

2017/2018



Africa Cyber Security Report - Lesotho



Cyber Security Skills Gap

2017/2018



Africa Cyber Security Report - Lesotho



**Cyber Security
Skills Gap**



“

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





IN THIS REPORT

07	Editor's Note and Acknowledgement	54	Cyber Intelligence
11	Foreword	60	Information Sharing Gap
14	Top Trends for 2018	66	Cybercrime and Cybercrime Bill, Lesotho
20	Survey Analysis	67	Top Priorities for 2018
32	Cost of Cybercrime	70	Fraud Exposures
36	Cyber Security Skills Gap	72	Cyber Visibility and Exposure Quantification (CVEQ™) Framework
43	The Gender Gap	74	References
46	State of Cyber Insurance in Africa		
47	Skills Mismatch		
50	Africa Cyber Immersion Club		





EDITOR'S NOTE AND ACKNOWLEDGEMENT

We are extremely pleased to publish the 1st Edition of Lesotho Cyber Security Report. This report contains content from a variety of sources and covers highly critical topics in cyber intelligence, cyber security trends, industry risk ranking and Cyber security skills gap. Over the last 6 years, we have consistently strived to demystify the state of Cyber security in Africa. In this edition themed Africa's Cyber Security Skills Gap, we take a deeper look at the limited technical skills, and financial limitations impacting many Lesotho organisations. Our research is broken down into the following key areas:

Top Trends: We analysed incidents that occurred in 2017/2018 and compiled a list of top trends that had a huge impact on the economic and social well-being of organisations and Lesotho citizens. This section provides an in-depth analysis of these trends.

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

Survey Analysis: This section analyses the responses we received from Africa and 60 organisations in Lesotho. It measures the challenges facing Lesotho organisations, including low Cyber security budgets and inadequate security impact awareness that eventually translates to limited capabilities to anticipate, detect, respond and contain threats.

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

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

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

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

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



Brencil Kaimba

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

2015 
Achieving Enterprise Cyber-resilience
Through Situational Awareness

\$3tn Cost of cybercrime



Achieving Cyber Security Resilience:
Enhancing Visibility and Increasing
Awareness

\$2b Estimated Cost of
Cybercrime in Africa



Demystifying African's Cyber
Security Poverty Line

\$3.5b Estimated Cost of
Cybercrime in Africa



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 2017/2018 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 2017/2018 - Lesotho Edition, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;



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



PKF Lesotho has been a key research partner. They provided immense support through distribution of surveys, collection of key statistics, survey responses, local intelligence on top issues and trends highlighted in the report were as a result of our interaction.



The Serianu CyberThreat Intelligence Team

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

CO-AUTHORS

Barbara Munyendo - Researcher, Cyber Intelligence
Margaret Ndungu - Researcher and Editor
Nabihah Rishad - Researcher, Framework
Salome Njoki - Researcher, Trends
Brilliant Grant - Researcher, Trends
Ayub Mwangi - Data Analyst

Collins Mwangi - Data Analyst
Daniel Kabucho - Data Analyst
David Ochieng' - Data Analyst
Joseph Gitonga - Data Analyst
Sheila Nyambura - Data Analyst
Vionna Muriithi - Data Analyst

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

Sunday Adache
Managing Partner, PKF Lesotho

International Data Corporation (IDC)

Joseph Mathenge
COO, Serianu Limited

Lerato Mphaka
MMI, Metropolitan

Molupe Molupe
ICT Manager, Lesotho Communications Authority

Makhele Molefe
Senior Systems Support Officer, National Manpower Secretariat

Lands Administration Authority

U. Ebisoh
Linkonkwin University, Maseru

Mamthe Nema
Boliba Savings and Credit

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 Lesotho.

Our new Serianu CyberThreat Command Centre (SC³) 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

Copyright © Serianu Limited, 2018

All rights reserved



FOREWORD

Welcome to the 1st edition of the Lesotho Cyber Security Report, with this inaugural report we tackle key themes that capture the challenges the industry face and what needs to be addressed to make progress in safeguarding the nation.

The Cyber-threat landscape in Lesotho is evolving fast and the looming cybersecurity skills gap has become an industry crisis. Organisations in Lesotho have little to no capacity to match the massive losses being recorded across all tiers of the economy, efforts to close the skills gap should be collaborative and intentional.

Lesotho is blessed with a youthful and highly educated population. Training our youth on cyber security skill presents a very viable opportunity to resolving the youth unemployment while at the same time securing the country.

Lesotho can take advantage of its youthful population to build a strong cyber security workforce and become a global player in the cyber security space. The formal education curriculum will need to be updated to include cyber security training starting from the high school curriculum all the way to university level. Non formal education with private sector training and short duration certification programs should be explored to build a strong cyber security work force for the country.

This report highlights 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.



LESOTHO CAN TAKE ADVANTAGE OF ITS YOUTHFUL POPULATION TO BUILD A STRONG CYBER SECURITY WORKFORCE AND BECOME A GLOBAL PLAYER IN THE CYBER SECURITY SPACE.

TRAINING OUR YOUTH ON CYBER SECURITY SKILL PRESENTS A VERY VIABLE OPPORTUNITY TO RESOLVING THE YOUTH UNEMPLOYMENT WHILE AT THE SAME TIME SECURING THE COUNTRY.

Sunday Adache
Managing Partner,
PKF Lesotho



EXECUTIVE SUMMARY

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 years.

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.



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.

William Makatiani
CEO, Serianu Limited

2018 HIGHLIGHTS

50 Cyber Security Skilled Professionals in Lesotho

Skills shortage at senior management and mid management levels

90% of Companies to face talent shortage of Cybersecurity professionals in 2019

Constraint when recruiting Cybersecurity professionals

- 1 Lack of solid experience / track record
- 2 Lack of certifications (i.e. CISSP, ITIL, etc.)

Increase in organisational spend in cybersecurity in 2017 to 2018

25% of respondents spend above \$10000

\$2M cost of cybercrime in Lesotho in 2018

99%

Cyber Crime cases go UNREPORTED OR UNRESOLVED


Increased Adoption of Cloud

Fake news is a growing concern in Lesotho


Increased Targeted Phishing Attacks

Increased involvement of Board members on cybersecurity matters



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, Ethereum etc. took Lesotho 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 Lesotho 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 Lesotho organisations. With the cost of cybercrime increasing every year across Lesotho, 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 Lesotho - 50 it is clear that Lesotho businesses are an easy target for both local and international hackers. Some companies in Lesotho 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



50

Cyber Security Skilled
Professionals in
Lesotho



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

02

Our analysis also discovered that Lesotho 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.



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.

INSTANCE OF FAKE NEWS

1

In 2017, photos of children who got sick with measles symptoms shortly after being vaccinated by the government spread across various social media platforms. Health minister however labeled these to be propaganda antics employed only because Lesotho was headed for elections.

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

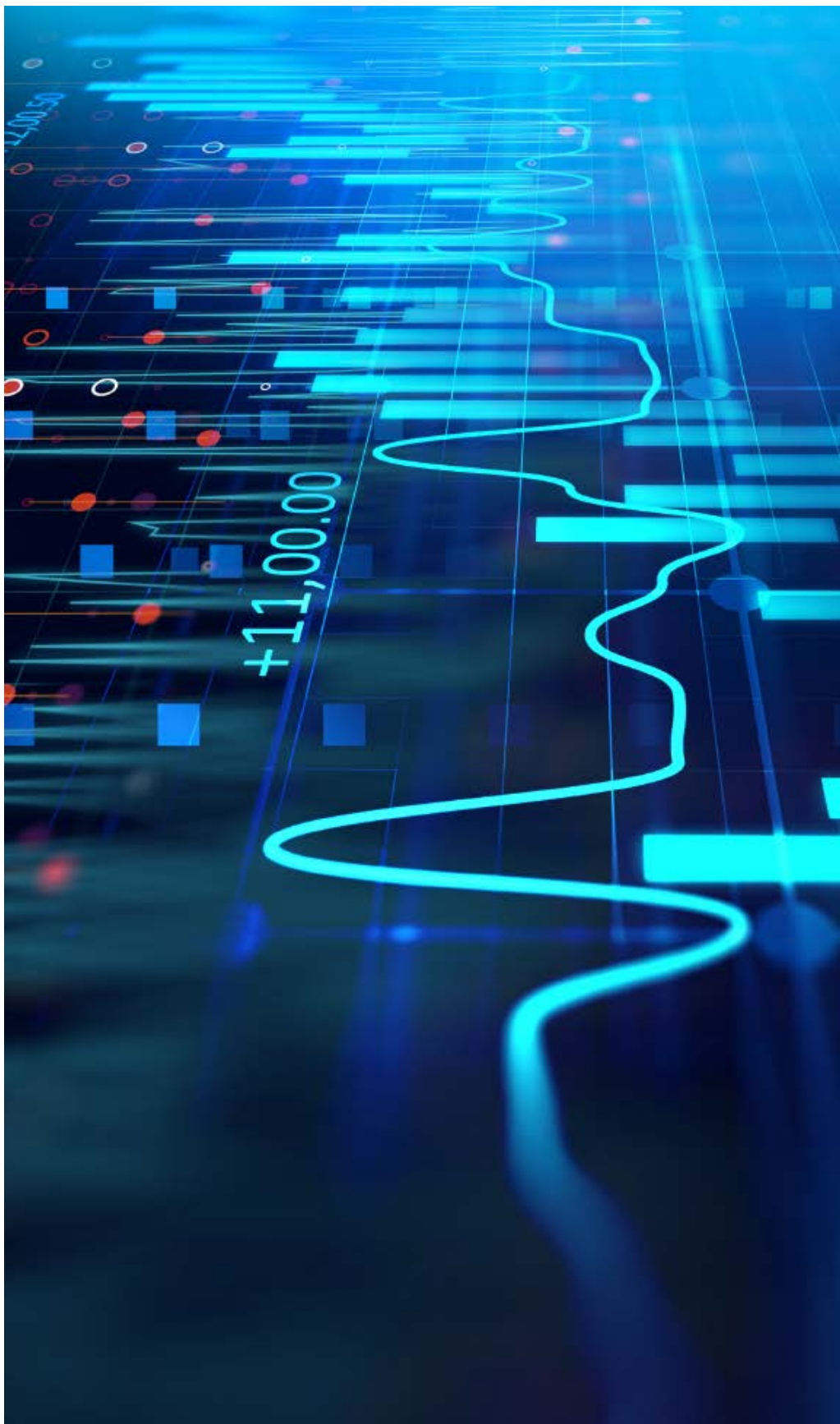
DID YOU KNOW?

