2018

Africa Cyber Security Report - Kenya

SERIANU

Cyber Security Skills G ap

United States International University-Africa

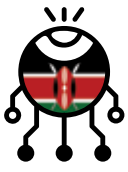
ISACA
Trust in, and value from, information systems

Africa Cyber Immersion Centre acic
Engage | Educate | Empower

CYBOTA INTEL
Africa's Cyber Threat Sharing Platform

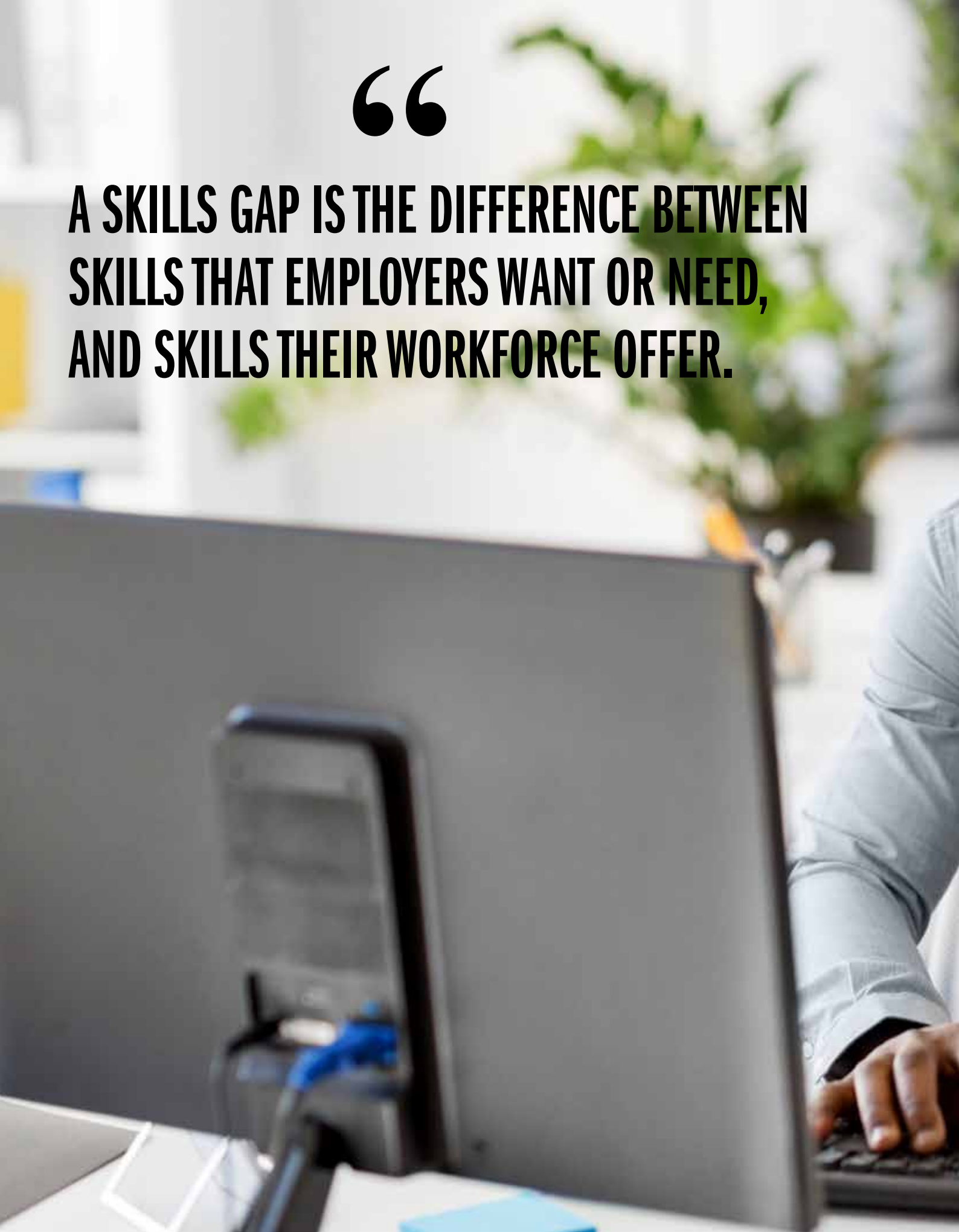
SERIANU

2018



Africa Cyber Security Report - Kenya

Cyber Security Skills G ap



“

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

2018 was an eventful year. We saw a rise in Cyber vigilance particularly among financial institutions, where regulators released a number of guidelines such as the Sacco Societies Regulatory Authority (SASRA) guidelines on Cybersecurity and the Ministry of ICT's Data Protection Bill-which is still under review in Kenya. On the flip side, there was an increase in attacks targeting Saccos and other SMEs, not just in Kenya, but across the African region. Malwares - particularly crypto mining malwares and ransomware - have been on the rise.

While previously in 2017, we highlighted that Cybersecurity spending was at an all-time low, we noted a slight improvement in this area, mainly due to the increasing regulatory demands for organisations to invest in cyber security activities such as vulnerability assessment, penetration testing, training and other critical Cybersecurity controls.

Over the 6 years that have led up to this 6th Annual Cyber Security Report we highlight the trends we have seen/covered so far:

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

2012

40
Average number of security breaches per company

2014

Rethinking Cybersecurity - "An Integrated Approach: Process, Intelligence and Monitoring

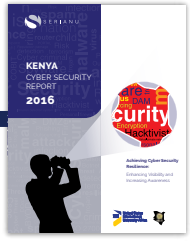
$500b
Global cost of cyber crime

2015

Achieving Enterprise Cyber-resilience Through Situational Awareness

$600b
Global cost of cyber crime

2016



Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness

$175m
Cost of Cyber Security

2017

Demystifying African's Cyber Security Poverty Line

$210m
Cost of Cyber Security

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 - Kenya Edition, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;

United States International University-Africa

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.

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

The ISACA-Kenya 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-Kenya chapter members.

The Serianu CyberThreat Intelligence Team

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

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

OTHER CONTRIBUTORS

Kevin Kimani
Martin Mwangi
Faith Mueni
Jeff Karanja
Daniel Ndegwa
Jackie Madowo
Bonface Shisakha
Samuel Momanyi
Samuel Keige
Stephen Wanjuki
George Kiio
Morris Kamethu

COPY EDITOR

Dickson Migiro

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)

Martin Kilungu
Information Security Officer
Office of the Auditor-General-Kenya

Joseph Mathenge
Chief Operations Officer, Serianu Limited

Paula Mwikali
Research Associate Director, Centre for Informatics Research and Innovation (CIRI), Digital Forensics, Information Security Audit Lecturer USIU-Africa

Eric Mugo
Senior Manager, Fraud Investigation
Safaricom PLC

Raymond Bett
President, ISACA-Kenya Chapter

Tom Mboya
Head of ICT, Unga Group Ltd

Victor Opiyo
Partner, Advocate, Lawmark Partners LLP

Nabihah Rishad
Senior Risk Consultant, Serianu Limited

Building Data Partnerships

In an effort to enrich the data we are collecting, Serianu 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 Kenya.

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

Welcome to the 6th 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, Kenya needs at least 10,000 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 100 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 50,000 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

1700 Cyber Security Skilled Professionals in Kenya

Skills shortage at senior management and mid management levels

60% 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

26% of respondents spend above $10000

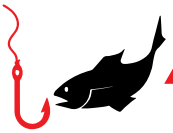
$295M cost of cybercrime in Kenya in 2018

11% ↑ reported Cyber crime incidents to the police

7% ↑ 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 Kenyans 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 Kenyan 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 Kenyan organisations. With the cost of cybercrime increasing every year across Kenya, 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 Kenya - 1700 it is clear that Kenyan businesses are an easy target for both local and international hackers. Some companies in Kenya 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

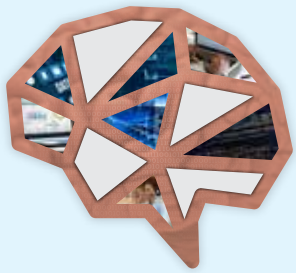
DID YOU KNOW?

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



1700
Cyber Security Skilled Professionals in Kenya

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 Kenyan 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 Kenya 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

Kenya 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 2017 election, pictures and videos of the 2007/2008 Post Election violence were being circulated to incite violence. The social media channels used were mainly Whatsapp, Twitter and Facebook.

2

In 2013, it is widely believed that one of the triggers of the South Sudanese civil war was attributed to a Facebook post that claimed First Vice President Riak Machar had been arrested by government forces. This post turned out not only to be untrue, but was posted by someone in Nairobi while the talks were happening in Juba. Over 5000 people lost their lives in the ensuing civil war.

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

"

FAKE NEWS HAVE FAR REACHING CONSEQUENCES SUCH AS MURDERS, REPUTATION DAMAGE, ELECTION LOSS E.T.C

@JANEGODIA

@AMWIK ASSOCIATION OF MEDIA WOMEN IN KENYA (AMWIK)

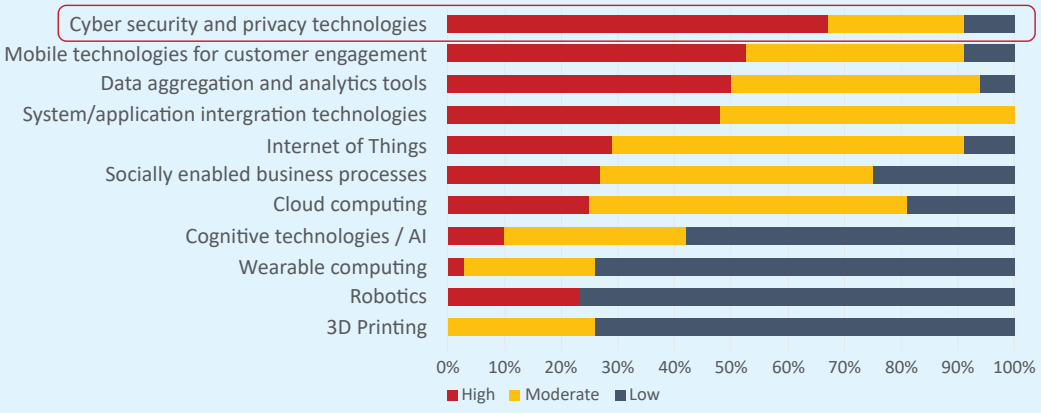
INDUSTRY PLAYER PERSPECTIVE

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



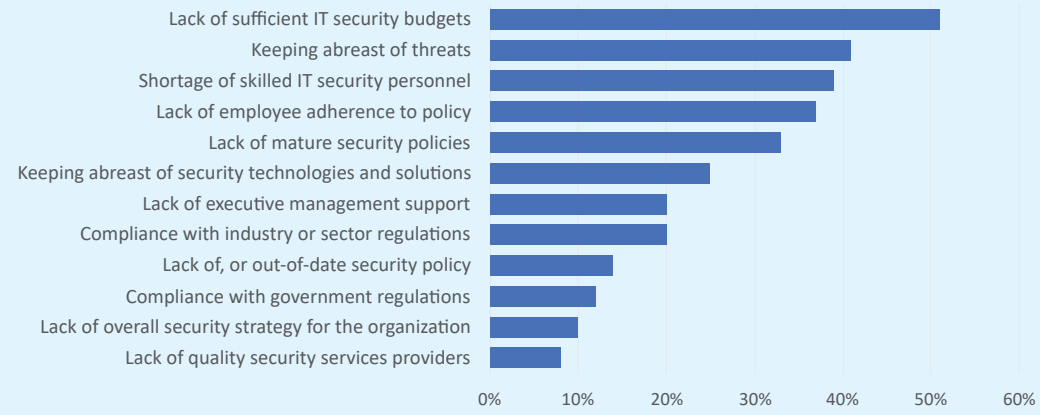
SOURCE 1: IDC

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:

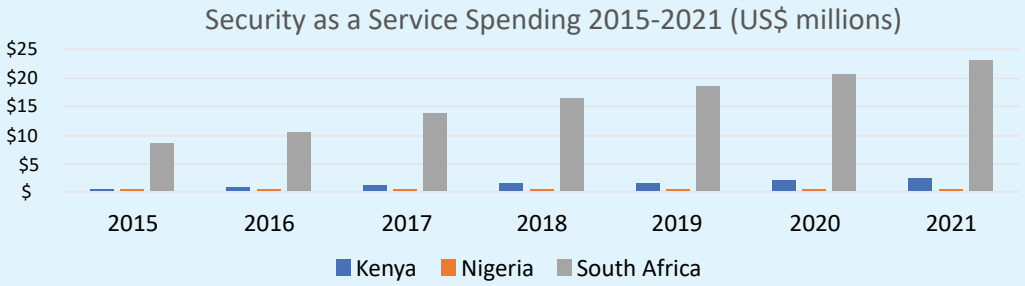
- Cloud (Spectre/Meltdown)
- IoT (auth/poisoning/DoS)
- AI/cognitive (subversion/DoS)
- Shadow IT (leakage/authentication/BC)

CHALLENGES IN MANAGING SECURITY



SOURCE 2: IDC

SECURITY AS A SERVICE SPENDING



SOURCE 3: IDC

- Kenya 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.

...Fake News cont'd

LEGAL ACTION OR REGULATION AGAINST FAKE NEWS

A new law in Kenya is the latest in East Africa to punish the spreading of "false information" and impose a lengthy jail term on offenders. It proposes a fine of KES. 5million ($50,000) and/or up to two years in prison for publishing "false" information. The Computer Misuse and Cybercrimes law also criminalizes abuse on social media and cyber bullying.

Critics of the "fake news" laws in Kenya, Uganda and Tanzania say they are meant to muzzle independent media. According to Kenya's Editor's Guild, the law "may be abused by state authorities to curtail media freedom".

SURVEY ANALYSIS

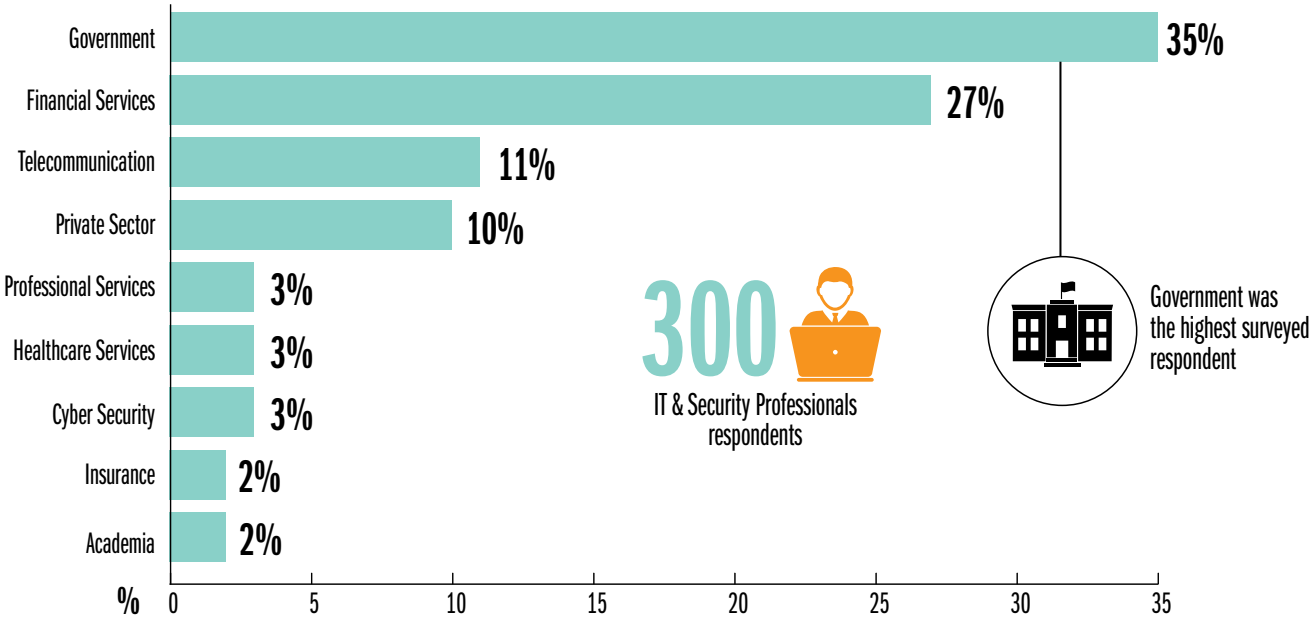
The 2018 Cybersecurity Survey provides insight into what Kenyan organisations are doing to protect their information and assets, in light of increasing cyber-attacks and compromises impacting them.

Based on the feedback from over 300 IT and security professionals, 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 Cybersecurity we interviewed and questioned several people across a broad spectrum of industries.



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 Kenyan 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)?

