent-plan

The Cybersecurity Workforce Gap William Crumpler & James A. Lewis

Carey, G., & Turner, B. (2019). Best free cybersecurity courses online. Retrieved April 17, 2019, from Tech Radar website: https://www.techradar.com/best/best-free-cybersecurity-courses-online

Class Central. (2019). Free Online Courses: Cybersecurity. Retrieved April 17, 2019, from https://www.classcentral.com/subject/cybersecurity#

CUE. (2018, November). Approved Academic Programmes Offered Universities in Uganda. Retrieved from http://www.cue.or.ke/index.php/approved-academic-programmes

Edwards, L. (2018, December 30). 7 Wearables to look out for in 2019. Retrieved April 16, 2019, from Tech Radar website: https://www.techradar.com/news/7-wearables-to-look-out-for-in-2019

Immersive Labs. (2019). Immersive Labs. Retrieved April 17, 2019, from https://dca.immersivelabs.online/

ISACA. (2019). State of Cybersecurity 2019. Part 1: Current Trends in Workforce Development.

(ISC)2. (2018). Cybersecurity Workforce Study.

Jabil. (2018, February). 7 Automotive Connectivity Trends Fueling the Future. Retrieved April 16, 2019, from iotforall website: https://www.iotforall.com/7-connected-car-trends/

MOOC List. (2019). Computer Science MOOCs and Free Online Courses. Retrieved April 17, 2019, from https://www.mooc-list.com/tags/cybersecurity

Muchiri, T. (2019, April 9). USIU-Africa and YelBridges to launch Cyber4Growth report. Retrieved April 16, 2019, from USIU-Africa website: https://www.usiu.ac.ke/1039/usiu-africa-yelbridges-launch-cyber4growth-report/

Oltsik, J. (2019). The Cybersecurity Skills Shortage Is Getting Worse. Retrieved from CSO Online website: https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html

Osborne, C. (2018, October). The most interesting Internet-connected vehicle hacks on record. Retrieved April 16, 2019, from ZDNet website: https://www.zdnet.com/article/these-are-the-most-interesting-ways-to-hack-internet-connected-vehicles/

Sapkale, Y. (2019, February). Aadhaar Data Breach Largest in the World, Says WEF's Global Risk Report and Avast. Retrieved April 16, 2019, from Moneylife website: https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html

Till, K. (2018). Why The Process Industries Need The Industrial Internet Of Things. Retrieved April 16, 2019, from Processing Magazine website: https://www.processingmagazine.com/industrial-internet-of-things/

Trueman, C. (2019). Top IT Security Certifications 2019. Retrieved from CIO website: https://www.cio.com/article/3310836/top-it-security-certifications.html

Verma, A. (2018, June 26). Top 10 Big Data Companies to Target in 2019. Retrieved April 16, 2019, from Whizlabs website: https://www.whizlabs.com/blog/big-data-companies-list/

https://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

https://resources.infosecinstitute.com/global-cost-cybercrime-rise/

https://www.wired.com/2012/08/cybercrime-trillion/

Skills Mismatch: https://medium.com/@LargeCardinal/we-need-to-kill-the-security-analyst-79ec205651f5

Mirai Botnet: https://thehackernews.com/2018/01/mirai-okiru-arc-botnet.html

Skygofree malware: https://gbhackers.com/skygofree-android-spyware/

Spectre and Meltdown: https://www.us-cert.gov/ncas/alerts/TA18-004A

https://censys.io/

https://www.shodan.io/

Cybercrime law review: https://www.nation.co.ke/news/Court-suspends-portions-of-cybercrime-law/1056-4585936-thh4s5/index.html

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

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

For more information contact:

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