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



"STUDIES HAVE SHOWN THAT OVER 90% OF THE MEDIA'S COVERAGE OF PRESIDENT TRUMP IS NEGATIVE." A DIRECT CONSEQUENCE OF FAKE NEWS





INDUSTRY PLAYER PERSPECTIVE

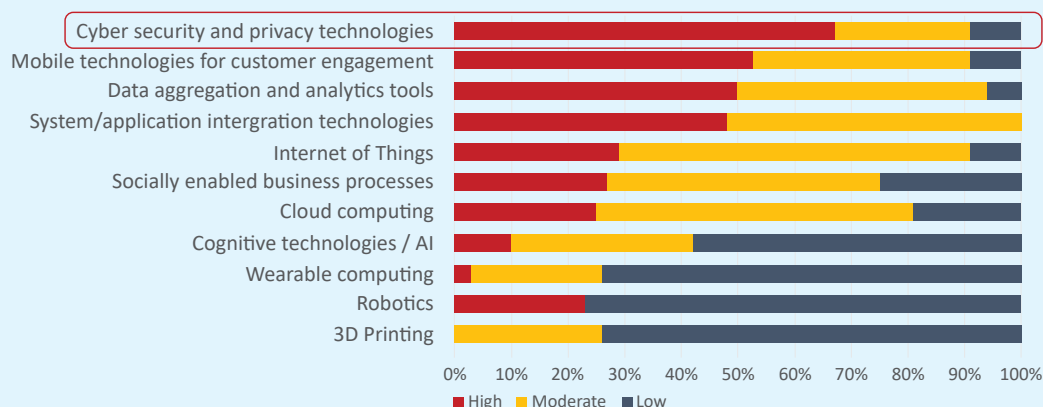


SUB SAHARAN AFRICA IT SECURITY LANDSCAPE AND TRENDS 2018-2019

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

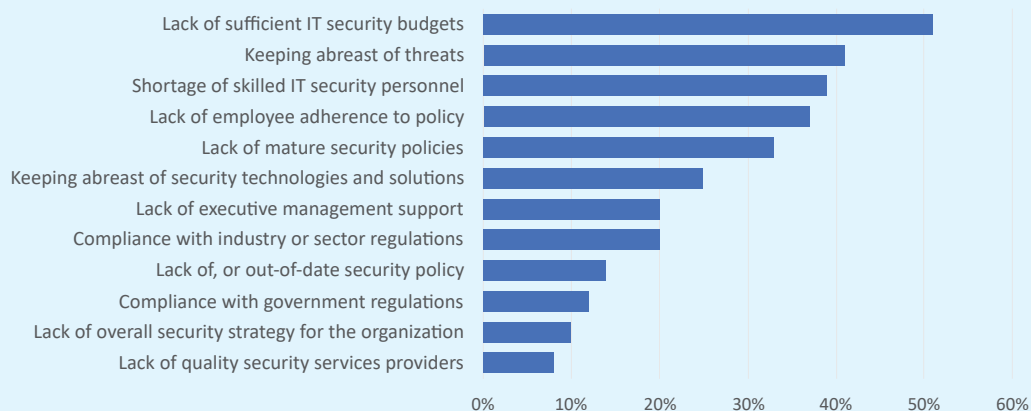
According to IDC's annual CIO Survey 2018, cyber security and privacy technologies rank the highest in importance for organisations looking at digital transformation.

Various Dx technologies are hotspots for (in) security:

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



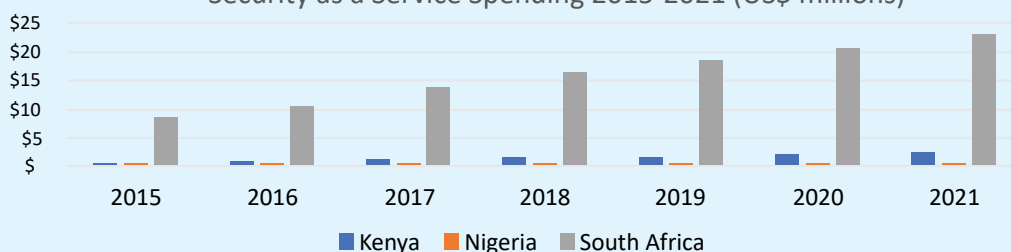
CHALLENGES IN MANAGING SECURITY



SOURCE 2: IDC

SECURITY AS A SERVICE SPENDING

Security as a Service Spending 2015-2021 (US\$ millions)



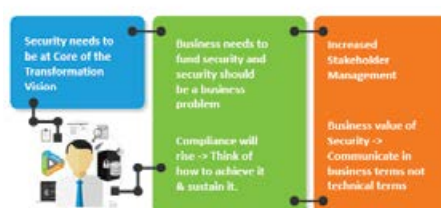
SOURCE 3: IDC

- Lesotho 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.

New Age CISO



Essential Guidance





IDC

ANALYZE
THE
FUTURE

ABOUT IDC

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

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

GIVEN
IDC'S
RESPECTED
STANDING

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

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

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





SURVEY ANALYSIS

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

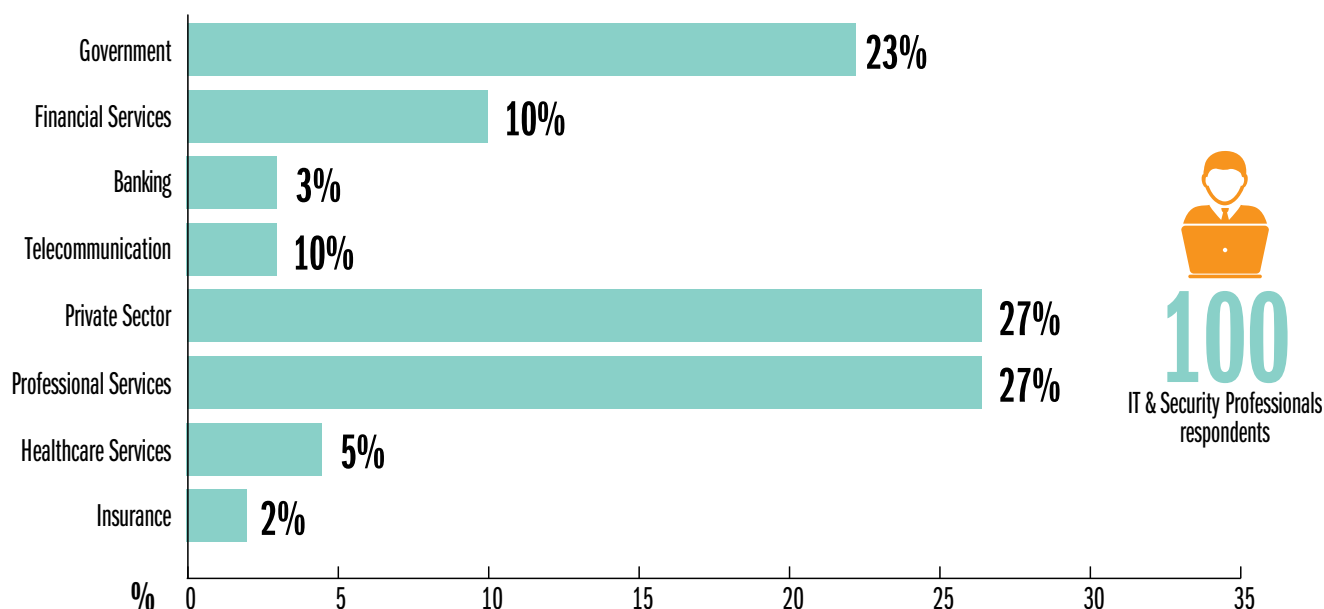
Based on the feedback from over 150 IT and security professionals, an analysis of the findings yielded a few notable themes, which are explored in greater detail in this report and highlights are summarized below:

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 Lesotho 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)?