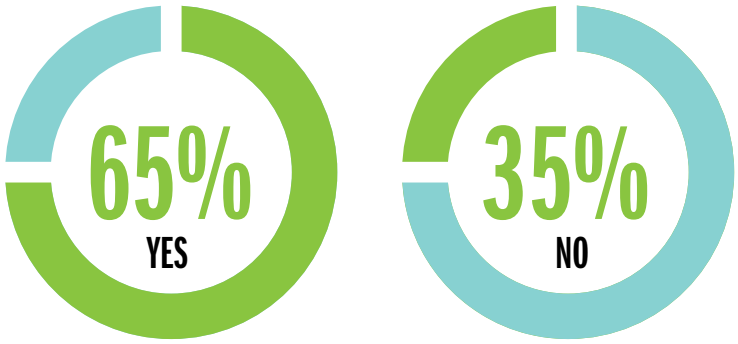
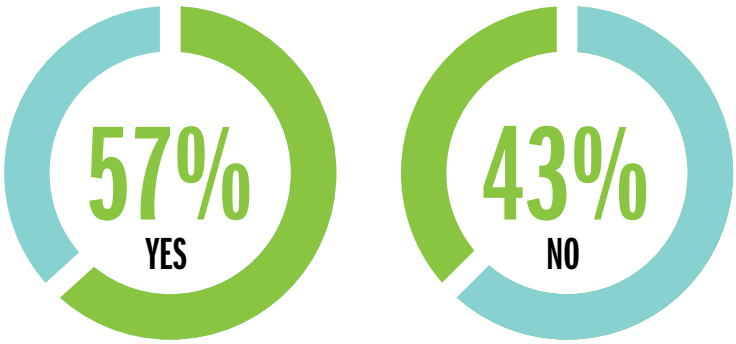


CHART 2: CLOUD SERVICES/ IOT USAGE.

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?

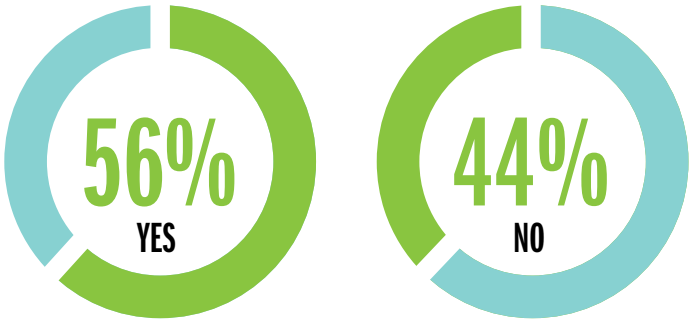
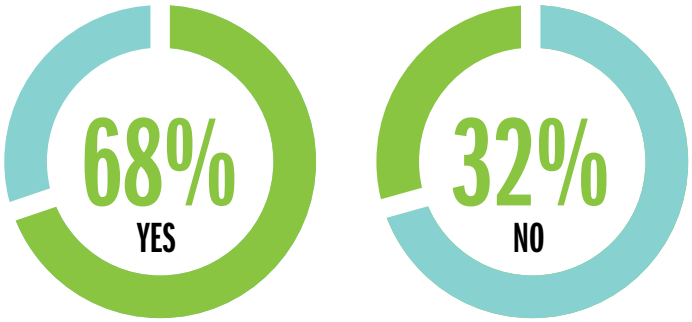


CHART 4: IOT AND CLOUD SERVICES BEST PRACTICE

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.

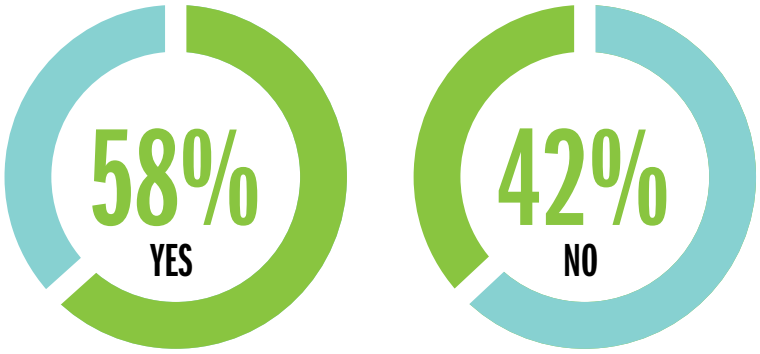
CYBER CRIME

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?

CHART 7: CYBER CRIME VICTIMS.

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



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.

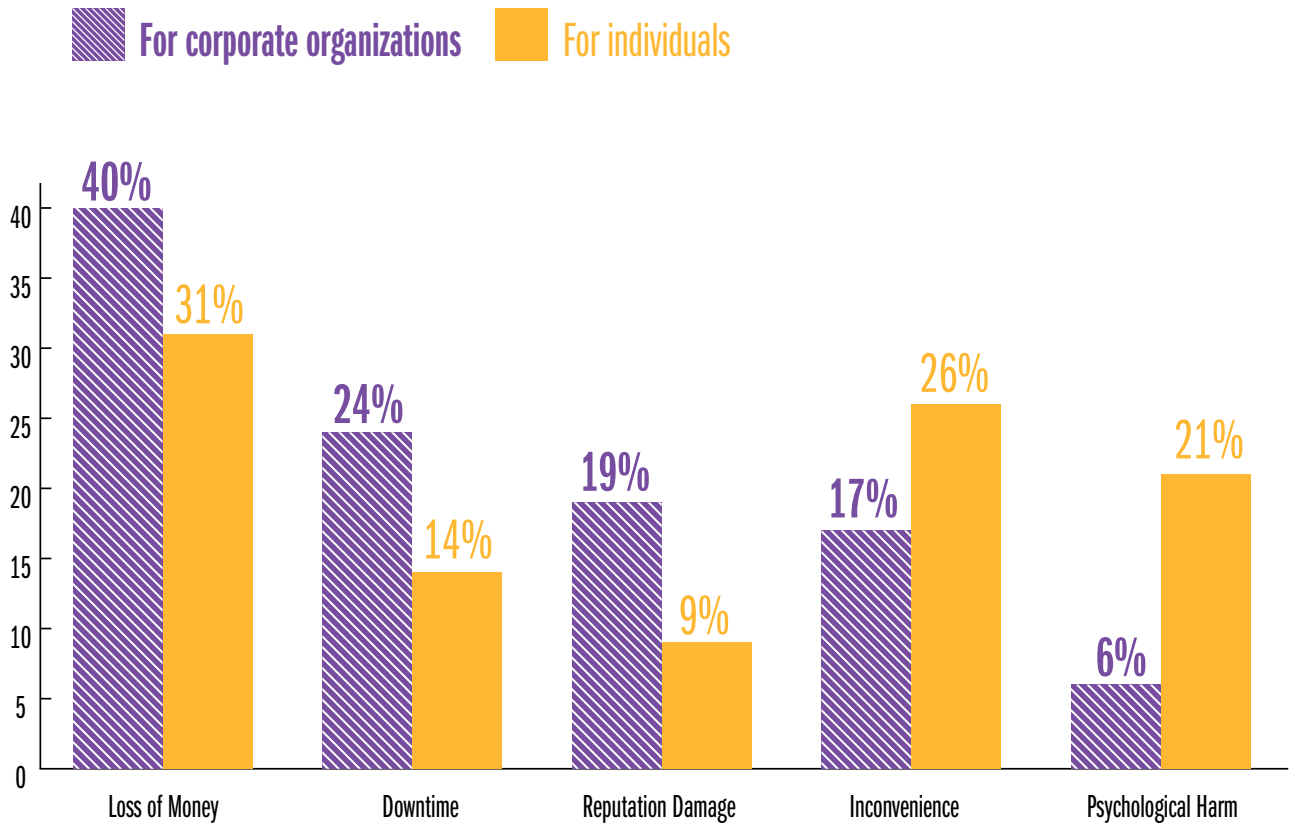
FBI ALERT 2016

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.



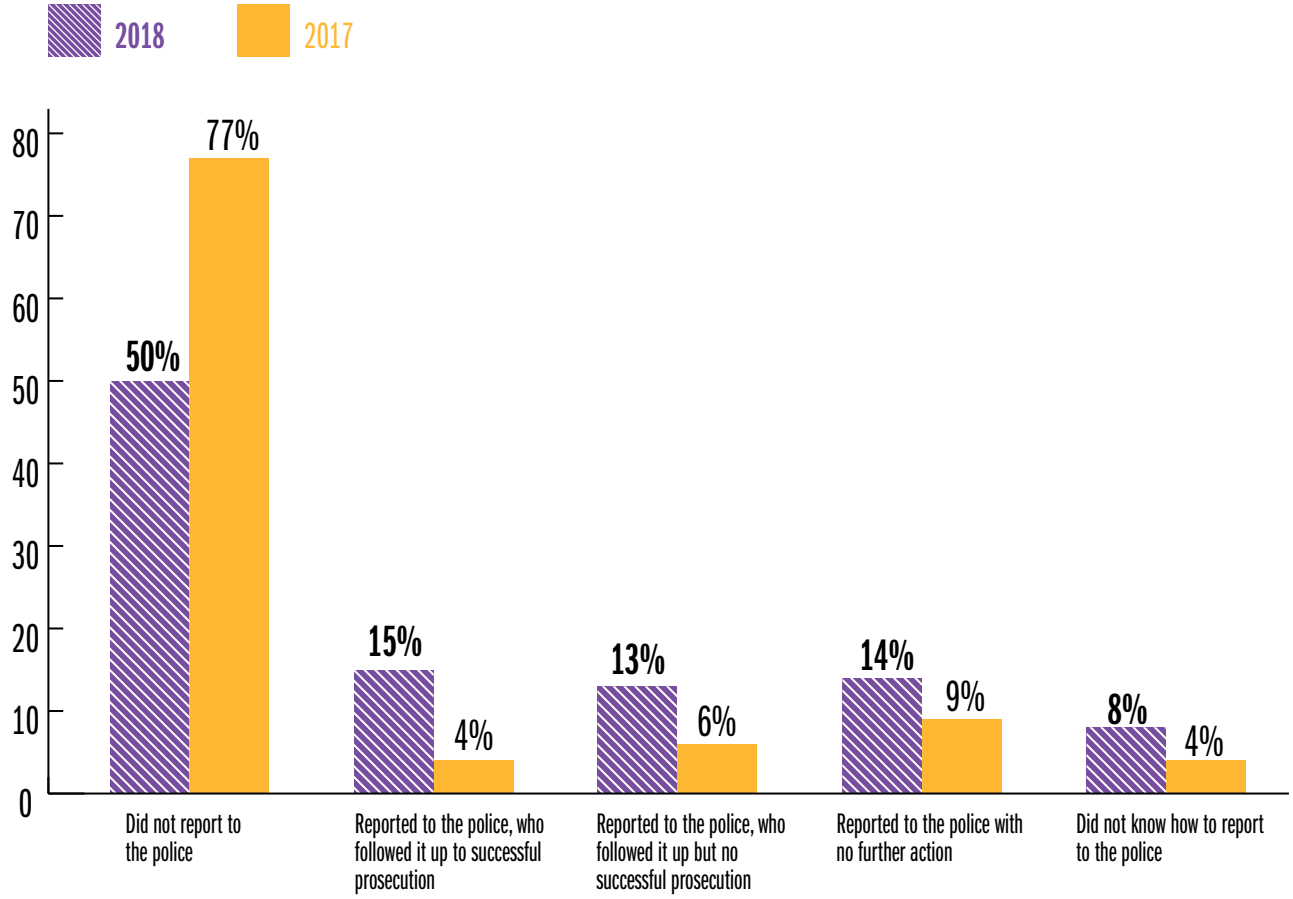
GRAPH 2: IMPACTS OF CYBERCRIME: CORPORATE VS INDIVIDUALS.

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?

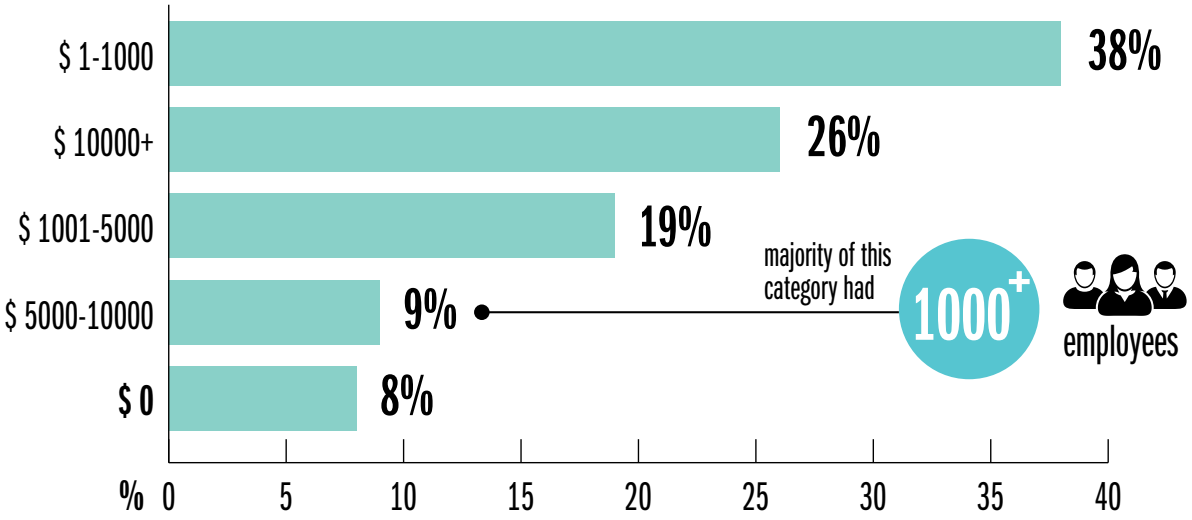


GRAPH 3: REPORTING OF CYBERCRIME .

- 2018 saw an 11% increase in the number of people who reported Cyber crime incidents to the police.
- 7% 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 2017, we saw a slight improvement of 7% whereby 88% reported to have spent less than $5,000 on cyber security. In 2018, 26% of respondents spent above $10,000. Further analysis also revealed that majority of organisations which spend $10,000 and above are from the banking and financial sectors. This not surprising since these industries are the most targeted.

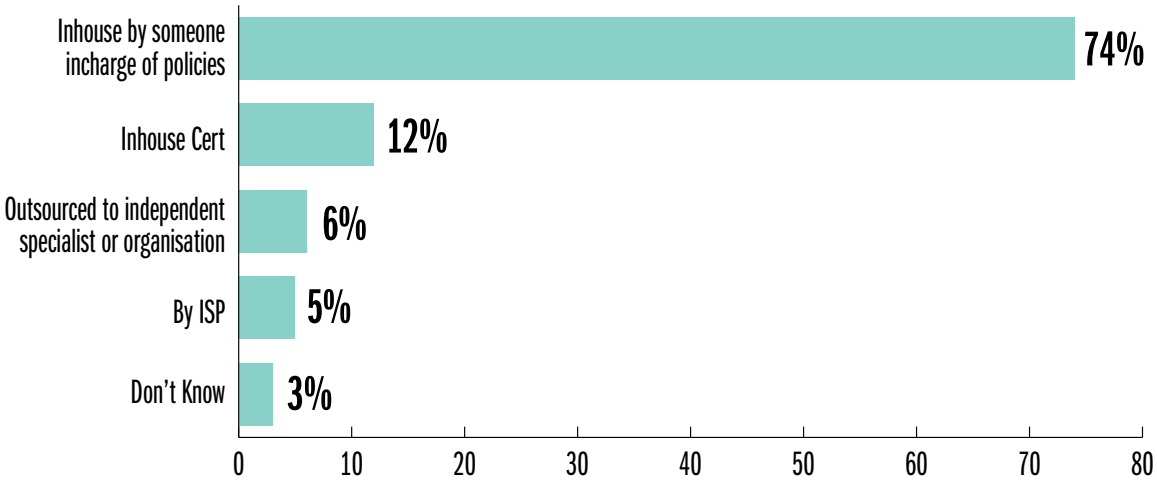


GRAPH 4: CYBERSECURITY SPEND.

MANAGING CYBER SECURITY

74% of organisations manage their cyber security inhouse while 12% 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?

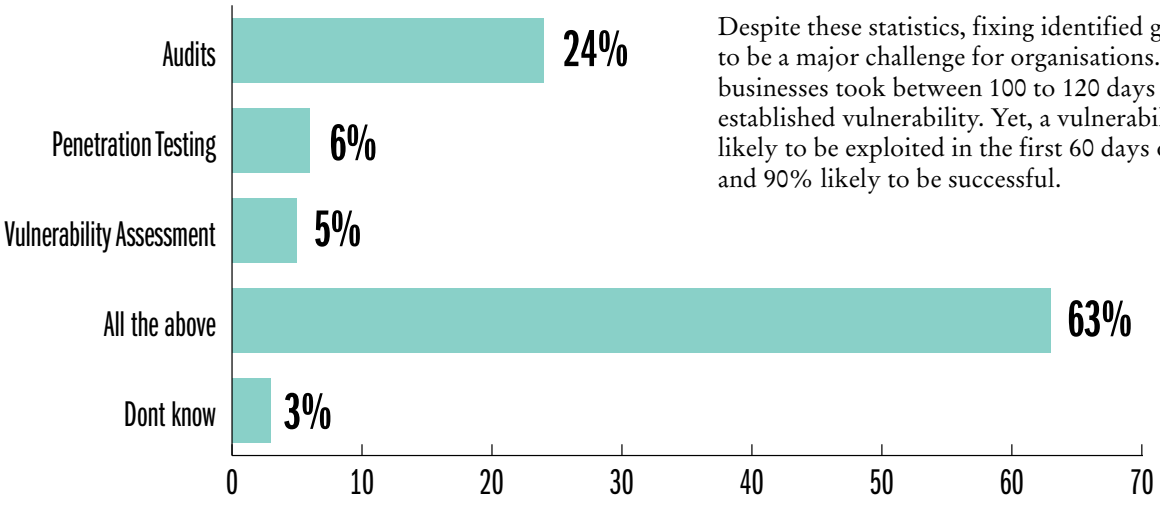


GRAPH 5: CYBERSECURITY MANAGEMENT.

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?



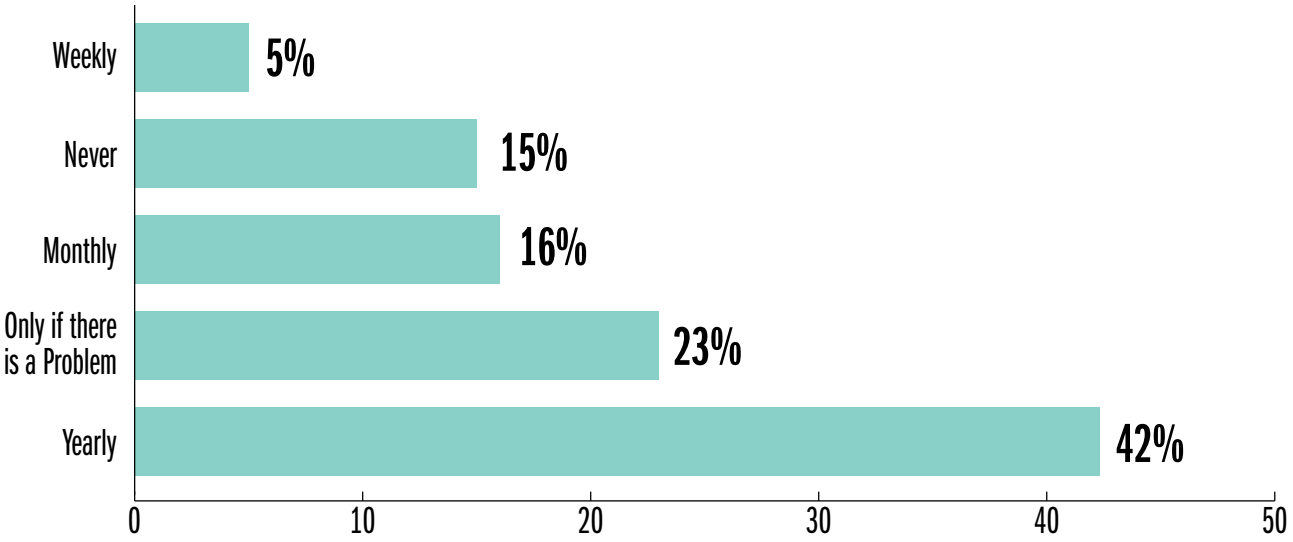
Despite these statistics, fixing identified gaps was found to be a major challenge for organisations. On average, businesses took between 100 to 120 days to fix an established vulnerability. Yet, a vulnerability is most likely to be exploited in the first 60 days of its release — and 90% likely to be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

GRAPH 6: SECURITY TESTING TECHNIQUES.

CYBER SECURITY AWARENESS

The level of cybersecurity awareness in Kenya 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

THE STATE OF CYBERSECURITY IN KENYA'S PUBLIC SECTOR

MARTIN KILUNGU

Information Security Office
Office of the Auditor-General - Kenya

IS THERE A COHERENT, CROSS-GOVERNMENT STRATEGY ON CYBERSECURITY IN KENYA? WHAT INITIATIVES HAVE BEEN PUT IN PLACE TO ENHANCE CYBERSECURITY IN GOVERNMENT INSTITUTIONS?

Yes, in 2014 the government of Kenya launched the national cybersecurity strategy as a guide aimed at securing Kenya's cyberspace while leveraging the use of ICT to promote economic growth. Although much has been done in executing the strategy, it requires constant improvement and review as cyber security is an everchanging landscape.

Among the initiatives originating from the strategy has been the creation of the Information Security Standard, establishment of Kenya National Public Key Infrastructure (PKI), review of Access to Information Act and enactment of the Computer Misuse and Cybercrime Act.

ARE THERE PARTNERSHIPS BETWEEN GOVERNMENT AUDIT OFFICES ACROSS AFRICA?

Yes, government audit offices commonly known as Supreme Audit Institutions (SAIs), in Africa established an umbrella body called African Organisation of Supreme Audit Institutions (AFROSAI) in 1979 which is further divided into AFROSAI-E and AFROSAI-F for English and French speaking countries, respectively. The main aim of this unity is to promote the exchange of ideas, knowledge and experiences among member SAIs. One of the areas AFROSAI-E is focusing on is IT audit and security, with SAI Kenya being an active member in this domain.

WHAT NEW DIGITAL INITIATIVES HAVE BEEN DEVELOPED IN THE PUBLIC SECTOR OVER THE LAST 5 YEARS?

Significant digital transformation initiatives have been witnessed in Kenya's public sector in the recent past. A key highlight has been the launch of the e-citizen platform which has enabled access to most government services online. Others include:-

- Digitization of registries including lands, courts, motor vehicles and citizens "huduma" database
- Adoption of biometric registration and verification of voters, and elections results transmission
- Automation of revenue collection systems by Kenya Revenue Authority and County Governments
- Automation of audit management and the use of data analytics by the Office of the Auditor-General

DIGITIZATION WITHIN GOVERNMENT PRESENTS MAJOR RISKS FOR GOVERNMENTS PARTICULARLY DATA LEAKAGE AND FRAUD. WHAT IS BEING DONE TO REDUCE THESE CASES?

In order to reduce these risks centered on data leakage and fraud, the government of Kenya has been keen to enhance corporate governance in Ministries Departments and Agencies (MDAs). In 2016, the government through the Ministry of ICT launched an ICT policy aimed at addressing some of the technology and information risks. The enactment of the Computer Misuse and Cybercrime Act, review of Access to Information Act, and most recently the initiation of Data Protection Bill are all initiatives aimed at curbing unauthorized access to systems, data leakage and or misuse of information. Courts are now admitting digital evidence through the new laws while the Office of the Auditor General is using business intelligence tools and data analytics to detect fraud perpetrated through electronic systems.

DOES THE GOVERNMENT ENGAGE THE PRIVATE SECTOR OR ACADEMIA IN ITS CYBERSECURITY WORK?

Cybersecurity is an emerging area in Kenya and most government entities do not have the capacity to deal with cybersecurity issues. Some entities are working hand-in-hand with the private sector and Universities, especially on capacity building. How effective are these partnerships? In my opinion, there is still room for improvement on how the government has been engaging with private sector on cybersecurity. There is need for a more structured collaboration across government entities, and by extension private sector and academia especially on cyber intelligence sharing and capacity building.

WHAT KEY CYBERSECURITY COMPETENCIES ARE LACKING WITHIN THE PUBLIC SECTOR?

The public sector has a large pool of ICT professionals but very few have cybersecurity competencies. In my opinion, there are competency gaps on specialized domains of cybersecurity but these are more pronounced in software applications security, cyber incident response and malware analysis.

IT IS SAID THAT PUBLIC SECTOR DOES NOT ATTRACT YOUNG PEOPLE. WHAT IS YOUR VIEW ON THIS?

The public sector does attract young talent especially in this age of unemployment but the motivation is low. The key issue is the perception that public sector has a culture of laziness and lack of professionalism. Most young people are energetic, passionate and curious and require a flexible working environment with innovation as the core objective.

WHAT CAN BE DONE TO ENSURE THAT WE ATTRACT YOUNG TALENT WITHIN GOVERNMENT AND PUBLIC SECTOR?

Public sector entities need to champion a culture change and foster a professional working environment in order to attract and retain young people. By adopting technology, innovation and enhancing employee terms of employment, the government can attract young talent and reverse the current trend where young people think public sector is a place to work towards retirement.

With the continued digitization of the economy, intensifying cyber-attacks and expanding skill gap, lack of specialized skills in cybersecurity if not well addressed may become a national vulnerability in most countries. Governments will need to give special attention to cybersecurity including reviewing their strategies and legislations, and collaborating more with the cybersecurity community and academic institutions. Organisations without relevant professionals will need to look within and reskill and retrain interested staff.

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.

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.

$295m
estimated cost of cybercrime

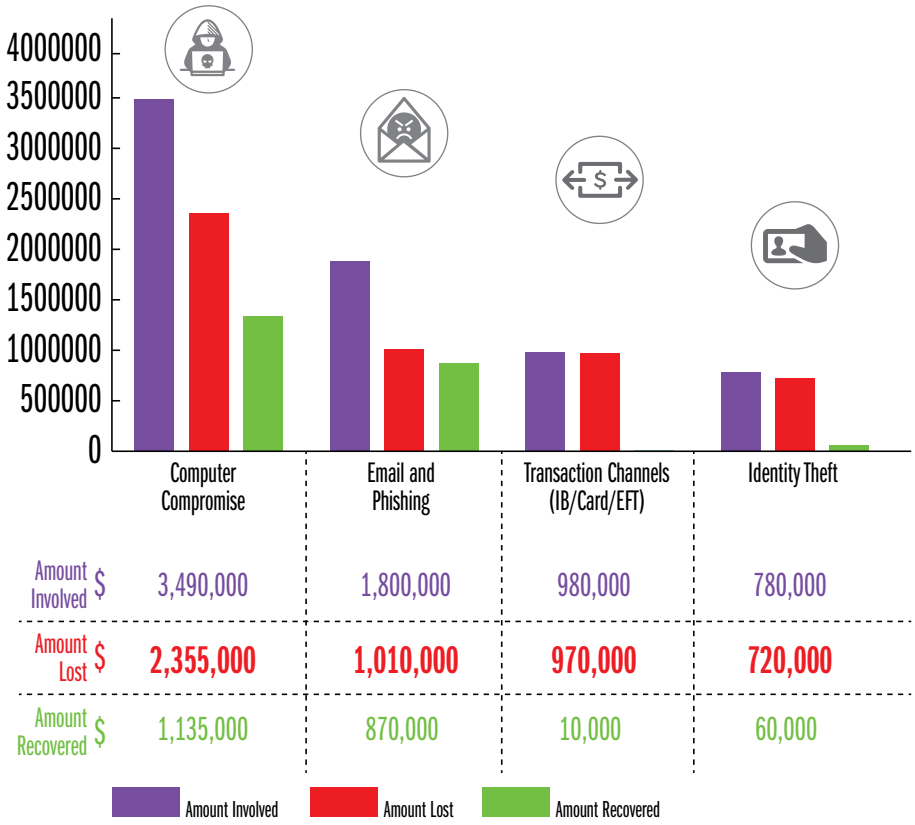
Direct Cost: $88.5m

Indirect Costs: $206.5m

MOST AFFECTED INDUSTRIES

1. Saccos
2. Banking
3. Financial Services Intergrators
4. Betting Firms
5. Government

REPORTED COST OF CYBERCRIME



Amount Lost vs Amount Recovered

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)	64,350,000.00	• 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	59,650,000.00			
Service Providers (Telcos, Fin-tech, Betting, Financial apps)	48,000,000.00			
Healthcare, Hospitality and Retail	7,000,000.00			
Others	27,500,000.00			

Total Indirect Loss: $206,500,000.00

DIRECT COSTS	Estimated Direct Cost (USD)	Activities
Financial Services (Banking, Insurance, Saccos and MFI)	28,000,000.00	• Data hijacking (ransomware attack) • Money lost • Fines from regulators • Law suits • Claims and Cyber Insurance • Forensic Investigations
Government and Public Sector	25,500,000.00	
Service Providers (Telcos, Fin-tech, Betting, Financial apps)	20,000,000.00	
Healthcare, Hospitality and Retail	3,000,000.00	
Others	12,000,000.00	

Total Direct Loss: $88,500,000.00

INDUSTRY PLAYER PERSPECTIVE

TRENDS, CHALLENGES, DEVELOPMENTS AND CYBER SECURITY SKILLS GAP THAT EXISTS IN TELECOMMUNICATION SECTOR

ERIC MUGO

Senior Manager, Fraud Investigation
Safaricom PLC

WHAT DO YOU THINK IS THE GREATEST CHALLENGE FACING THE TELECOMMUNICATION SECTOR?

The main challenge of the telco sector is that it has remained a great channel that is used by attackers to commit fraud.

The next frontier of concern that the Telco ecosystem should be aware of is:

- Commercial banks – These still remain attractive to cybercriminals since they still hold the biggest cash reserves.
- Fintechs – Mobile money lenders that are usually targeted in Bank to Customer Transaction
- Integrators / Aggregators – These are IT firms that are used by banks to carry out transactions.
- Saccos and MFIs – These are a target due to their limited knowledge on security awareness and the lax controls in terms of user access rights on the core banking systems.

WHAT INITIATIVES WOULD YOU RECOMMEND TO REDUCE THE IMPACT OF THESE CHALLENGES?

Implement Robust Cyber security programs in organisations. Invest in technology and people resources with the support of Executive level investments.

Implement transaction monitoring especially for organisations that offer 24/7 digital services where funds transfers and cash transactions form a big percentage of the transactions.

Collaborate with industry peers in terms of incidents response such that reaction time is reduced to bare minimal.

THERE WERE MANY REPORTED CASES OF SIM SWAP ATTACKS IN 2018, WHY IS THIS? WHAT IS BEING DONE TO REDUCE THESE CASES?

The typical telecommunication customer is oblivious of the sim swap threat and further trust their telecommunication company with their data. Unfortunately the trust is abused by criminal elements who will often pose as telecommunication employees and take advantage by extracting necessary information to execute simswaps.

What is being done to reduce cases of Sim Swap is adoption of awareness at the grass root level. This has been achieved by reaching out to local and vernacular media houses and radio stations to help spread the awareness.

Technological controls have also been implemented to prevent simswaps or offer a quick detection path such that the lines suspended before any damage is done. Since then, reported cases of SIM swapping have greatly reduced.

PROCESSES: WHAT KEY AREAS OF THE TELCO ECOSYSTEM SHOULD SECURITY ANALYSTS FOCUS ON TO ENSURE IMPROVED SECURITY?

FOR TELCOS:

- Cybercrime awareness to all stakeholders in the telco ecosystem
- Increased fraud monitoring
- More cooperation with DCI to help curb cybercrime

IT SERVICE FIRMS AND FINANCIAL ORGANISATIONS:

- Carry out thorough background checks to ensure employees are whom they claim to be.
- Invest in cyber-insurance covers that will absolve them of liability in case of such attacks.
- Perform thorough security posture reviews for their infrastructure to proactively close all loopholes that can be exploited by attackers.
- Invest in Cybersecurity and transaction monitoring to guard their infrastructures.
- Take advantage of various Security related services such as managed security solutions, SIM history services from to further secure their businesses.
- Implement two factor authentication as well as dual password ownership for critical infrastructure.

PEOPLE: WHAT KEY COMPETENCIES ARE NEEDED IN THE TELCO SECTOR TO ENSURE CONTINUED SUPPORT FOR INFORMATION SECURITY?

Key competencies required are for analytical skills for big data as well as development of solutions around big data analytics and machine learning. This will go a long way in helping organisations in the ecosystem to detect and stop fraud before it happens.

TECHNOLOGY: FROM YOUR PERSPECTIVE, WHAT ARE THE KEY TECHNOLOGIES THAT ARE TARGETED BY ATTACKERS WITHIN THE TELCO SECTOR? WHY THESE TECHNOLOGIES?

Key technologies targeted are largely those that process transactions particularly with the ability to transfer funds. If not properly secured, such systems will be compromised by cybercriminals with the main objective of stealing those systems. The next frontier will be data theft.

HOW DO THE LOCAL LAWS AND REGULATIONS ADDRESS THE ISSUE OF CYBER SECURITY IN TELCOS? (ISSUES SUCH AS ORGANISATION STRUCTURE/ROLES AND RESPONSIBILITIES, TECHNOLOGIES, TRAINING, SECURITY ASSESSMENTS ETC) WHAT WOULD YOU RECOMMEND?

Currently, there is no law addressing the issue of Cyber security from a Policy perspective. However the regulators both in Financial industry and telecommunication have come up with comprehensive guidelines which if adhered to in addition to international best practices are enough to build Cyber security programs to a mature level such that they are resilient against any cyber-attacks.

WHAT ARE YOUR EXPECTATIONS FOR 2019?

There has been a general increase in the number of organisations targeted, the amounts targeted as well as those lost. It is my hope that going forward this trend will change after comprehensive security assessments and sufficient awareness have been implemented across all sectors.