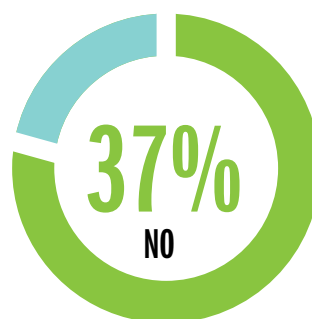
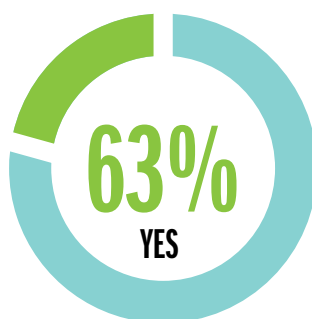
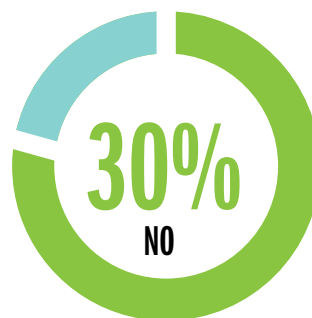
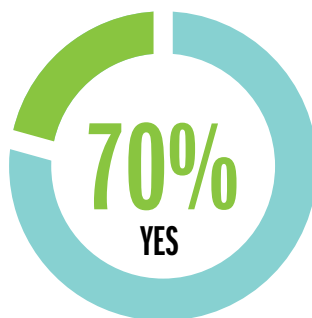


CHART 2: CLOUD SERVICES/ IOT USAGE.

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?

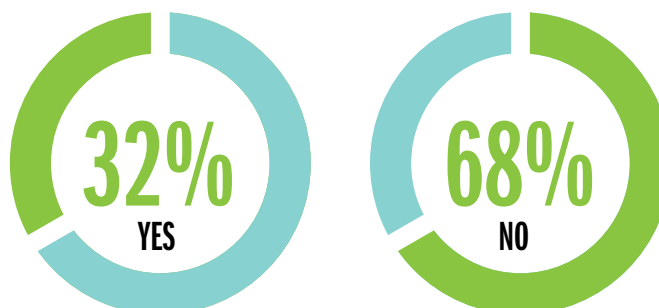
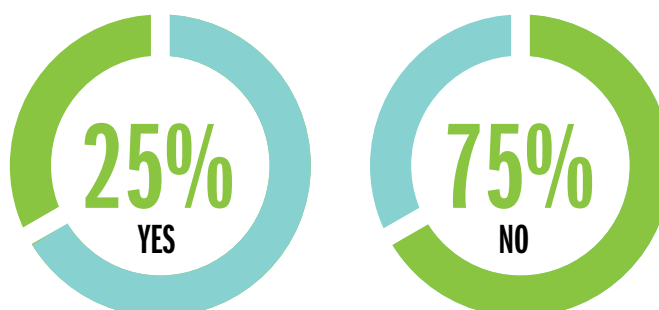


CHART 4: IOT AND CLOUD SERVICES BEST PRACTICE

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.



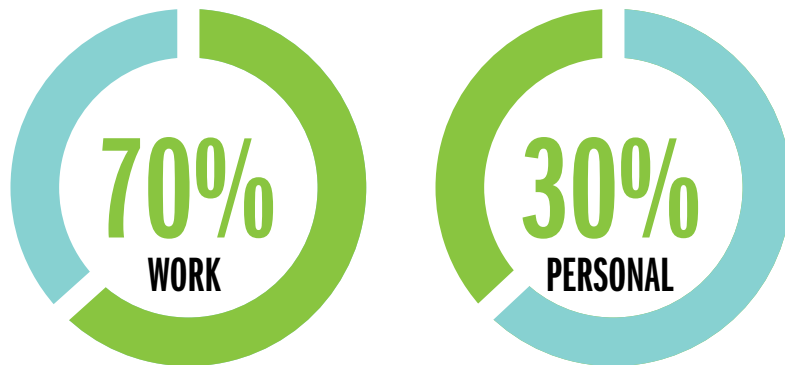
CYBER CRIME

The explosion of online fraud and cyber-crime affected almost 70% 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?



ON AVERAGE, ORGANISATIONS VICTIMIZED BY CEO FRAUD ATTACKS LOSE BETWEEN \$25,000 AND \$75,000.

FBI ALERT 2016

WHY YOU ARE A TARGET

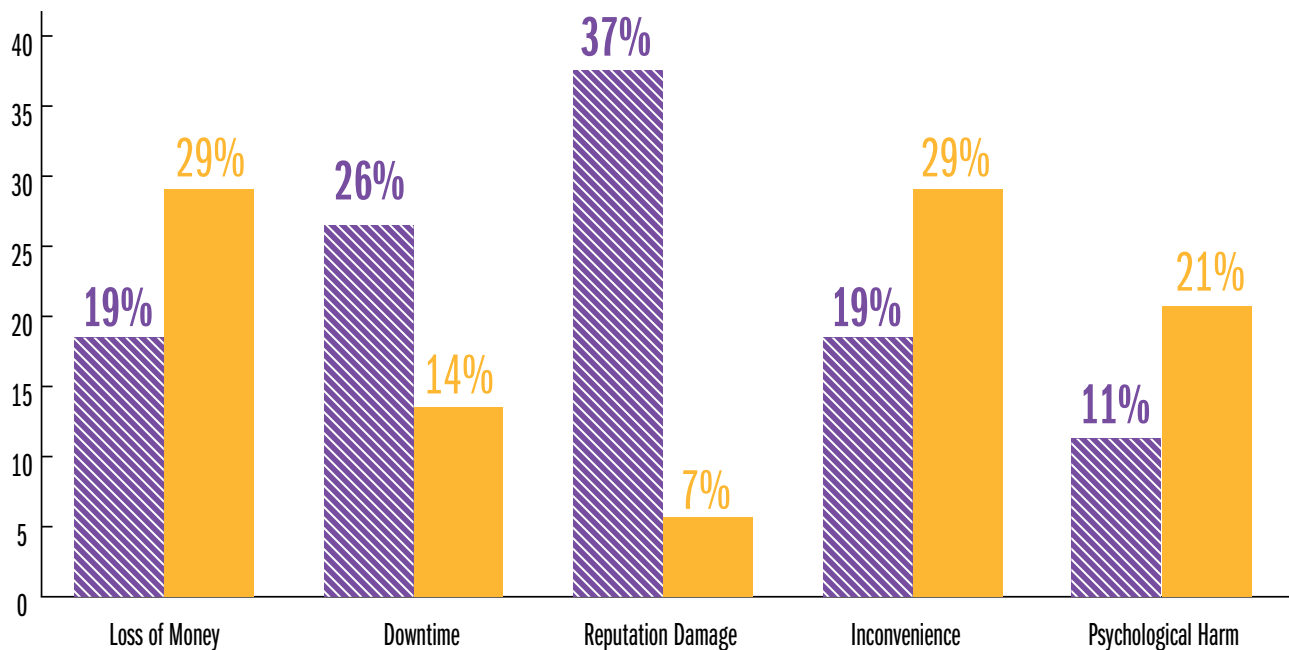
Who	Why	How
HR Managers	Have direct access to payroll systems and information	Social Engineering
Board	Have access to sensitive information such company strategy, bank approvals and audit reports	Phishing e-mails
System Administrators	Custodians of credentials to critical infrastructure	Use of Keyloggers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

 For corporate organizations  For individuals



GRAPH 2: IMPACTS OF CYBERCRIME: CORPORATE VS INDIVIDUALS.