I am also hoping to see much better collaboration between stakeholders, law enforcement and Judiciary to help investigate, prosecute and convict cyber criminals.

FOCUS ON 2019 LIKELY TARGETS AND NEW WAYS TO MOVE FUNDS

COMMERCIAL BANKS

Commercial Banks remain attractive due to their amount of money available as well as ease of recruiting their staff.

SACCO'S AND MFI'S

Sacco's and MFI's are an easy target due to their perceived immature information security posture as well as ease of recruiting their staff.

They remain less attractive compared to banks and integrators.

FINTECH'S

Fintech's largely covers mobile money lenders. They are targeted from a Mobile lending and B2C fraud perspective.

INTEGRATORS/AGGREGATORS

These are IT firms offering service as a product. They carry and are responsible for transactions of various organisations.

They are attractive due to the large pool of funds at their disposal for their different clients.

NEW CREATIVE WAYS TO EXIT FUNDS

- Sports betting wallets.
- Bank prepaid cards
- International money transfer.

CURRENT

- Digital currencies
- Virtual bank accounts

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.


CRIME SCENE DO N
5
5
3
3

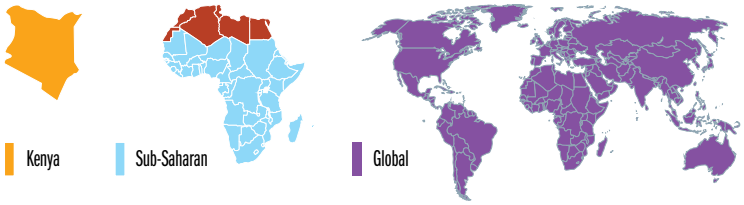
CYBER SECURITY SKILLS GAP

Kenya 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 Kenya to determine the approximate number of skilled professionals within the country.

FIGURE 1: OBIS QUAS ACERCHILIT FUGITAE CUM VOLE.

No. of Skilled Professionals in 2018



		Kenya	Sub-Saharan	Global
ISACA	CISA Certified Information Systems Auditor	586	3795	84,484
	CRISC Certified in Risk and Information Systems Control	42	646	19,163
	CISM Certified Information Security Manager	134	945	32,233
	CGEIT Certified in the Governance of Enterprise IT +Others	-	324	5749
(ISC)²	CISSP Certified Information Systems Security Professional	53	844	*
CEH, CHFI, CCNP, CompTIA, OSCP	OTHERS	885	6554	*
	TOTAL	1700	13,500	*

(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

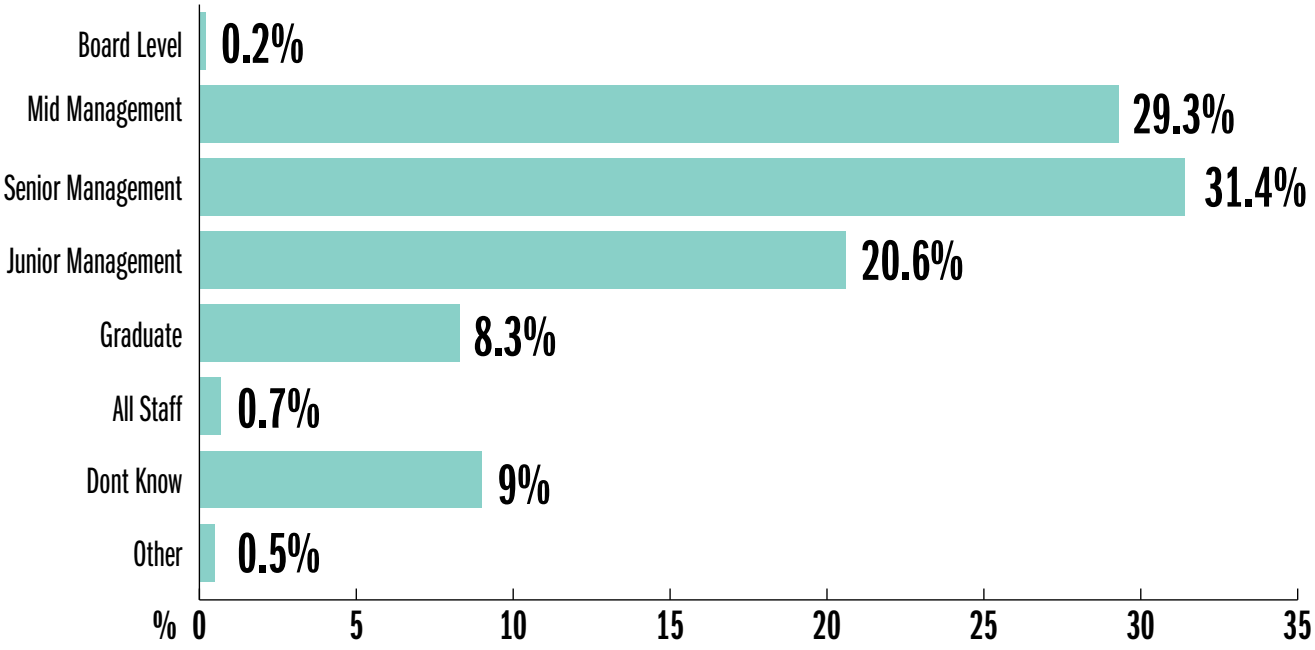
The above figures are estimates, for more accurate data, please confirm with the specific training institutions.

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

FIGURE 2: SKILLED PROFESSIONALS.

To determine where the pain points are, we asked over 300 professionals to provide more insights on the issues they faced. Below are the findings:

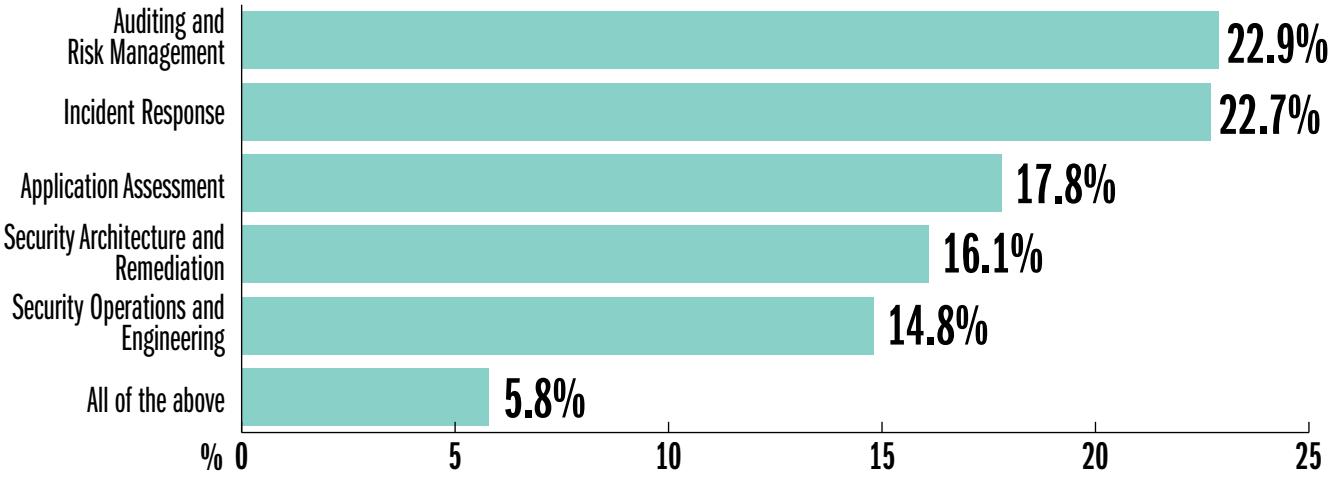
AT WHICH LEVEL DOES YOUR ORGANISATION FIND THE SKILLS SHORTAGE TO BE THE MOST ACUTE?



GRAPH 8: SKILLS SHORTAGE PAIN POINT.

All industries reviewed declared a challenge in finding top-tier professionals. About 60% 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.

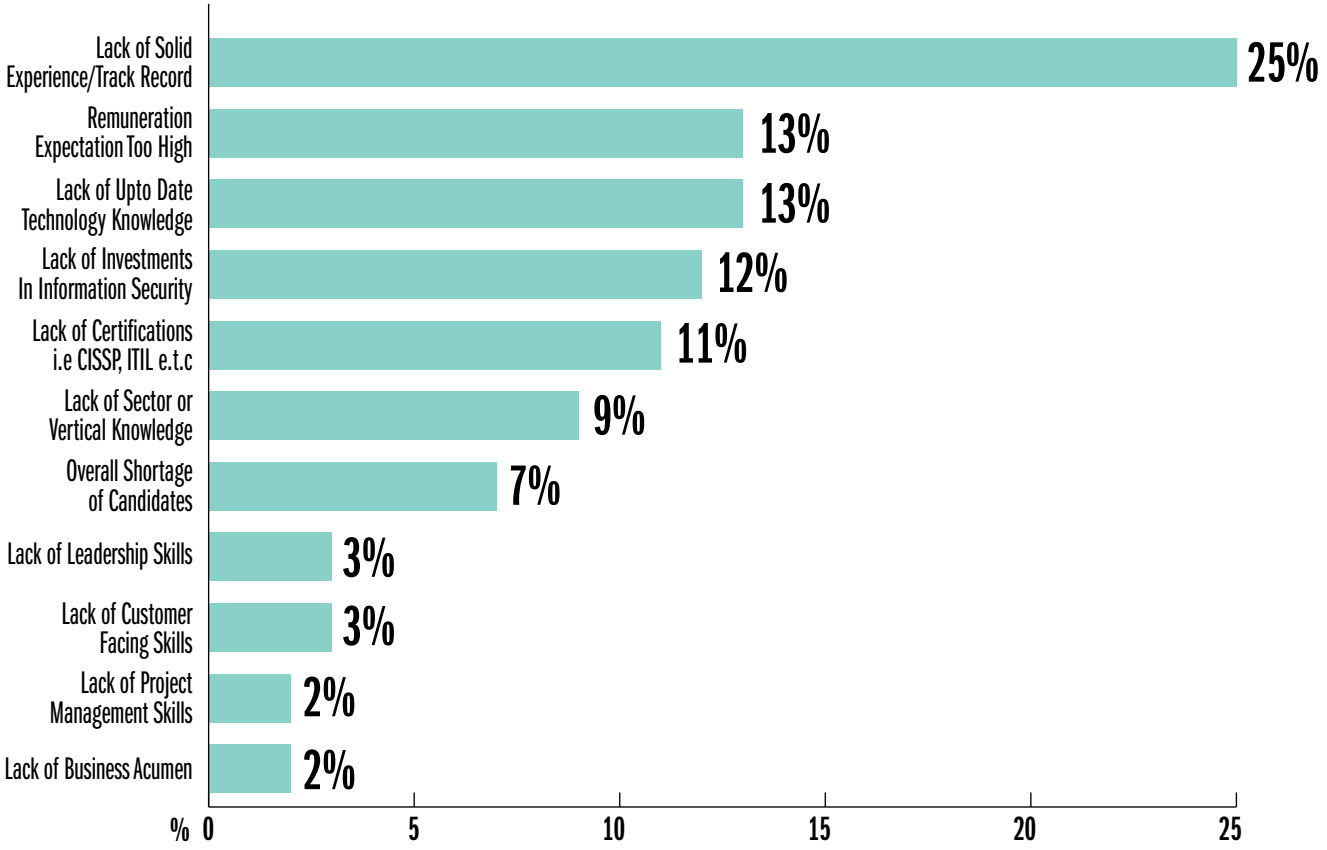
Security Architecture and Engineering allows an organisation to start with the very basics. Build a strong foundation upon which security technologies and processes can be build.

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

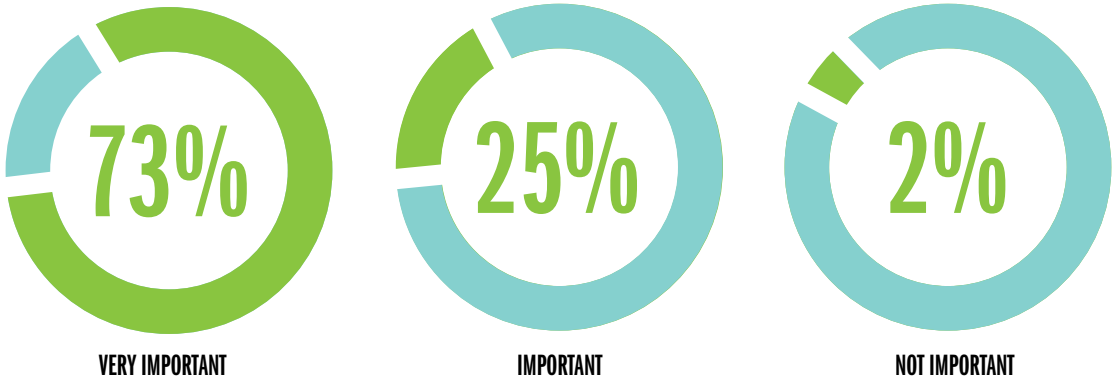
Hiring new skilled professionals has become strenuous this is because they are few and easily poached by the highest bidding recruiters.

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." Raconteur

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

DEMYSTIFYING AFRICA'S SKILLS GAP

PAULA MWIKALI

Research Associate Director, Centre for Informatics Research and Innovation (CIRI), Digital Forensics, Information Security Audit Lecturer USIU- Africa

There is global consensus that there is a cybersecurity skills gap and this gap is widening. The 2018 (ISC)2 Cybersecurity Workforce Study puts this shortage at about 2.9 million people globally with the EMEA region (that includes Africa) accounting for a shortfall of about 142,000 people. This has surpassed previous predictions that by 2020 this skills gap would be at 1.5 million. The Enterprise Strategy Group (Oltsik, 2019) states that organisations reported a 53% shortage of cybersecurity skills in 2018-2019 and this percentage has increased every year since 2015. Furthermore, ISACA's 2019 State of Cybersecurity Report (ISACA, 2019) reports that organisations are struggling to fill cybersecurity positions and retention of qualified individuals is very difficult.

This skills gap has been created because the demand for cybersecurity staff is much higher than the current sources of supply can meet. Using a simple framework that considers both demand and supply gives us a useful tool to demystify the factors that have led to this skills gap and subsequently enable us to identify solutions to address it.

Let's start by examining the demand side of the equation. The demand for cybersecurity staff has predominantly arisen from the wide-scale adoption and reliance on information systems. Every aspect of our personal, social and business life is increasingly becoming dependent on technology. As we adopt smart devices in everyday life, the distinction between what is 'virtual' and what is 'physical' is slowly fading and attack options are increasing. Commuting with internet enabled and driverless cars is expected to be commonplace in the not-so-distant future. It is predicted that 90% of the cars produced by 2020 will be connected to the internet (Jabil, 2018). The Internet-of-things is ushering us to the 4th industrial revolution that promises great efficiencies and levels of productivity (Till, 2018). Wearable technology is trending in the consumer marketspace with options for microchip implantations available (Edwards, 2018).

The vast amounts of data generated as we interact with technology is being harvested and information systems are being built to ingest this big data, analyze it and use it to influence our current and future actions. This has led to the big data and analytics wave (Verma, 2018). Governments are increasingly centralizing systems and collecting vast amounts of citizen data. An example worth highlighting is the Indian Aadhaar system that is considered the largest repository of Personally Identifiable Information (PII), including biometric data, for over 1.2 billion individuals. Kenya is following suit with the recently launched Kenya Huduma Namba system.

All these elements have created huge treasure troves that have attracted nefarious actors willing to exploit them for fraudulent gain. Huge repositories of personal information such as those provided on Aadhaar have led to the largest known data breach world-wide with all records of over 1.1 billion citizens compromised (Sapkale, 2019). Such large data sets present high hack-value platforms and the international hacker community cannot resist the temptation. This makes identity theft a gruesome reality for many. These bad actors are highly motivated, well-resourced and skilled. They have established great collaboration over the dark web, meet-ups and knowledge sharing platforms that enable them identify vulnerabilities in systems and exploit them quickly before they can be fixed. As we use smart and autonomous devices, the danger is no longer just about the information that can get into the hands of malevolent actors but more about what they can do to hurt us physically. The risk to physical harm was clearly demonstrated in 2015 through the hacking of a Jeep Cherokee and subsequently in 2016 when its braking system was disabled leading to its crash (Osborne, 2018). Threats of cyber warfare and cyber terrorism are increasingly becoming a reality when critical infrastructure such as nuclear facilities, electricity grids, hospital systems and air traffic control systems become accessible through networks.

This kind of pervasive reliance on information systems and smart technology has created a huge need for skilled people to protect us. In many cases their services are required 24 hours a day and 365 days a year. They are required to have advanced skills that cut across different technology spheres due to the interconnected nature of systems. ISACA's 2019 State of Cybersecurity Report adds that organisations are not only looking for individuals with such technical skills but more importantly those who understand the business context and can apply their skills to meet enterprise goals. That makes it even harder to find such individuals and even harder to retain them.