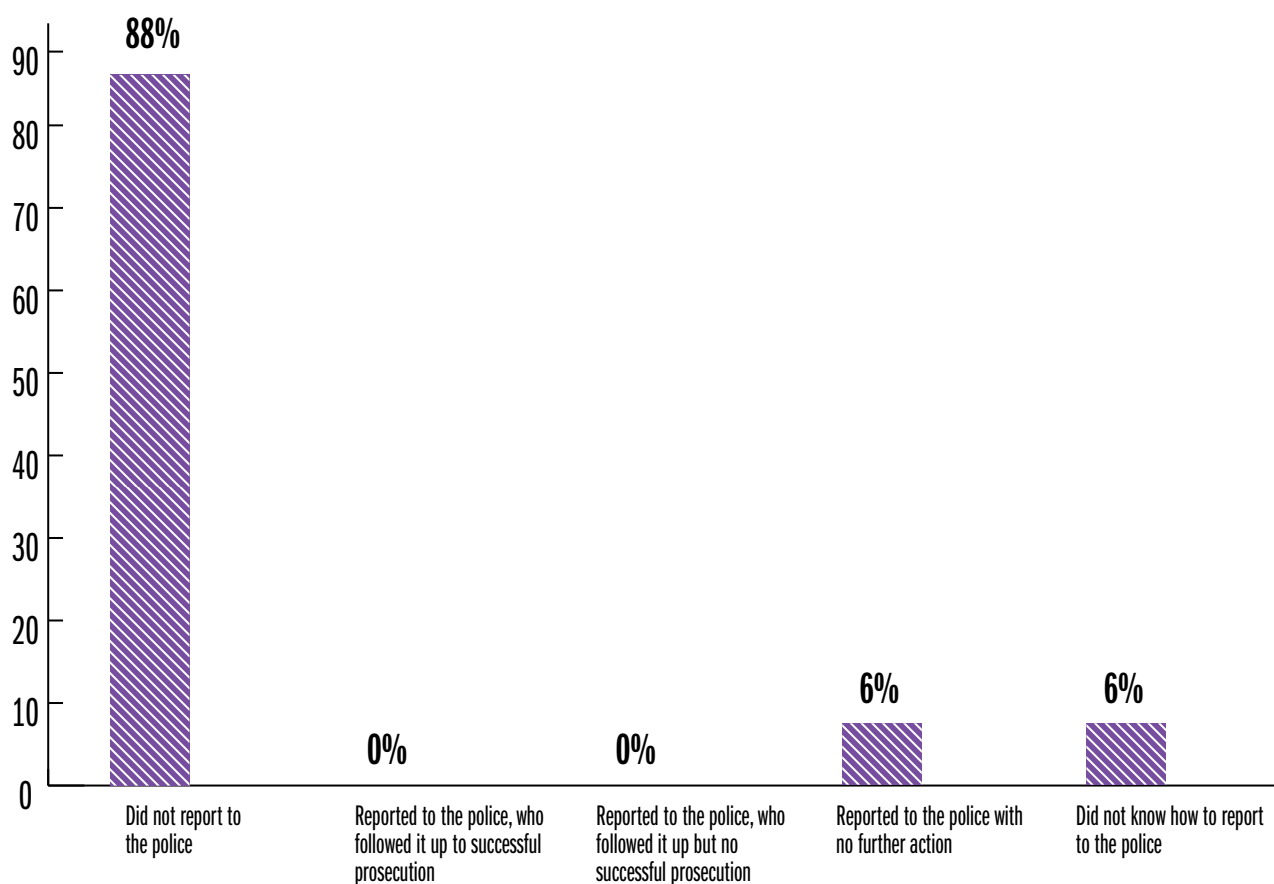
This presents one conclusion that majority of attacks in Africa are motivated by financial gain – suggesting reasons why financial institutions, Saccos and organisations that deal primarily with transaction processing are primary targets for the Cyber-attacks.



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 .

- Up to 94% of Cyber related cases either go unreported or unresolved.
- This can be attributed to the low awareness levels within the public and law enforcement.





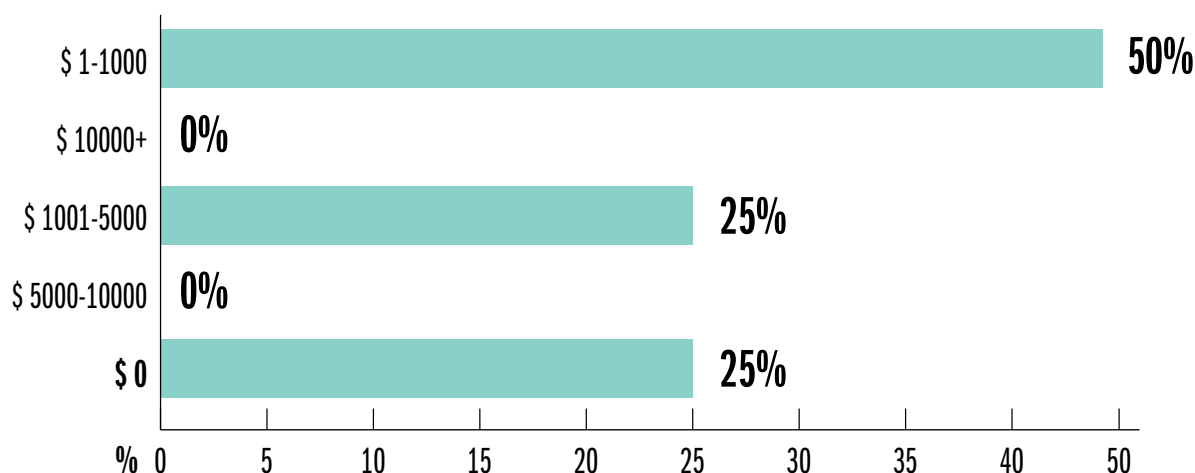
CYBER SECURITY SPENDING



Organisations are now investing more to achieve cybersecurity resilience. From our analysis in 2017/18, 99% of respondents invested less than \$5,000 on cyber security during the year.

Further analysis also revealed that majority of organisations which spend USD 5,000+ are from the Banking and Financial sectors.

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



GRAPH 4: CYBERSECURITY SPEND.

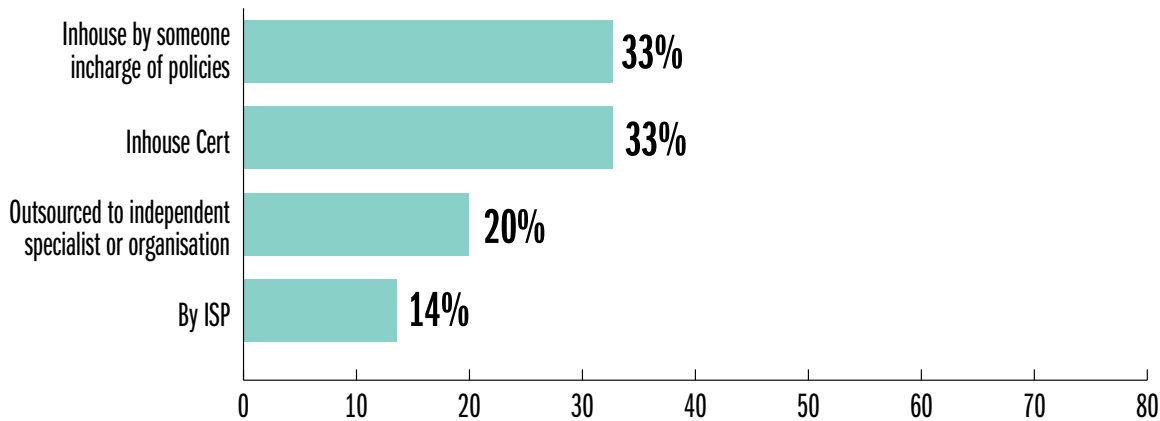


MANAGING CYBER SECURITY

66% of organisations manage their cyber security inhouse while 34% have outsourced 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?



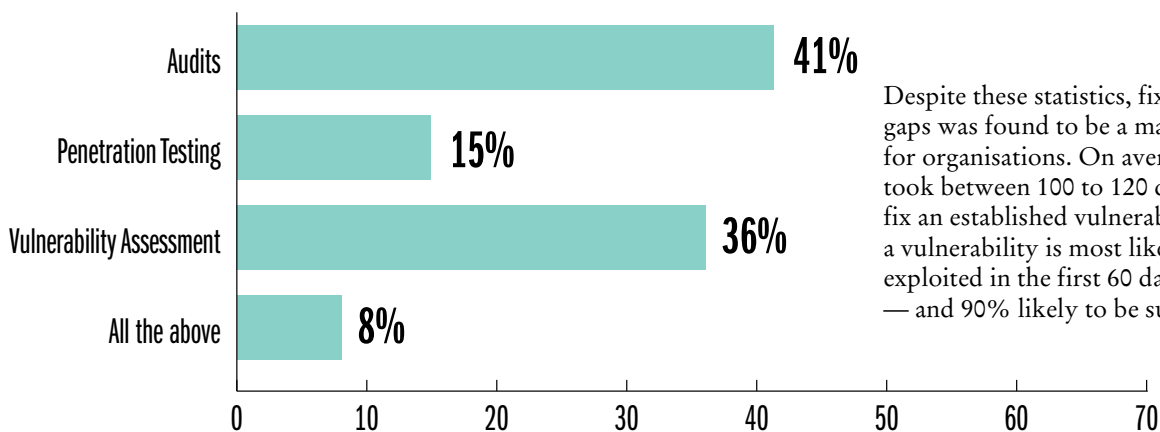
GRAPH 5: CYBERSECURITY MANAGEMENT.



CYBER SECURITY TESTING TECHNIQUES

Security testing is a process performed to reveal flaws in security mechanisms and find 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, 15% perform Penetration testing while 41% perform Audits and 36% perform Vulnerability assessments. . All these testing techniques are not independent and in fact work best when they are applied concurrently.

WHICH OF THE FOLLOWING SECURITY TESTING TECHNIQUES DOES YOUR 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.

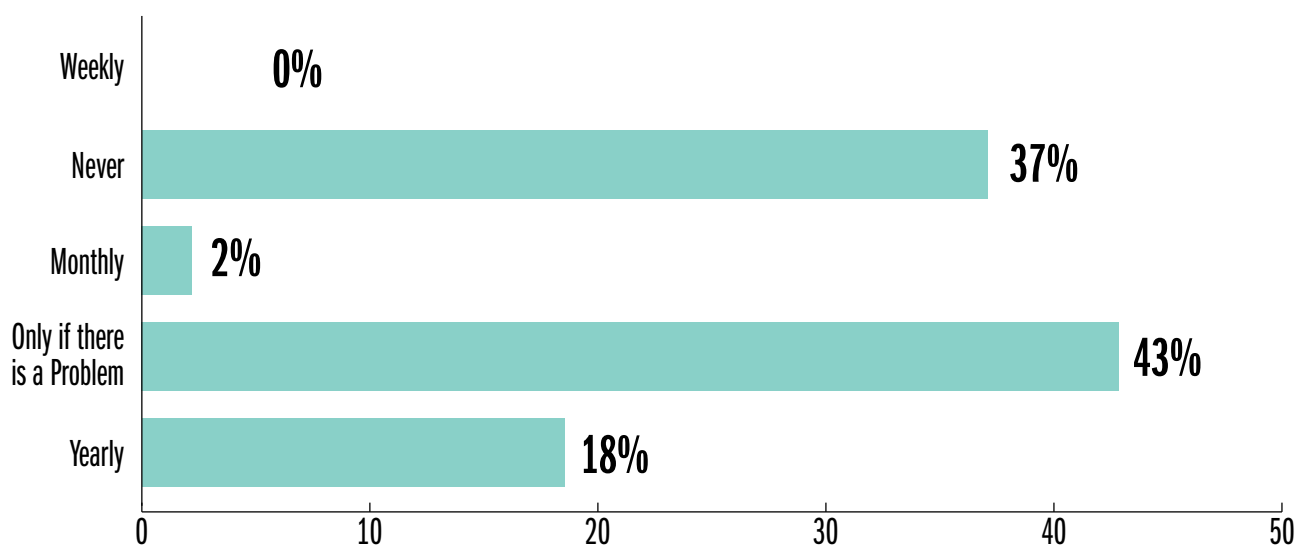
GRAPH 6: SECURITY TESTING TECHNIQUES.



CYBER SECURITY AWARENESS

The level of awareness in Lesotho is still low with 37% of organisations not having an established cyber security training program. Most organisations (43%) are also still very reactive when it comes to cyber security training, these organisations train their staff only when there is an incident/problem. This is worrying considering 50% of all cyber attacks reported in the survey was through work. On the other hand, it is important to point out that 20% of respondents reported to have a regular training program in place. The importance regular security training for employees cannot therefore 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

**SUNDAY ADACHE**

Managing Partner, PKF Lesotho

KINDLY HIGHLIGHT SOME OF THE TOP CYBER SECURITY ISSUES OF 2017 AND HOW THESE ISSUES IMPACTED YOU PERSONALLY, YOUR ORGANIZATION OR COUNTRY?

The most prevalent cyberattack known to me in Lesotho is email hacking, in most instances, when emails are hacked, the hackers use their victim's email to send fraudulent mails to the contacts of the victim. The fraudsters use it to send messages with intention to defraud. This has resulted in financial losses.

DO YOU THINK FAKE NEWS IS A MAJOR PROBLEM IN YOUR COUNTRY/AFRICA? IF YES, WHO SHOULD BE RESPONSIBLE FOR CONTROLLING THE CREATION AND DISTRIBUTION OF FAKE NEWS (GOVERNMENT, END USERS, TELCOS/ISPs OR CONTENT OWNERS)?

Fake news is a big problem as it induces people to act or react on a wrong premise. When people become vulnerable to fake news, they tend to doubt even true information. This destroys the positive essence of information on various issues. The dominant intentional generation of fake news usually intends to gain advantage, blackmailing of political opponents, business competition and even merely deriving joy in causing panic in the society.

SHOULD REGULATORS FORCE INFLUENTIAL PLATFORMS LIKE GOOGLE AND FACEBOOK TO REMOVE FAKE NEWS AND OTHER EXTREME FORMS OF CONTENT FROM THEIR PLATFORMS?

Yes, this is very essential and urgent if news through these platforms will maintain relevance. And most importantly, they should not allow these channels to be taken over and used for criminal activities.

WHAT CAN BE DONE TO IMPROVE THE GENERAL USER AWARENESS ON THE DETECTION OF FAKE NEWS IN THE COUNTRY?

The means of detecting fake news is through education on the characteristics of fake news. Secondly by publication to the general public of any fake news identified so that the society can be aware. It might also be helpful to create a communication channel for individuals to clear the authenticity of any information which they suspect might be fake.

MANY GOVERNMENTS IN AFRICA ARE INVESTING IN E-SERVICES (E-GOVERNMENT, E-VOTING, E-TAX SYSTEMS AND MANY OTHER PORTALS.) DO YOU THINK THE AFRICAN**CITIZENRY IS READY TO CONSUME AND UTILIZE THESE SYSTEMS WITHOUT THE WORRY OF PRIVACY, SECURITY AND FRAUD?**

The e-services investments are a necessity as it brings efficiency of service delivery. The migration to e-services is imperative in view of very poor service delivery by the average public servant across Africa. It is my opinion that e-services complements efforts by governments to combat fraud, security challenges since the world over has shifted to information technology applications and it is not possible for Africa to operate in isolation.

However, African governments need to invest in education and improvement in standards of living before the e-services investment can offer optimum results.

WHAT ARE SOME OF THE RISKS WE FACE WITH THE INTRODUCTION OF GOVERNMENT DRIVEN E-SERVICES AND DO YOU HAVE ANY EXAMPLES OF THESE CASES IN YOUR COUNTRY?

With introduction of government e-services we might be faced with declining quality of service delivery. An instance in our country relates to company registration and on-line visa application. We have had instances of delays without an opportunity to contact someone for follow up. It is a dilemma when applications are submitted and there is no response without having a channel of obtaining an update. Also, with the level of internet resource reliability, it might be an irrecoverable disaster in the event of a system crash. Disaster recovery and backups are not reliable in some of the systems.

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

I am not aware of such attacks in Lesotho.

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

CONSIDERING THE SHORTAGE OF SKILLED RESOURCES IN AFRICA, HOW CAN WE LIMIT THE IMPACT OF RANSOMWARE CASES?

The best strategy for Africa is education and more professional practice development.

DO YOU THINK ORGANIZATIONS ARE SPENDING ENOUGH MONEY ON COMBATING CYBER-CRIME?

In Lesotho, organizations are not spending and are not ready to spend money on combating cyber-crime. May be due to limited attack incidences in Lesotho.

WHAT CAN BE DONE TO ENCOURAGE MORE SPENDING ON CYBER SECURITY ISSUES?

Creating more awareness on cyber-risks, the government setting up opportunities and creation of enhanced internet services.

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

IN YOUR OPINION, WHAT SHOULD AFRICAN COUNTRIES/ UNIVERSITIES FOCUS ON TO ENCOURAGE INNOVATION IN THE DEVELOPMENT OF CYBER SECURITY SOLUTIONS?

General enhancement of studies in innovation, creation of an enabling environment which should include funding of research and development, refund of research and development costs for successful innovative discoveries, granting of tax incentive for R&D projects, licensing of intellectual property and funding commercialization of successful inventions.

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

Consumers and professionals should be motivated to patronize local products. The government could also subsidize the local products.

IN YOUR OPINION AND FROM AN AFRICAN CONTEXT, WHAT ARE THE TOP 2018 CYBER SECURITY PRIORITIES FOR AFRICAN COUNTRIES AND ORGANIZATIONS?