The supply side of the equation has unfortunately not grown at the similar rate. There are efforts to train cybersecurity professionals in colleges and universities to meet this exponential demand. Statistics show that only 5% of the Universities in East Africa offer Bachelor-level Information Technology courses with specializations in Cyber Security (Muchiri, 2019). A look through the approved academic programs offered by Universities in Kenya as at November 2018 (CUE, 2018) shows that there are only 3 Bachelor of Science degree programs, 4 Masters programs, 2

Post Graduate Diploma programs and 1 Doctor of Philosophy programs in the area of information security. This represents a meager 0.2% of the over 4,000 degree programs offered in Kenyan universities and is likely to represent approximately 100 graduates annually specializing in information security.

The reality is that organisations are unlikely to directly hire fresh graduates into cyber security positions. Fresh graduates often lack adequate hands-on skills and are low on business acumen and organisations need to establish trust with these employees. ISACA (2019) State of Cybersecurity Report points out that majority of cybersecurity positions remain unfilled because applicants lack necessary qualifications. Fresh graduates are often expected to prove technical expertise by undertaking professional certifications. The top ten security certifications (Trueman, 2019) that boost employability include the entry-level ones like CompTIA Security+, SANS GIAC Security Essentials (GSEC) and Certified Ethical Hacker (CEH) and the more advanced hands-on Offensive Security Certified Professional (OSCP) for penetration testers. Other certifications like the Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) and the Certified Protection Professional (CPP) target those moving into managerial levels after requisite years of experience.

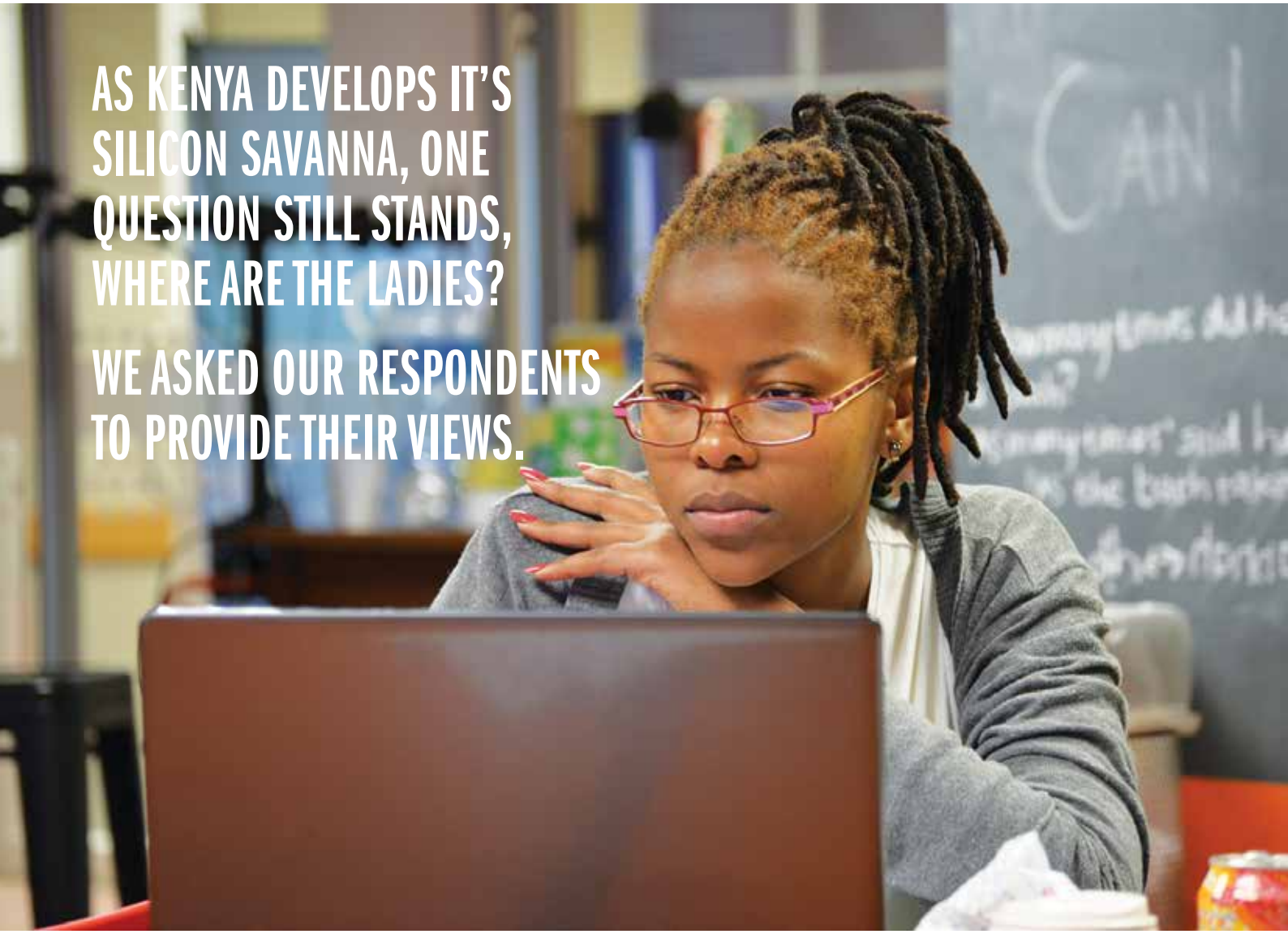
The Cyber Security space is demanding and requires professionals to continue learning and engaging so as to keep up with the emerging threats. There are now numerous options available to people seeking to grow their cybersecurity skills. There are many online courses and resources available many of which are freely available (Carey & Turner, 2019) from sites like Cybrary, Udemy, Coursera, EdX and many more can be listed using services like MOOC List (2019) and Class Central (2019). One that is gaining popularity as practical online platform with real-life scenarios for practicing cyber security skills is Immersive Labs (2019).

Therefore in light of these considerations, the way to close the cyber security skills gap is by increasing the supply side of the equation. We are clearly on a trajectory of exponential demand which will not change soon. A collaborative ecosystem involving academia, professional bodies, public and private organisations has to work together to deliver qualified and competent individuals who can deliver on business objectives.

SEE REFERENCES IN THE APPENDIX

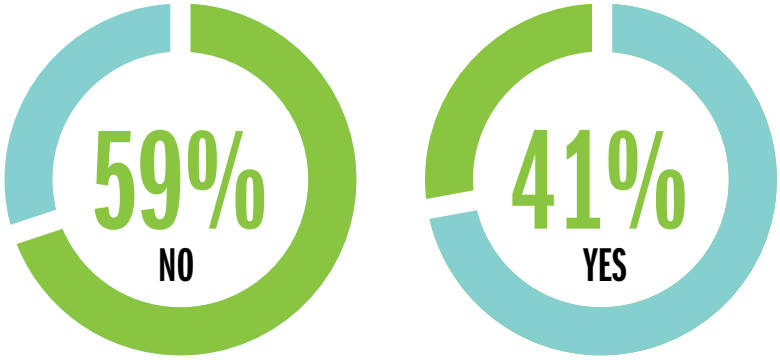
THE GENDER GAP

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.



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 is 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. They include Shehackske, AkiraChix, Shesecures and Africa Cyber Immersion Center (ACIC) to mention a few.

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"

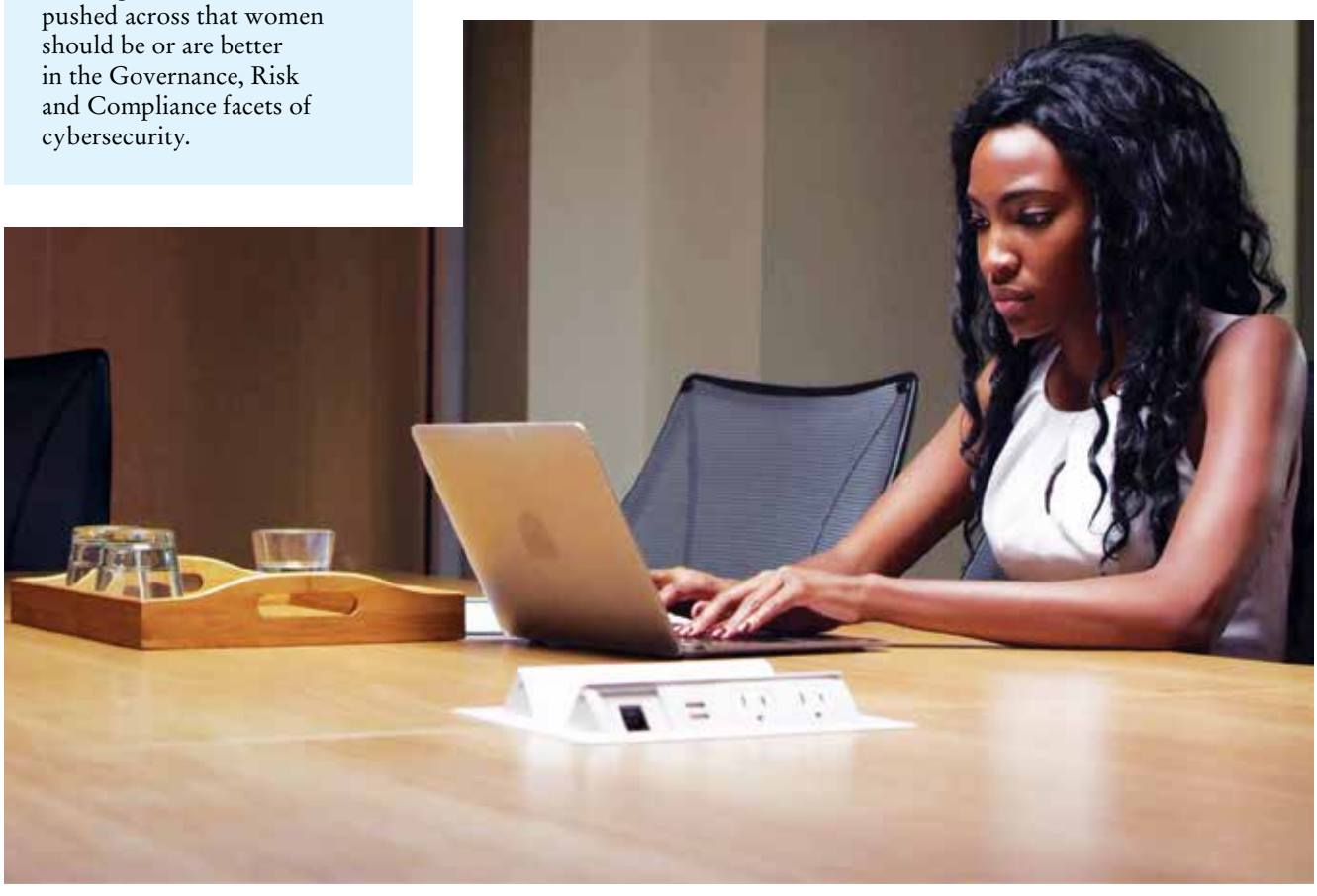
THE TECHNICAL SKILLS QUESTIONS?

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.



STATE OF CYBER INSURANCE IN KENYA

DESPITE GROWING CYBER RISK, AFRICAN CORPORATIONS ARE SLOW TO ADOPT CYBER INSURANCE. WHY IS THIS?

Lack of Awareness. Digital technology in Kenya is increasingly becoming a threat to industries and organisations. With the integration of technology into businesses and the inclusion of emerging innovations such as Internet of Things (IOT) and Artificial intelligence, organisations have to develop risk, resilience and mitigation plans in order to secure their environment hence the need for cyber insurance. Cyber Insurance involves the coverage of not only technology assets but any fallout that occurs due to cyber-based attacks. Organisations in Kenya have not fully embraced cyber insurance due to:

- Lack of knowledge of the advantages of the service
- High cost implications of investing on the stated minimum requirements with the inclusion of annual premiums.
- Lack minimum requirements of implementing cyber insurance in the organisation
- Industries are scared of the implications of an increase in premiums as the number of threats increase.
- Insurance premiums are charged based on the criticality of data stored meaning that financial and health care industries are charged more.
- Cyber insurance claims may rescind due to a lack of minimum-security controls

WHY SHOULD AN ENTERPRISE TAKE UP A CYBER INSURANCE COVER? WHAT OPPORTUNITIES DOES CYBER INSURANCE PROVIDE TO ORGANISATIONS IN AFRICA?

Organisations should implement some form of risk mitigation for its cyber risks. Risk management requires that organisations implement a strategy on identifying, preventing and resolving risks. Cyber insurance helps the organisation mitigate such risks by offering coverage for losses sustained during an attack. Management no longer has to worry about the losses due to compensation but they will have to come up with ways to mitigate the attacks from occurring again.

HOW DO YOU DETERMINE CYBER RISK EXPOSURE FOR AN ORGANISATION?

Cyber risk exposure is determined by identifing and assessing all risks, implementing controls to mitigate the risks, veriffying that you are compliant with governing regulations and implementation of continuous improvement. The rule that should always govern organisations while developing strategies around cyber insurance is that the more security controls implemented the lower the premiums. Ideally, if the organistion does not have skilled professionals to help determine the organisations cyber risk exposure, they can always use a third-party to conduct the analysis.

ARE THERE ANY LOCAL LAWS AND REGULATIONS THAT ADDRESS OR PROMOTE CYBER INSURANCE?

There are no specific laws that target Cyber Insurance, however general Cybersecurity laws and regulations such as GDPR, Cybercrime act, CBK guidance note, Bill of rights, Data protection bill etc guide organisations on how to attain the minimum-security requirements.

WHAT FUTURE TRENDS SHOULD WE ANTICIPATE WITHIN CYBER INSURANCE SECTOR?

Cyber Insurance is expected to grow exponentially. As various legislations (GDPR, Data protection bill, CBK prudential guidelines etc) are implemented, the uptake of Cyber Insurance will increase.

AN ESTIMATED **$7,000,000** WAS PAID OUT IN CLAIMS IN KENYA IN 2018.

MANY ORGANISATIONS IN KENYA HAVE TAKEN UP CYBER INSURANCE FROM INTERNATIONAL PROVIDERS, MAINLY BASED IN UK.

MAJORITY OF THE INSURANCE COMPANIES LACK THE APPETITE FOR CYBER INSURANCE BECAUSE THE EXPOSURE IS TOO HIGH.

INDUSTRY PLAYER PERSPECTIVE

RAYMOND BETT

President, ISACA-Kenya Chapter

WHAT ARE SOME OF THE CYBERSECURITY CHALLENGES FACING THE INDUSTRY?

- Right Skilled Professionals. It is becoming a big challenge to ensure that organisations have skilled personnel with the required credentials, technical skills and communication skills that can help address cybersecurity challenges.
- Inadequate Budget. Lack of awareness or perception within the organisations board members leads to the lack of mobilization of funds to address key risks affecting industries.
- Increased Threat Landscape. We see adversaries localizing and weaponizing cybercrime to suit local needs. Gone are the days of random ransomware or virus attacks but now attacks are specialized with a clear goal in mind. If mobile banking is popular in Kenya, attackers are mapping out weaknesses in the transaction chain and with collusion of insiders are able to perpetrate serious attacks.

WHAT INITIATIVES WOULD YOU RECOMMEND TO REDUCE THE IMPACT OF THESE CHALLENGES?

Reducing the Skill Gap.

Once you get the right skilled professionals, we need to train them using hands-on courses, so they are able to stay on top of the latest issues and trends. We need to connect them with their peers so they can better share information. Increasing the awareness of all other users.

Increasing Budget.

While budget will always be a problem, one of the key ways to address this is by mapping out the risk and finding a solution. This needs to be organisation and industry specific. Further awareness to the decision makers will also come in handy.

Opting for Resilience.

Constant vigilance is needed to address the evolving threat landscape. We have to focus on cyber resilience through embracing core concepts of cybersecurity which includes detection, prevention, response and recovery.

WHAT ARE YOUR EXPECTATIONS FOR 2019?

Greater awareness on cybersecurity matters outside the traditional financial sector to other industries such as government institutions, the education sector, manufacturing and non-profit organisations. We are likely to see an increase in the number of cyber security professionals equipped with the right skills matrix. We shall also see organisations prioritizing cybersecurity in the board rooms as security strategy becomes aligned with business objectives.

On the downside, we shall also see more targeted attacks which will also target the SME sector and social media with the increase in fake news and ransomware.

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: OBIS QUAS ACERCHILIT FUGITAE CUM VOLE.

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 Kenya 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.