- Initiation of a cybersecurity continental body;
- Regulation of the industry
- Giving legislative mandate for minimum industry standards.
- Improvement of inter-continental connectivity
- Reduction in internet costs etc.



INDUSTRY PLAYER PERSPECTIVE

JOSEPH MATHENGE

Chief Operations Officer, Serianu Limited

ADDRESSING CYBER SECURITY SKILLS GAP
IN THE ENTERPRISE ENVIRONMENT

“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. 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 IN LESOTHO

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.



\$2m

estimated cost
of cybercrime



Direct Cost

\$0.6m



Indirect Costs

\$1.4m

MOST AFFECTED INDUSTRIES

1



Banking

2



Public Sector

3



Microfinance

4



Hospitality
and Retail

5



Others



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)	436,270.00	<ul style="list-style-type: none"> • SIEM • Network Access Controls • IPS/IDS 	<ul style="list-style-type: none"> • Penetration Testing • Audit • Forensic Investigations 	<ul style="list-style-type: none"> • General Awareness Training • Technical Training
Government and Public Sector (Utilities)	404,400.00	<ul style="list-style-type: none"> • Active Directory • Vulnerability Management 	<ul style="list-style-type: none"> • Risk Assessment • Compliance Review 	<ul style="list-style-type: none"> • Board Training • Business Managers
Service Providers (Telcos, Fin-tech, and Financial apps)	325,430.00	<ul style="list-style-type: none"> • Solutions • PAM • Antivirus 	<ul style="list-style-type: none"> • Post-Implementation • Review 	<ul style="list-style-type: none"> • Training
Manufacturing, Healthcare, Hospitality and Retail	47,460.00	<ul style="list-style-type: none"> • HIDS • Proxy • WAF 	<ul style="list-style-type: none"> • BCP/DR Testing and • Review 	
Others	186,440.00	<ul style="list-style-type: none"> • Load Balancer 		

Total Indirect Cost is \$1.4m

DIRECT COSTS	Estimated Direct Cost (USD)	Activities
Financial Services (Banking, Insurance, Saccos and MFI)	189,830.00	<ul style="list-style-type: none"> • Data Hijacking (ransomware attack)
Government and Public Sector (Utilities)	172,880.00	<ul style="list-style-type: none"> • Money Lost
Service Providers (Telcos, Fin-tech, Betting, Financial apps)	135,600.00	<ul style="list-style-type: none"> • Fines from Regulators • Law Suits
Manufacturing, Healthcare, Hospitality and Retail	20,340.00	<ul style="list-style-type: none"> • Claims and Cyber Insurance
Others	81,350.00	<ul style="list-style-type: none"> • Forensic Investigations

Direct Costs is \$0.6m



INDUSTRY PLAYER PERSPECTIVE



LERATO MPHAKA

MMI, Metropolitan

KINDLY HIGHLIGHT SOME OF THE TOP CYBER SECURITY ISSUES OF 2017 AND HOW THESE ISSUES IMPACTED YOU PERSONALLY, YOUR ORGANISATION OR COUNTRY?

a. High Impact Cyberattacks:

On May 12, 2017, the world was stunned by an unprecedented global ransomware attack dubbed WannaCry that infected more than 200,000 computers in 150-plus countries. This attack severely impacted the UK, but the ripple effects were felt especially worldwide. The MMI group ITIL policy had to be reviewed in answer to the sudden risk as well as user training interventions to combat Phishing campaigns.

b. Wikileaks CIA Vault 7:

On March 7, WikiLeaks published a data trove containing 8,761 documents allegedly stolen from the CIA that contained extensive documentation of alleged spying operations and hacking tools. Revelations included iOS and Android vulnerabilities, bugs in Windows, and the ability to turn some smart TVs into listening devices. The effects of this while felt in America, shed light on the weaknesses in core operating systems and may have spurred Microsoft's aggressive shift to Windows 10 and system fixes using patches. This unfortunately has translated into increasing bandwidth usage, leading to slower business system responses for country operations.

c. Makhaola Qalo Government Leaks:

Similar to the emails that were hailed as the ones that created the loss of Hillary Clinton's presidency in the USA, Lesotho had a similar data breach over the internet. A Facebook user account Makhaola Qalo was responsible for the spreading of Government of Lesotho classified information which we are not sure ended in this country. Similarly in 2018, it was found that suggestive mass manipulation (Cambridge Analytica saga) could be responsible for the victory and subsequent presidency of the 45th President of the USA.

d. Data Fraud From Within:

As an insurance firm, there is always a risk of internal system breaches in the spirit of committing fraud. 2017 was no exception as the company was among those targeted by fake identity documents that were stolen and reproduced from Home Affairs.

DO YOU THINK FAKE NEWS IS A MAJOR PROBLEM IN YOUR COUNTRY/AFRICA? · IF YES, WHO SHOULD BE RESPONSIBLE FOR CONTROLLING THE CREATION AND DISTRIBUTION OF FAKE NEWS (GOVERNMENT, END USERS, TELCOS/ISPS OR CONTENT OWNERS)?

Fake news is an increasing problem in Lesotho and the rest of Africa. Fake news is normally promulgated during electoral campaigns to sway the opinion of the masses. Unfortunately, a post on a social media platform is not peer reviewed and cannot be verified as true or false upon posting. It becomes an incredible feat for providers of the internet or devices that use data to regulate the spread of fake news especially on free versions of social media platforms.

What giants like Facebook are doing is to create subscription based services (e.g. a subscribed Facebook) where the quality of content by virtue of a small user base can be verified. This is obviously done at the risk of curbing the growing internet usage rates in Africa, which from 2000-2017 have grown a collective 9,942%. Lesotho has achieved a 15,596% usage growth.

<https://www.internetworldstats.com/stats1.htm>

The onus still remains of content owners to spread the right messages. Recognition and notoriety (such as social media influencers) can be given to persons who post responsible content aimed at debate and not slander.

SHOULD REGULATORS FORCE INFLUENTIAL PLATFORMS LIKE GOOGLE AND FACEBOOK TO REMOVE FAKE NEWS AND OTHER EXTREME FORMS OF CONTENT FROM THEIR PLATFORMS?

No regulators should not for or regulate social media platforms. The task is an ominous one but also borders dangerously on the infringement of our constitutional rights of freedom of speech, expression and association. It is the media platforms themselves that can allow users to filter the type of news they wish to see. This will curb to a degree the spread of fake news, but also spur holders of information to disclose previously private records, to the benefit of the masses. Facebook can put in cues that allow users to flag posts that may be harmful

WHAT CAN BE DONE TO IMPROVE THE GENERAL USER AWARENESS ON THE DETECTION OF FAKE NEWS IN THE COUNTRY?

Fake news can only be detected in the presence of the "real" version of events. This goes against a culture of Basotho where incidents are hardly made public knowledge. We also need to determine who the subject matter experts are and allow those to gain a following big enough to create influence. Councils of peers can be set up to review the information shared, and publish reviewed and accurate accounts of events. It is a lot of work to set up, but if practiced and adhered to can create a healthy balance of fact against the easier spread fiction.

MANY GOVERNMENTS IN AFRICA ARE INVESTING IN E-SERVICES (E-GOVERNMENT, E-VOTING, E-TAX SYSTEMS AND MANY OTHER PORTALS.) DO YOU THINK THE AFRICAN CITIZENRY IS READY TO CONSUME AND UTILIZE THESE SYSTEMS WITHOUT THE WORRY OF PRIVACY, SECURITY AND FRAUD?

Data privacy and security is a worry in Africa and needs to be looked into before e-based services can be bolted onto current citizenry services. Security and the ability of Governments to show the capability to secure citizen data has been shown to be one of the factors influencing e-governance adoption. [http://citeseerx.ist.psu.edu/viewdoc/](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.517.8969&rep=rep1&type=pdf)

[download?doi=10.1.1.517.8969&rep=rep1&type=pdf](http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.517.8969&rep=rep1&type=pdf)

The concept of smart cities as is being piloted in Cape Town South Africa, is done to understand the current challenges associated with the Internet of Things and personal data security. The learnings for those initiatives could benefit other countries.

WHAT ARE SOME OF THE RISKS WE FACE WITH THE INTRODUCTION OF GOVERNMENT DRIVEN E-SERVICES AND DO YOU HAVE ANY EXAMPLES OF THESE CASES IN YOUR COUNTRY?

The biggest risks are data breaches and malware attacks. The uncertainty of adequate server maintenance and disaster recovery practices at a government level, leave citizenry with very little trust about whether government can survive cyber-attacks or the continued classified security breaches as seen in the last government elections.



IN 2017, WE HAD SEVERAL CASES OF CYBER SECURITY ATTACKS INCLUDING RANSOMWARE ATTACKS ACROSS THE WORLD- WERE YOU IMPACTED BY THESE ATTACKS? IF YES, HOW DID YOU (COMPANY OR COUNTRY) RESPOND TO THESE CASES?

The group did experience phishing attacks on user email addresses and these were immediately quarantined. Response efforts done included:

1. Augmenting the security exclusions on the Firewall
2. Blocking of websites
3. End User education of Phishing scams.

CONSIDERING THE SHORTAGE OF SKILLED RESOURCES IN AFRICA, HOW CAN WE LIMIT THE IMPACT OF RANSOMWARE CASES?

1. Don't skimp on market ready and tested security solutions such as firewalls. Many small businesses and start-ups make the mistake of thinking that their businesses are too niche to be targets. In reality, half of all cyberattacks target smaller companies because they're more likely to have limited budgets devoted to cybersecurity. While not having security is a costly mistake, security can become costly in its own right if not planned and monitored.

2. Monitor Your Current Solutions to Plan Future Ones

While it's important to always budget for today's maintenance, don't let that prevent you from pursuing new methods that can provide better and more proactive protection to combat tomorrow's threats. Not all solutions are created equal, as there are always some systems or departments that are more vulnerable across an organisation. And never trust outside computers in the hope of saving some money. For instance, consultants shouldn't be allowed to use their own devices on your internal network. Either have a device you control and secure designated for them or force them to use only the guest network.

3. Invest in Your People.

As vital as the right security software is, what's even more important is that the people being protected by that software are educated on the best security practices. Your tools are only as strong as your people. For instance, while filtering tools can help weed out malicious emails, if your employees can't spot a fake email, then your company is at risk

DO YOU THINK ORGANISATIONS ARE SPENDING ENOUGH MONEY ON COMBATING CYBER-CRIME?

Not in the context of Lesotho, especially in small and medium companies. The reason really is that cybersecurity has not been included in the risk management portfolio as a pertinent and recurring risk. This is why it flies under the radar. Also, a compound to the problem is that money is spent on the wrong solutions because there is no cybersecurity policy in place.

WHAT CAN BE DONE TO ENCOURAGE MORE SPENDING ON CYBER SECURITY ISSUES?

Spending can increase in cyber security and data security can become a regulatory imperative for private sector organisations. If we include cybersecurity in company risk portfolios, and create commitment from top management to monitor progress then it will become a strategic imperative which commands investment to implement.

Regulators can also force compliance by creating penalties for financial institutions whose data privacy policies and procedures are out-dated or not followed adequately.

BASED ON OUR RESEARCH THE AFRICA CYBER SECURITY MARKET WILL BE WORTH USD2 BILLION DOLLARS BY 2020. DESPITE THIS OPPORTUNITY, AFRICA HAS NOT PRODUCED A SINGLE COMMERCIALLY VIABLE CYBER SECURITY PRODUCT/ SOLUTION.

IN YOUR OPINION, WHAT SHOULD AFRICAN COUNTRIES/UNIVERSITIES FOCUS ON TO ENCOURAGE INNOVATION IN THE DEVELOPMENT OF CYBER SECURITY SOLUTIONS?

The push for development can only come from industry demand. That can be fuelled by ensuring that cybersecurity becomes a business strategic imperative as explained above.

WHAT ROLE CAN THE PRIVATE SECTOR AND CONSUMERS OF IMPORTED CYBER SECURITY PRODUCTS PLAY TO ENSURE WE CAN ENCOURAGE LOCAL PLAYERS TO START DEVELOPING AFRICAN GROWN CYBER SECURITY PRODUCTS/SOLUTIONS OR EVEN SERVICES?

Same as above. This will naturally drive sourcing to less expensive providers, which can fuel development in country.

IN YOUR OPINION AND FROM AN AFRICAN CONTEXT, WHAT ARE THE TOP 2018 CYBER SECURITY PRIORITIES FOR AFRICAN COUNTRIES AND ORGANISATIONS?

a) Focusing on preventing more sandbox-evading malware

In recent years, sandboxing technology has become an increasingly popular method for detecting and preventing malware infections. However, cyber-criminals are finding more ways to evade this technology. For example, new strains of malware are able to recognise when they are inside a sandbox, and wait until they are outside the sandbox before executing the malicious code.

b) Creating standards for multi-factor authentication

Companies have a tendency to shy away from implementing multi-factor authentication, as they feel that it would negatively affect user experience. However, according to research carried out by Bitdefender, there is a growing concern about stolen identities amongst the general public. As such, we will likely see an increase in the number of companies implementing some form of MFA.

c) Increasing the budget for security

Security is getting more expensive and difficult to manage

In addition to reporting a significant rise in the new types of attacks they're seeing, organisations also report struggling to keep the cost and complexity of managing security down.

In an attempt to respond to new threats and provide more advanced protection beyond file analysis, some traditional and next-generation antivirus vendors have begun offering supplemental add-ons and additional features.



CYBER SECURITY SKILLS GAP

Lesotho 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 Africa; 13500, to determine the approximate number of skilled professionals within the country.

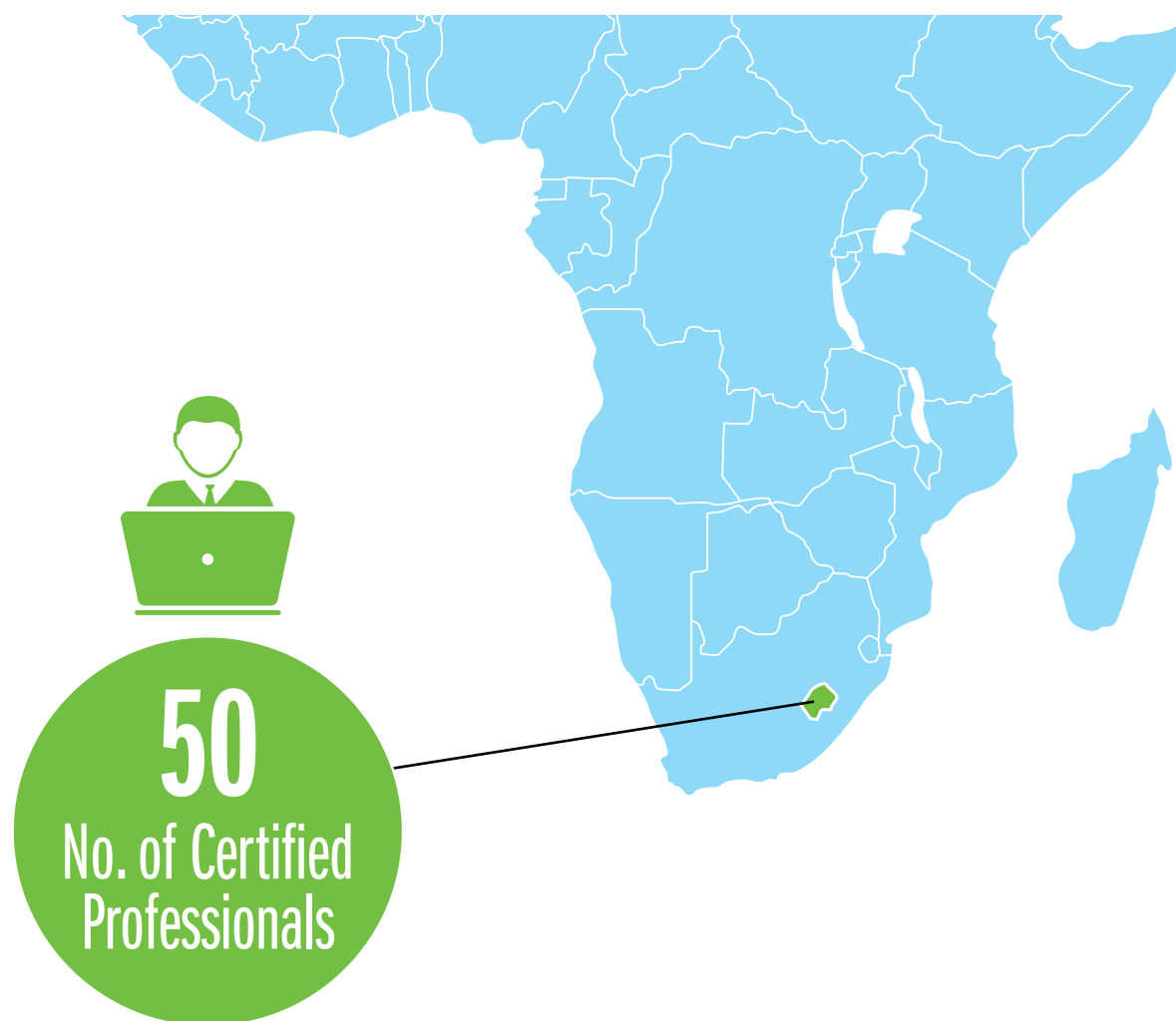
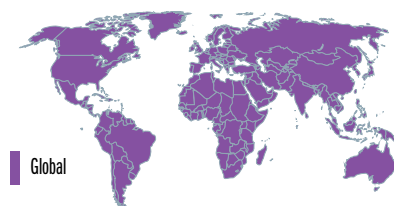
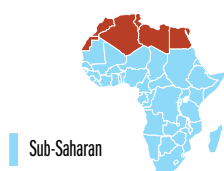













FIGURE 1: SKILLS PROFESSIONAL IN AFRICA.