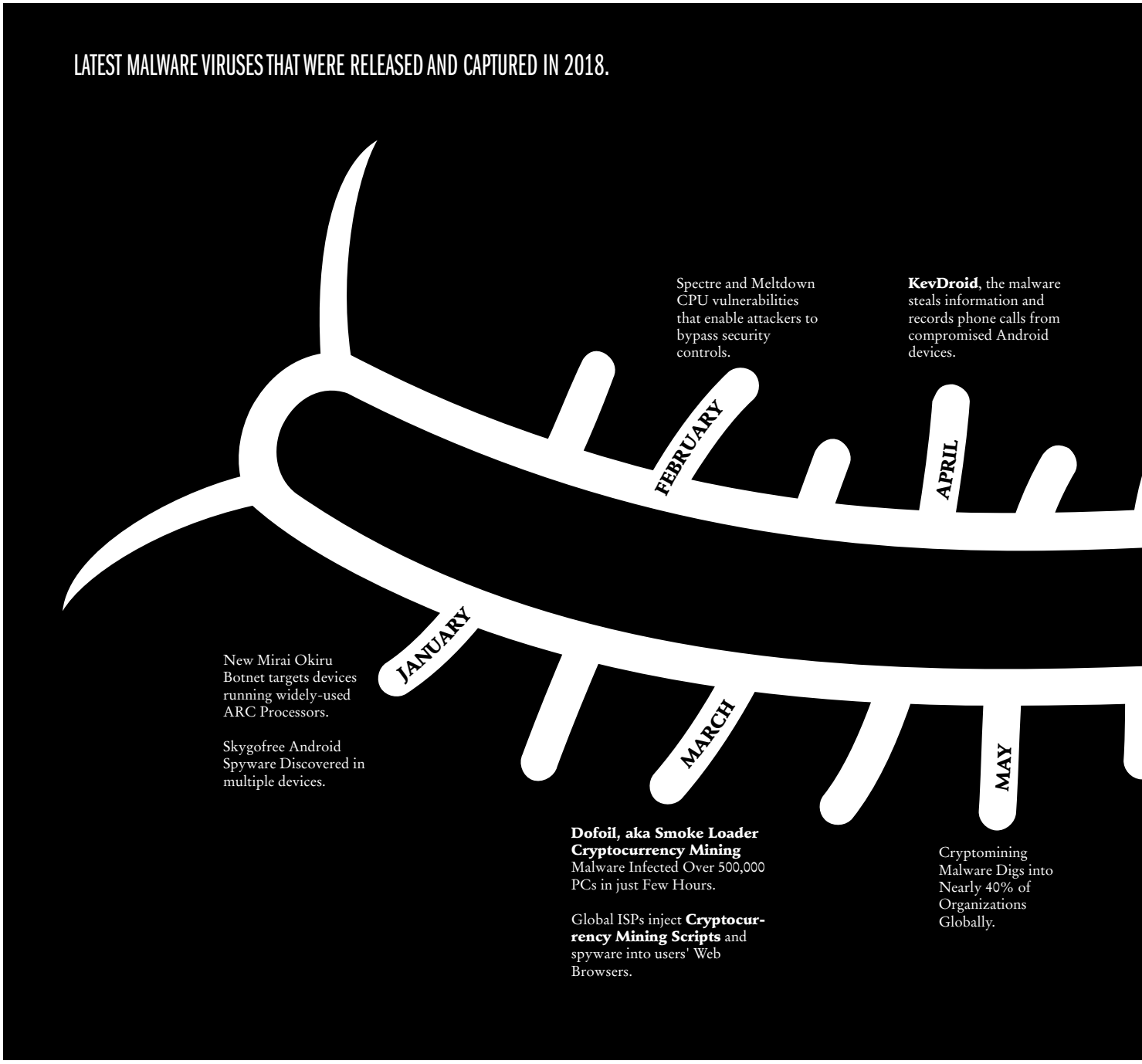
Another challenge exists within the full integration of ICT and cybersecurity skills in the school curriculum within the education system as a means of reducing the number of cybersecurity attacks targeting individuals. The government has supported the inclusion of ICT in the academia sector but has 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



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.

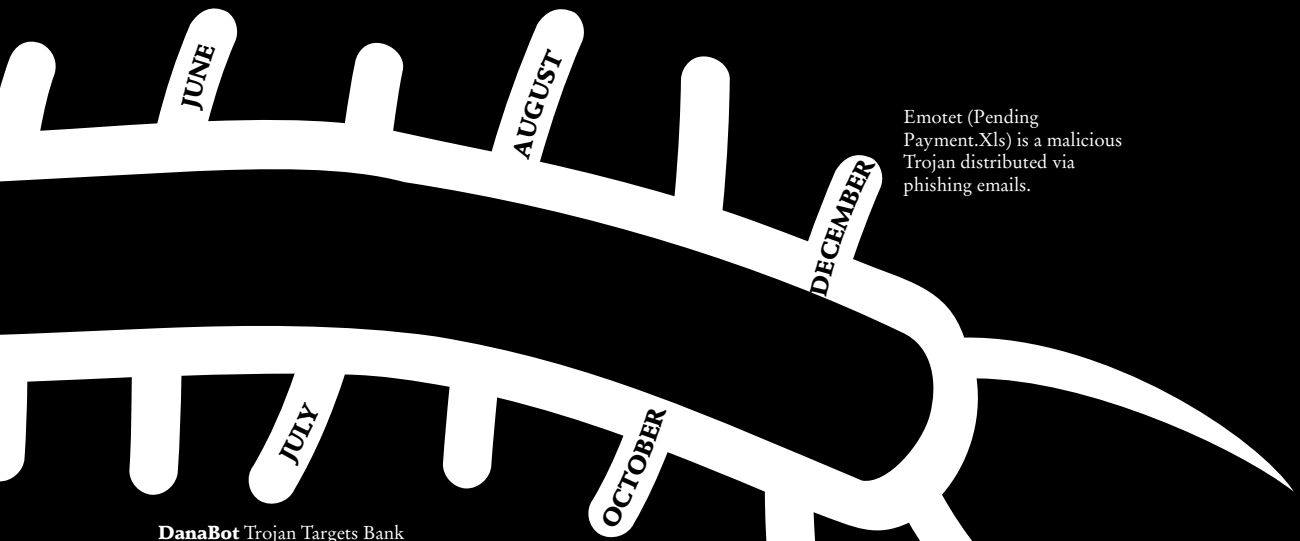
Locally re- engineered Malware discovered by the ACIC team;

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.

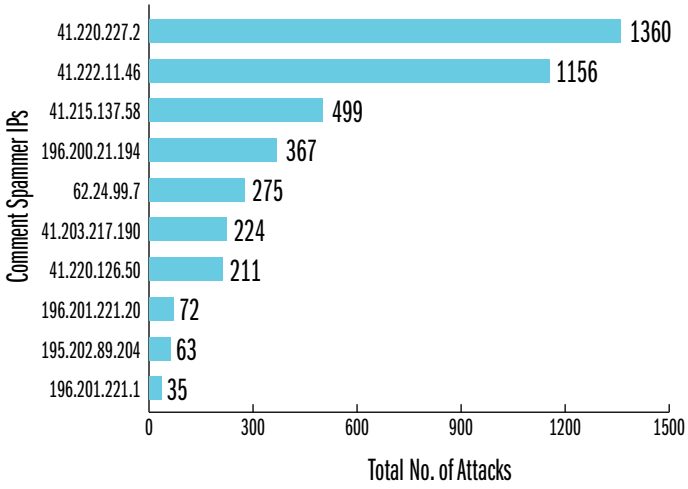
Rakhni Malware Variant. This malware infects systems with either a cryptocurrency miner or ransomware.

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

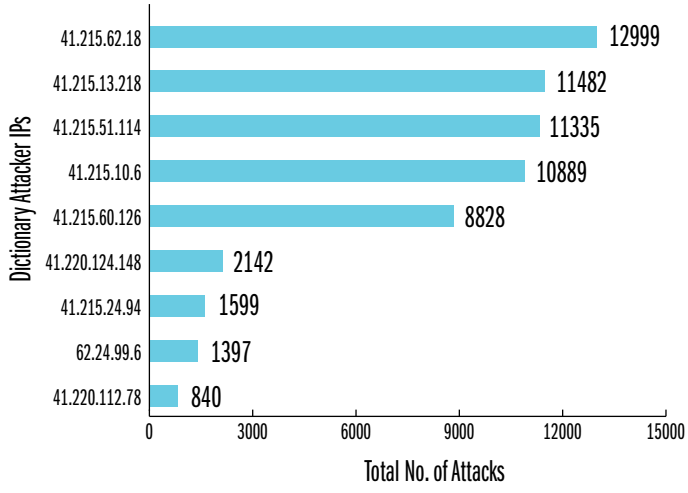
The main aim of this phase was to identify active systems easily accessible online and using this information identify areas of weaknesses and attack vectors that can be leveraged by malicious players to cause harm.

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



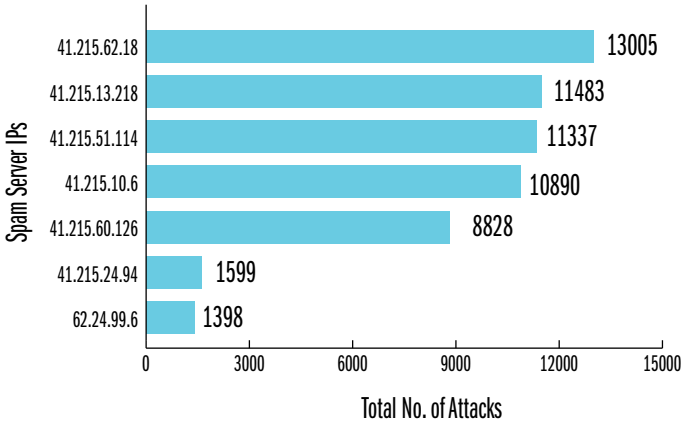
GRAPH 13: COMMENT SPAMMER IPS

A dictionary attack involves making up a number of email addresses, sending mail to them and seeing what is delivered.



GRAPH 14: DICTIONARY SPAMMER IPS.

A spam server –The computer used by a spammer in order to send messages.



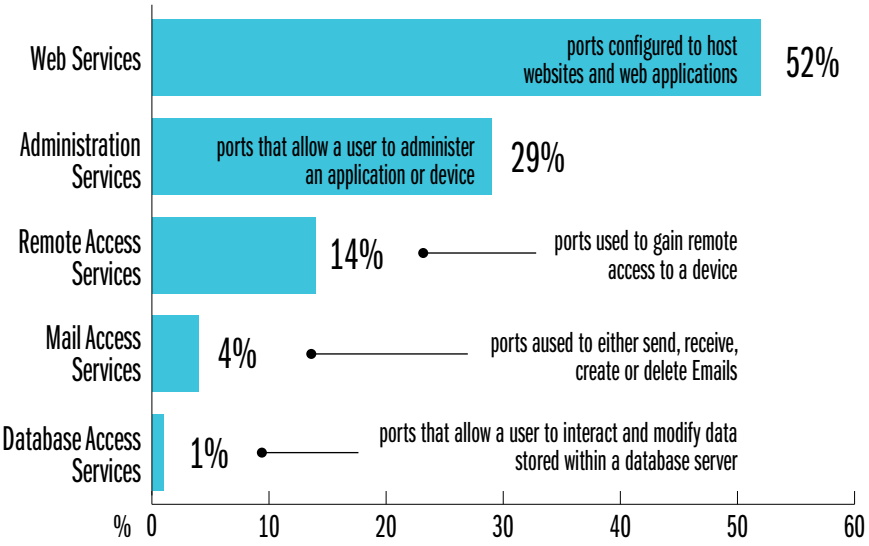
GRAPH 15: SPAM SERVER IPS

> 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

OPEN PORTS

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

We categorized the services into the following:

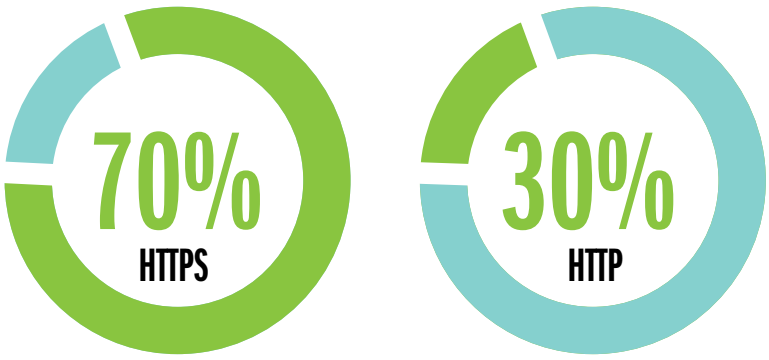


GRAPH 12: EXTERNALLY ACCESSIBLE SERVICES.

WEB SERVICES

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

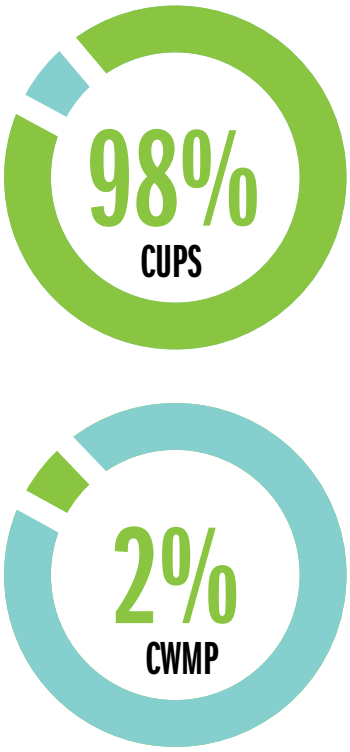
CHART 11: WEB SERVICES.



ADMINISTRATION SERVICES

Administration services are protocols that allow system administrators to configure their devices. As part of the top ten (10) open ports, we identified a printing service port (2%) CUPS and (98%) CPE WAN Management Protocol (CWMP).

CHART 12: ADMINISTRATION SERVICES.



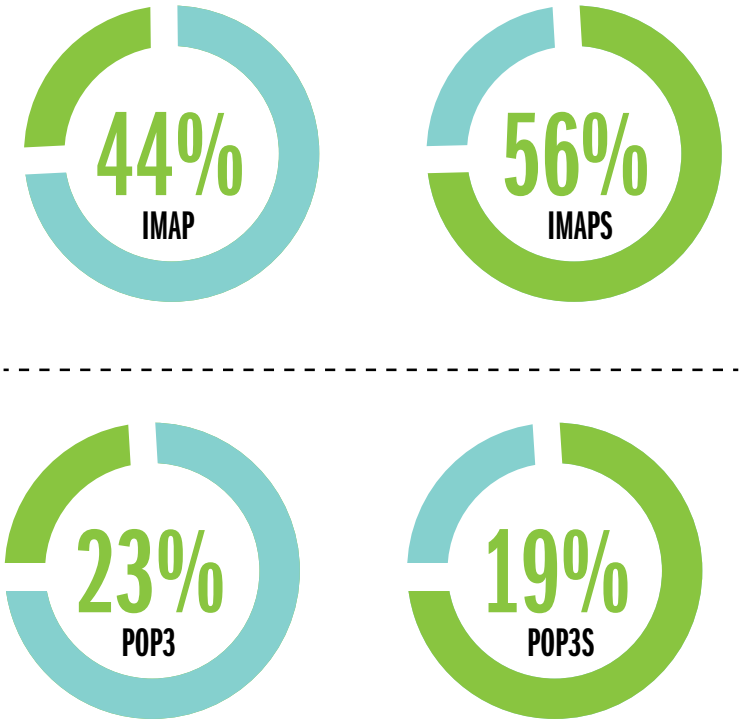
CUPS manages print jobs and queues and provides network printing while CWMP protocol enables devices to be remotely configured through the use of SOAP based Remote Procedure Calls (RPC).

- 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

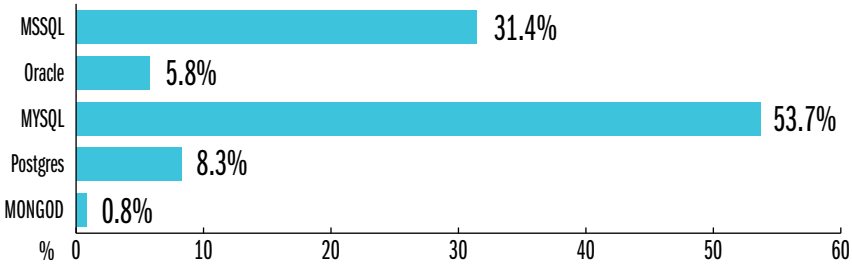
KENYA

CHART 13: MAIL ACCESS SERVICES.



DATABASE ACCESS SERVICES

KENYA



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.

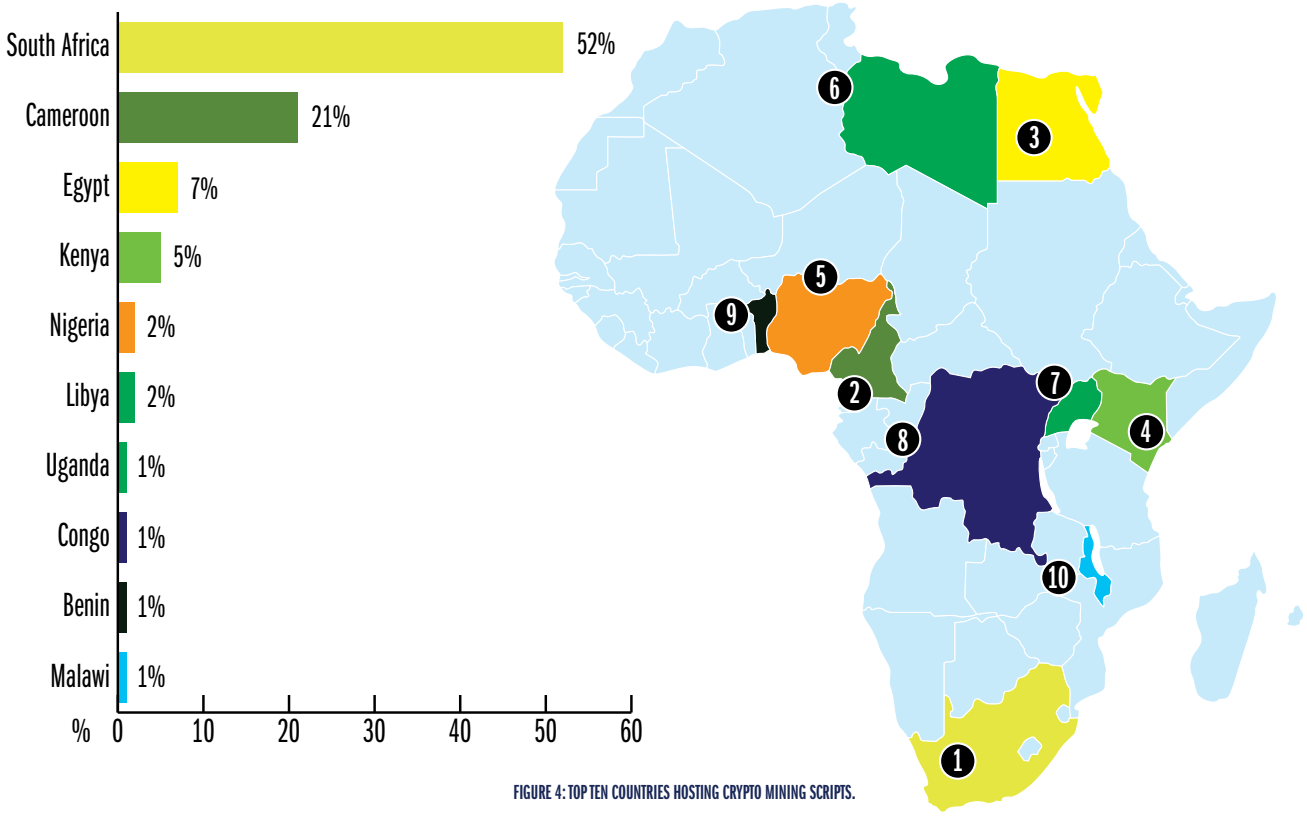


FIGURE 4: TOP TEN COUNTRIES HOSTING CRYPTO MINING SCRIPTS.

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

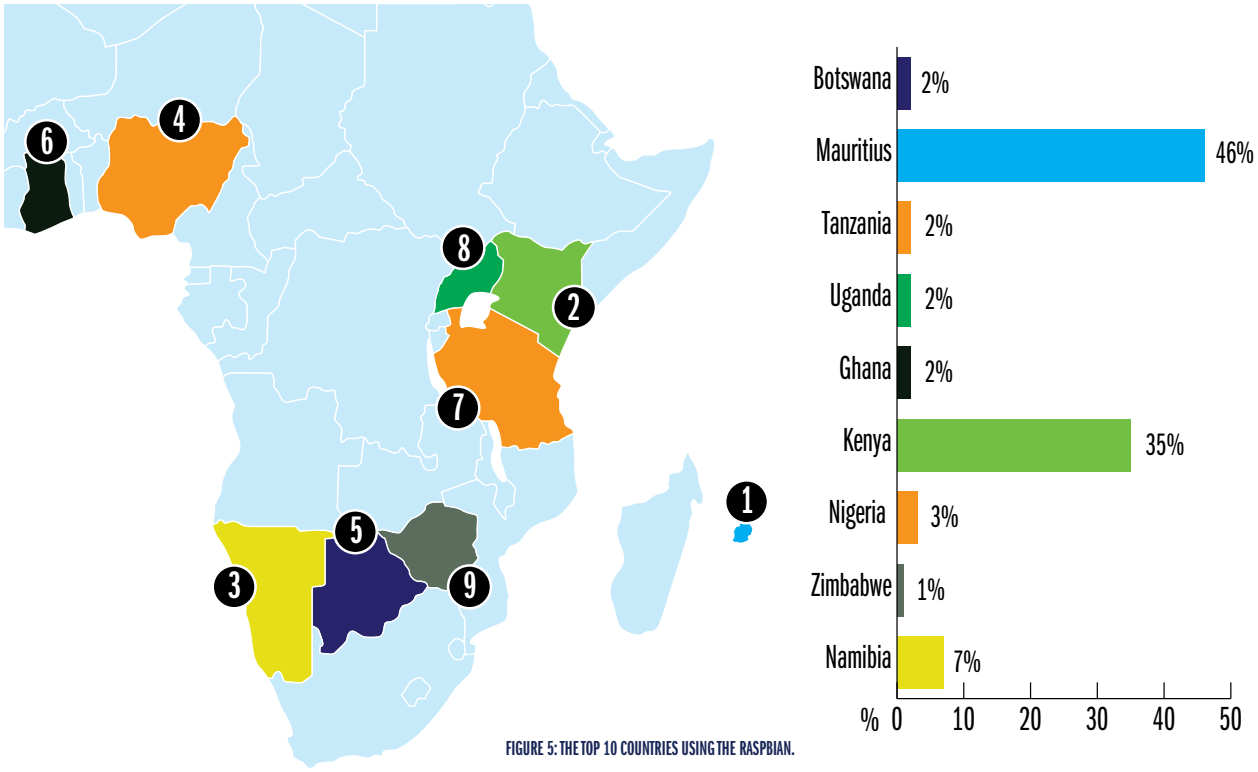


FIGURE 5: THE TOP 10 COUNTRIES USING THE RASPBIAN.

DNSSEC ADOPTION

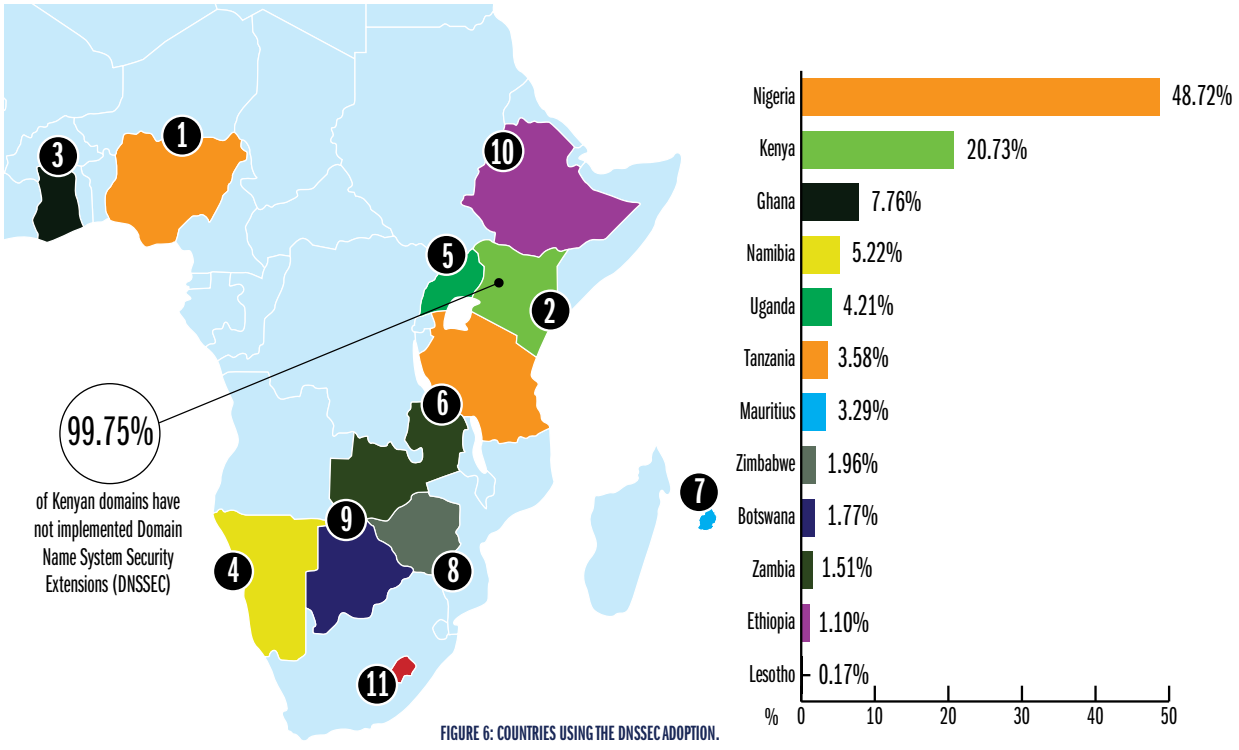
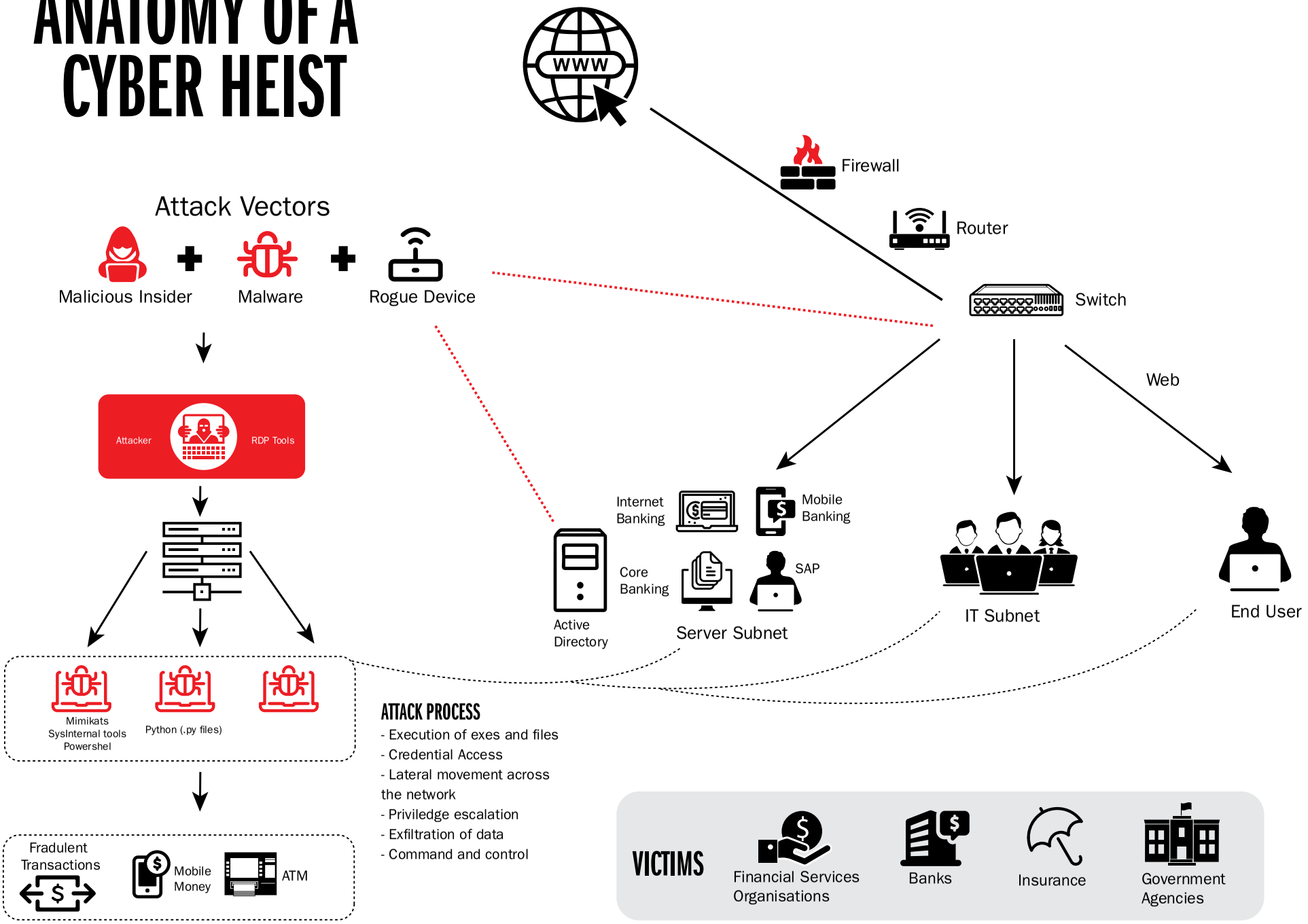


FIGURE 6: COUNTRIES USING THE DNSSEC ADOPTION.

ANATOMY OF A CYBER HEIST



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.

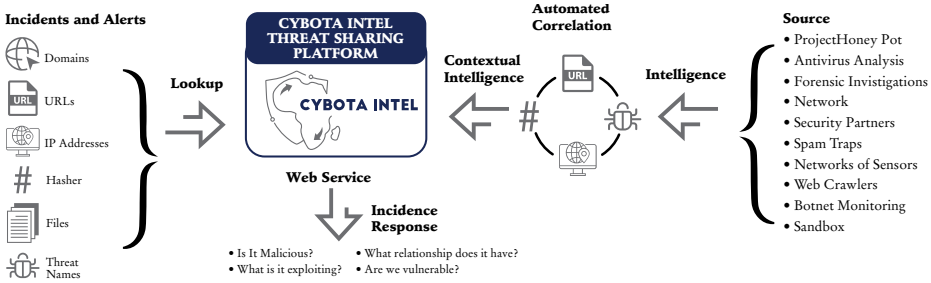
Rapid Response: Early detection leading to rapid incident response.

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

TOM MBOYA

Head of ICT, Unga Group Ltd

WHAT WERE THE BIGGEST TRENDS FOR THE KENYAN MANUFACTURING INDUSTRY IN 2018 (ERP IMPROVEMENT, BIG DATA ANALYTICS FOR ENHANCED VISIBILITY)?

I would go with ERP Improvement. Most manufacturing companies in previous years have worked on acquiring and implementing an ERP of some sort such as SAP, Oracle, Navision, etc. and are now currently working on improving its utilization, reporting and compliance to business and security regulations.

ARE THERE ANY INTERESTING TECHNOLOGIES AND REGULATIONS THAT HAVE COME UP THAT DEMAND A CHANGE IN TECHNICAL OPERATIONS IN MANUFACTURING INDUSTRIES? WHAT ARE THEY AND WHAT IS THEIR IMPACT, FROM YOUR POINT OF VIEW?

I think Artificial Intelligence, Business intelligence, Robotic IoT, Robotic Process Automation (RPA), GDPR and Lean Six Sigma are a current trend in the manufacturing industry. Industries are trying to enhance their competitive edge by embracing Business Intelligence modules existing on the ERP platforms.

My current interest is in Robotic Process Automation (RPA) and its role in simplifying and automating our daily processes at Unga Group. Of course, this only covers machine related tasks so, we implemented Kaizen techniques derived from Lean Six Sigma to aid in the continual improvement of processes. After streamlining processes within the business, advancing into IOT, Machine learning and Artificial intelligence-based solutions are items we are looking forward to.

As a means of being compliant with regulations, Industries are implementing General Data Protection Regulation (GDPR) and The Data Protection Bill 2018 laws as a means of securing customer and business data.

THE CYBER SECURITY SKILL GAP IN THE COUNTRY IS HIGH, ESPECIALLY IN THE MANUFACTURING INDUSTRY. HOW HAS THIS AFFECTED YOU OR THE INDUSTRY AT LARGE?

HOW DO YOU THINK THIS SHORTAGE CAN BE ADDRESSED?

In order to address the security skills gaps requires a multi-pronged attack, targeting users, ICT staff and infrastructure. It is known that people are the weakest link within the organisation and we have implemented user awareness trainings as a means of alleviating existing risks.

There is a dire need to train cyber security professionals even in your industry, especially since the manufacturing industry has been thought to attract low risk when it comes to cyber security?

Although Manufacturing industries threat level may be assumed to be lower compared to financial sectors, we strive to exceed the minimum Cyber security requirements offered by the governing bodies of the financial sectors. Industries cannot afford to be lax and should invest in employing strategies to minimize this risk

WHAT ARE SOME OF THE THINGS THAT HAPPENED IN THE PAST YEAR IN THE INDUSTRY THAT INDEED SUPPORT THIS VIEW?

With the cost of Cybercrime constantly increasing, industries should work to reduce the amount by ensuring their data is secured.

WHAT ARE YOUR EXPECTATIONS FOR 2019 WITH REGARDS TO CYBER SECURITY AWARENESS AND CLOSING THIS SKILL GAP?

A lot of companies are embracing use of Cybersecurity awareness programs and this is good in the long run. Embracing cyber security should be a basic necessity of our education system, and should be a strategy supported by industries and the governing bodies.

CYBER LAWS IN KENYA

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

COMPUTER MISUSE AND CYBERCRIMES ACT, 2018

Year Enacted: 16th May 2018

It has taken Kenya's ICT sector close to eight years to draft, review and approve the cyber security bill which was passed into law on 14th May 2018 by President Uhuru Kenyatta. This law represents great milestones for cybersecurity professionals within the country as follows:

- The law provides a framework for prosecuting cybercrime in Kenya.
- Standard Definition and Procedures: Whereas previously we did not have standard definition of what qualifies as cybercrime such as publishing of fake news, unauthorized interception, Cyber bullying, and unauthorized access. The cybercrime bill, provides a clear description of offences that qualify as cybercrimes and goes further to provide law with procedures that they need to follow during investigation of these crimes. It also gives the Kenya Judiciary a benchmark on how to treat different instances of cybercrime.
- Standard Penalties: The law defines penalties for cybercrime, the toughest being KES. 25 million fine or 20 years in jail for offences involving protected computer systems. Child pornography also carries a heavy fine of KES. 20 million or 25 years jail time.
- Mobile money fraud has been addressed.

CYBERCRIME BILL: FREEDOM OF SPEECH, PRIVACY VIOLATIONS, CENSORSHIP

Top concerns from the public with regards to this law was vagueness of terms particularly those that impact citizens data privacy and the possibility of leveraging this vagueness to eavesdrop on citizens. This matter is still being addressed by the High Court of Kenya.

Overall, the bill aims to boost security and Kenya'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.

ENFORCEMENT OF CYBERCRIME BILL

Implementation of any laws is the most strenuous work. Limited Technical skills is a key hindrance to effective implementation of these laws. Cybersecurity is a new field in Africa and even more so for the stakeholders involved in implementing the Cybersecurity bill. Law enforcement and judiciary will need advanced training and upskilling to bridge the skill gap and ensure that they can be able to implement the law.

See appendix for the detailed Cybercrime law penalties and Procedures.

DATA PROTECTION BILL, 2018

Have you ever wondered why you receive promotion texts from say Supermarket X yet you've never subscribed to it? Well, selling of personal data has become big business in Kenya, particularly all the phone number, Identification Numbers and email addresses that we leave at the front desk.

The bill aims to protect personal data of Kenyan citizens. It seeks to hold companies who collect, process or store personal data acquire the relevant permissions before they do so.

TOP ISSUES ADDRESSED

1. Right to protection of privacy
2. Collection of personal data
3. Quality of information
4. Rights of the data subject
5. Duty to notify
6. Data processing
7. Protection and security of personal data
8. Notification of security compromises
9. Access to data
10. Correction of information
11. Retention of information
12. Misuse of information
13. Commercial use of data
14. Use of unique identifiers
15. Interference with personal data

07

DID YOU KNOW?

THE HIGH COURT SUSPENDED SECTIONS OF THE CYBERCRIME LAW. THIS WAS AFTER COMPLAINS FROM VARIOUS STAKEHOLDERS, MAINLY BLOGGERS, WHO DISPUTED THAT THE LAW CONTAINS PROVISIONS WHICH DENY, INFRINGE AND THREATEN FREEDOM OF EXPRESSION, RIGHT TO PRIVACY.

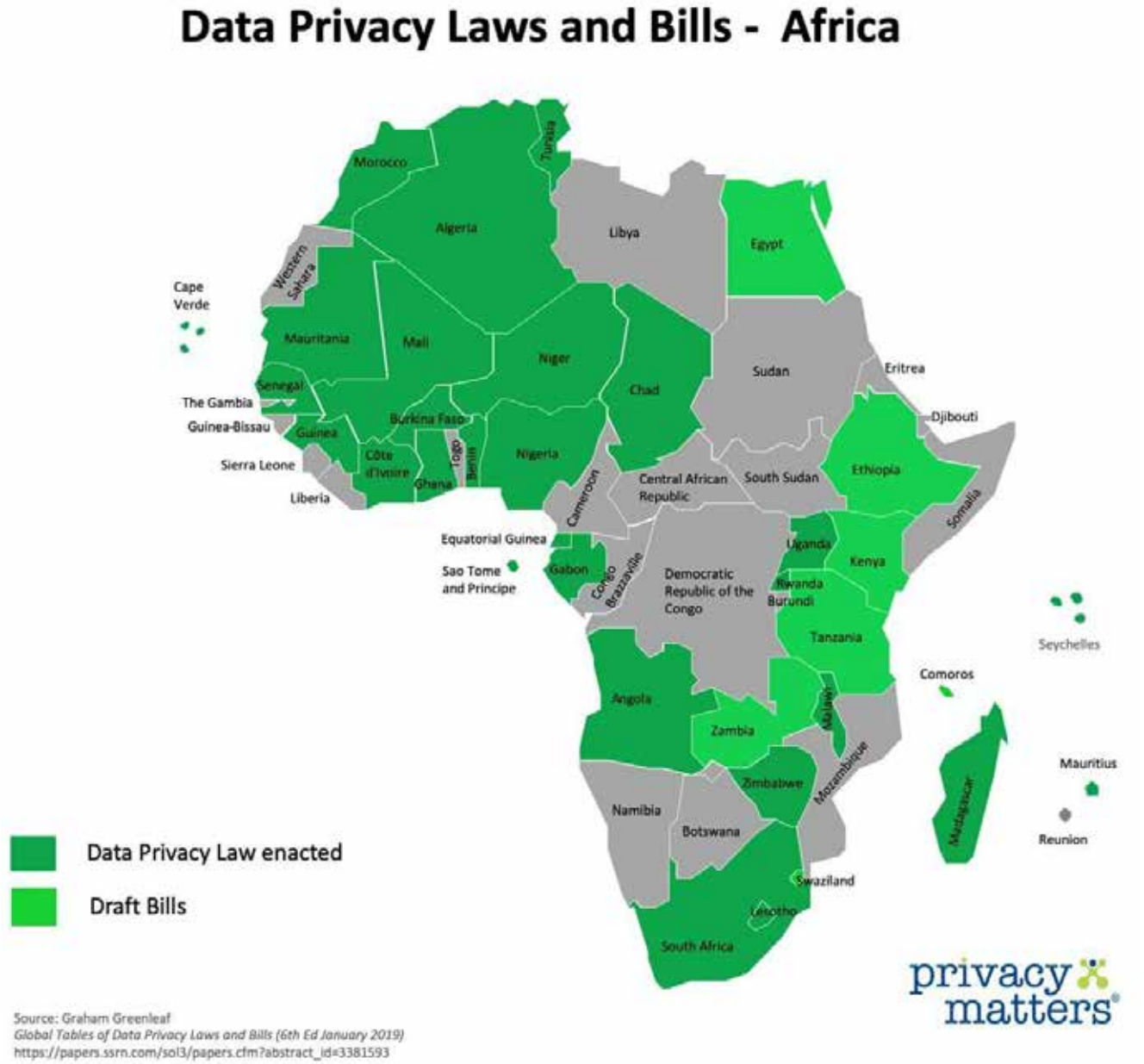
NATION MEDIA ARTICLE BY MAUREEN KAKAH

INDUSTRY SPECIFIC REGULATIONS

Industry Specific Laws	Year Enacted	Top Areas Covered
SASRA Guidelines on Cyber Security Risk Management	2018	These guidelines set the minimum standards that DTS' should adopt to develop effective Cybersecurity governance and risk management frameworks.
CBK Guidance Note on Cybersecurity	August 2017	• Governance – Roles of the Board of Directors, Senior Management and CISO • Role of Internal Auditors • Role of Risk Management Function • Role of External Auditors • Outsourcing • Training/Awareness • Reporting of cyber security incidents

Guidelines on Cybersecurity for Payment Service Providers	Draft – August 2018	• Categories of Payment Service Providers
		• Governance of PSPs
		• General Risk Management Requirements for PSPs
		• Dependency Risk Management Strategies & Cyber Resilience
		  ▪ Internal Dependency Management
		  ▪ External Dependency Management
		  ▪ Incident Response and Cyber Resilience
		• Regular Independent Assessment and Testing
		  ▪ Role of Risk Management Function
		  ▪ Role of Internal Audit function
		  ▪ Role of External Auditors
		• Outsourcing
		• Training/Awareness
		• Reporting of Cybersecurity incident

Sacco Societies Regulatory Authority Guideline on Risk Management Practices For Deposit-Taking Sacco Societies	June, 2015	• Overview of Risk Management Framework Requirements • Strategic Risk Management • Credit Risk Management • Operational Risk Management • Information and Communication Technology Risk Management • Liquidity Risk Management • Market Risk Management • Compliance Risk Management



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

INDUSTRY PLAYER PERSPECTIVE

VICTOR KOPIYO

Partner, Advocate, Lawmark Partners LLP

KENYA'S POLICY AND LEGISLATIVE FRAMEWORK FOR CYBERSECURITY

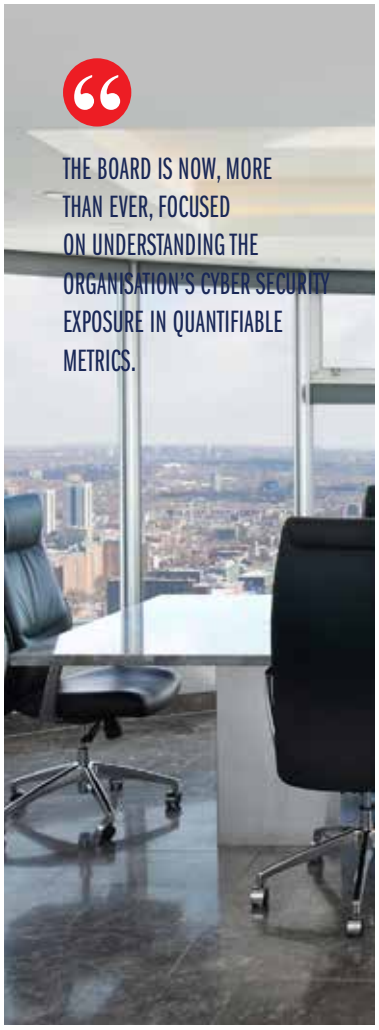
Kenya is yet to embrace an enabling policy and legal framework for cybersecurity. The current ICT Policy was adopted in 2006, while the sector law, the Kenya Information and Communications Act was enacted in 2009. Whereas the government has made significant strides in developing new policies and legislation, its disjointed approach towards cybersecurity remains of concern.

For example, the draft ICT Policy developed in 2016 is yet to be adopted. The Senate and the Ministry of ICT are working at cross-purposes by developing similar bills on privacy data protection. Further, despite the enactment of the Computer and Cybercrimes Act, 2018, the constitutionality of its provisions has been challenged in court for violating human rights. Moreover, key policies such as the ICT Master plan, 2014 - 2017 and the National Cybersecurity Strategy 2014, have suffered poor implementation and remain in dire need of review.

As the country embraces digital technologies, cybersecurity concerns and challenges have become mainstream, and therefore call for responsive policy and legislative frameworks. The confidence and integrity of information systems will be strengthened not just by technology, but by robust laws, policies and strategies developed, coordinated and implemented through multistakeholder approaches.

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 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.

INCREASE IN REGULATORY REQUIREMENTS

Stricter enforcement has already begun in Kenya with the enactment of Cybercrimes bill, SASRA cyber risk guidelines and CBK guidelines. We anticipate that regulators will become stricter with enforcement of the regulations in 2019.

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 Kenya, 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.

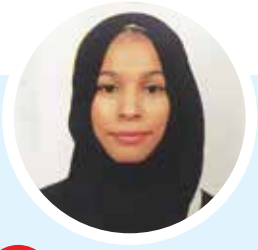
As we embark on strengthening our Cyber resilience, it is critical that we identify what's priority. Below are key questions you need to answer going forward.

- 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.



INDUSTRY PLAYER PERSPECTIVE

NABIHAH RISHAD

Senior 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, Kenya 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, Kenya 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.

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

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?

CBK GUIDANCE NOTE ON 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.**

Risk

- Technology
- Processes
- People

Controls

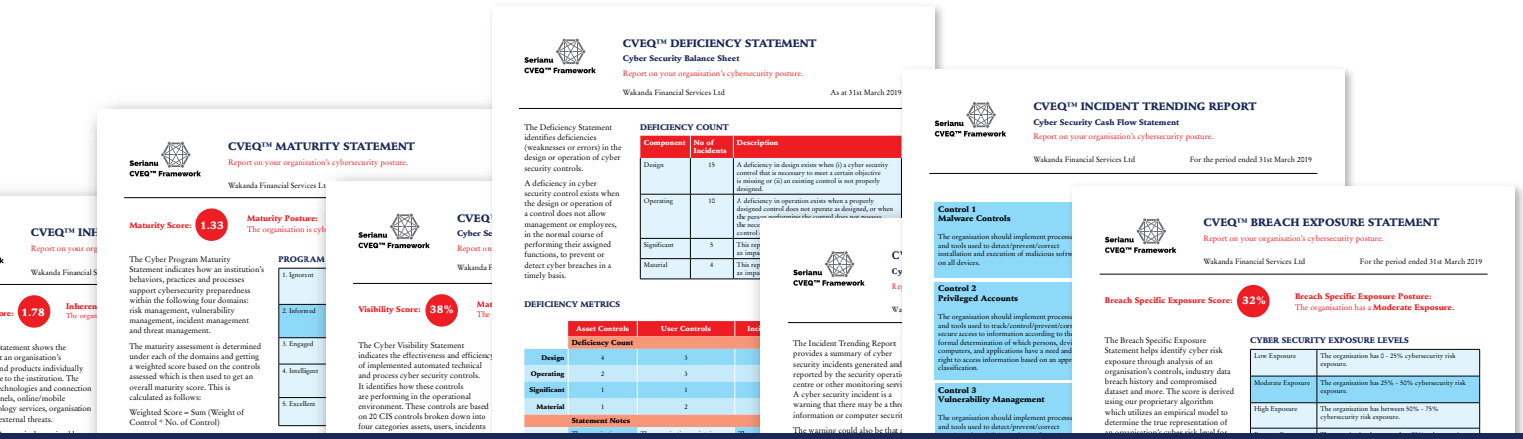
- Risk Management (Anticipate Risks)
- Incident Management (Respond to Incidents)
- Vulnerability Management (Detect Vulnerabilities)
- Threat Management (Contain Threats)

Visibility

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

Exposure

Fraud	IP Theft	Sabotage
Email Based Fraud	Data Breach	DDOS
Online Fraud	Counterfeit	System Outage
Wire Transfer	Domain Theft	Data Hijacking
Mobile Fraud	Unauthorized Disclosure	Data Manipulation



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.

APPENDIX

PENALTIES

Crime	Penalty In Cash	Penalty In Jail
Unauthorized Access To Computer Data	500,000	3 years
Unauthorized Modification Of Computer Data	200,000	2 years
Damaging or Denying Access To Computer Systems	5,000,000	3 years
Unauthorized Disclosure Of Access Code	250,000	3 years
System Interference	250,000	3 years
Illegal Devices	1,000,000	3 years
Unauthorized Receiving Or Giving Access To A Computer Program Or Data	500,000	2 years
Computer Forgery	10,000,000	10 years
Computer Fraud	5,000,000	10 years
Unauthorized Access To Protected System	1,000,000	5 years
Child Pornography	20,000,000	25 years
Hate Speech	1,000,000	5 years
Cybersquatting	500,000	5 years
Cyberstalking	300,000	5 years
Phishing	5,000,000	7 years
Spamming	500,000	3 years
False Publication	5,000,000	2 years

PROCEDURES AND INVESTIGATIONS

Powers of Access, Search and Seizure	The court may issue a warrant authorizing a police officer or lawful authority, to enter any premises to access, search and seize the thing or computer data.
Preservation Order	Lawful authority may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system.
Expedited Preservation	lawful authority is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the police officer may, by written notice given to a person in control of the data, require the person to ensure that the data specified in the notice be preserved for a period of up to ninety (90) days as specified in the notice.
Disclosure of Data	A police officer or lawful authority may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of all preserved or specified data stored or processed by means of a computer system.
Production Order	Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, a police officer or lawful authority may apply to court.
Collection of Traffic Data	If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the court may order a person in control of such data to collect or record traffic data.

Interception of Traffic Data	If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath, that there are reasonable grounds that traffic data is reasonably required for the purposes of a criminal investigation, the court may authorize a police officer or lawful authority to collect or record traffic data.
Obligation To Report Data Loss	All public or private corporations processing personal data shall as soon as practicable report any security breaches resulting in theft, loss or misuse of data to the police.
Interception of Content Data	If a court is satisfied on the basis of an application by a police officer or lawful authority supported by information on oath that there are reasonable grounds to believe that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the court may order a service provider whose service is available in Kenya through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data.
Forensic Tools	If a court is satisfied on the basis of an application by a police officer or lawful authority, supported by information on oath that in a criminal investigation concerning an offence under this Act, there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments and is reasonably required for the purposes of a criminal investigation, the court may authorize the police officer or lawful authority to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence
Duty To Cooperate	A person who is required to cooperate with police or lawful authority
Jurisdiction	The Kenyan courts shall have jurisdiction

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 Kenya. 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