No. of Skilled Professionals in 2018



		3795	84,484
		646	19,163
		945	32,233
		324	5749
	+ Others		
		844	*
		6554	*
			
	OTHERS		
	TOTAL	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>

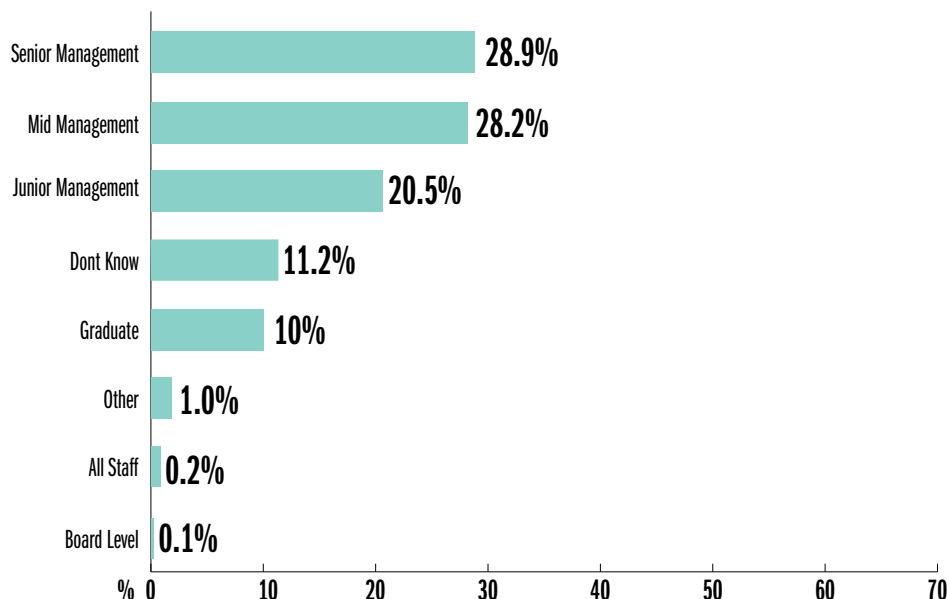
FIGURE 2: SKILLED PROFESSIONALS.



SKILLS GAP IN AFRICA

To determine where the pain points are, we asked over 1000 professionals to provide more insights on the issues they faced. Below are the findings:

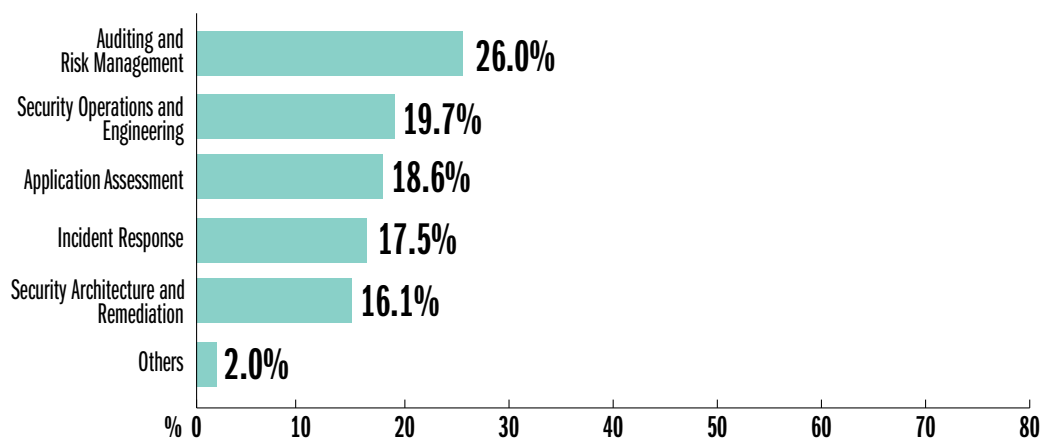
AT WHICH LEVEL DOES YOUR ORGANISATION FIND THE SKILLS SHORTAGE TO BE THE MOST ACUTE?



GRAPH 8: SKILLS SHORTAGE PAIN POINT.

All industries reviewed declared a challenge in finding top-tier professionals. About 90% 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.



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.

05



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

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

Secure Network Architecture and Design

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

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

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

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

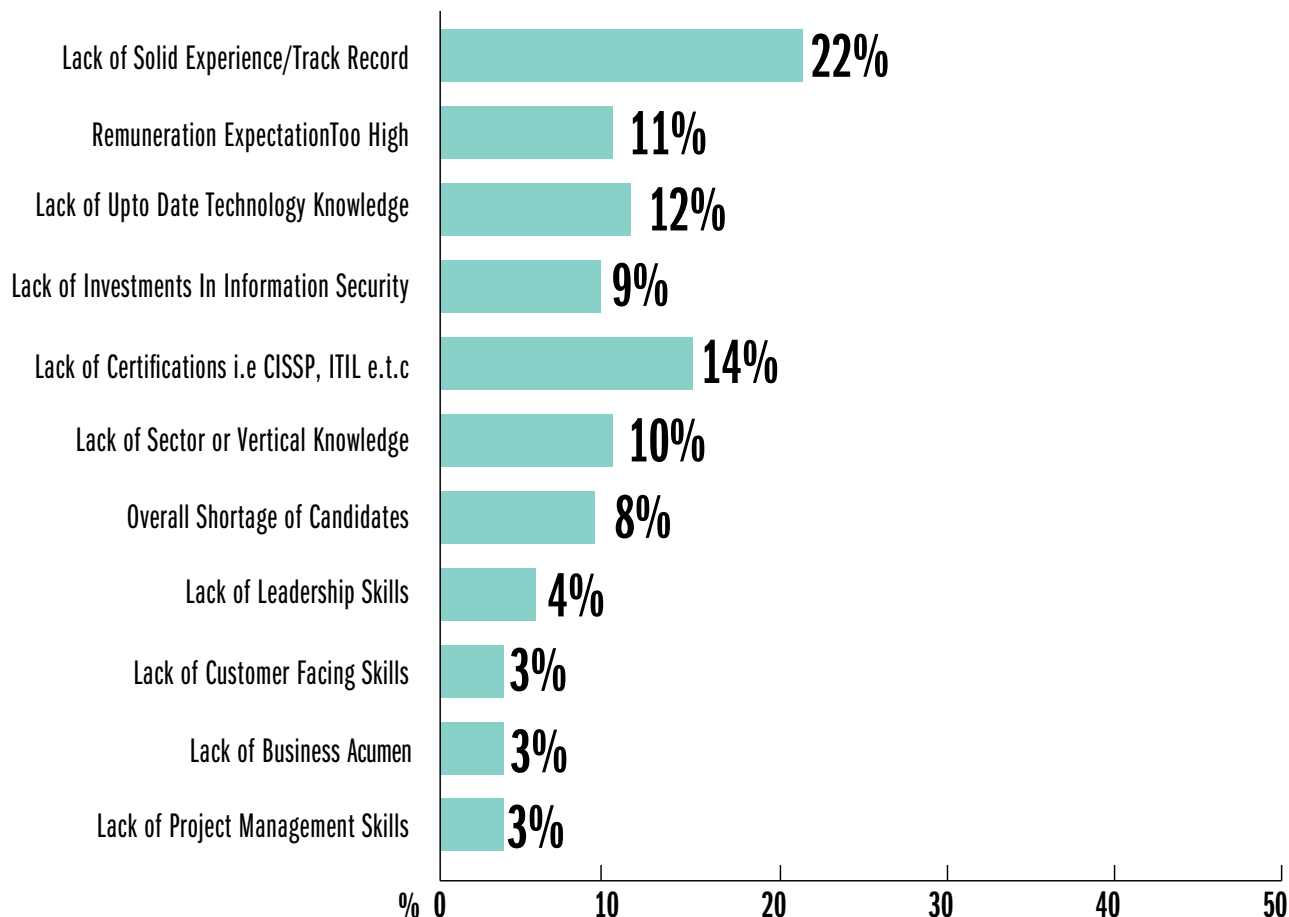
- **A bank** relies on the availability of their channels, security of their customer data and

proper dispensation of monies occurring on a 24/7/365 basis to meet demand and generate revenue. System downtime or malicious transactions costs the organisation. With this understanding, the architect designs the network to be able to identify and withstand any threats and attacks that may lead to the successful exploitation of these dearly.

- **Legal firms** handle confidential information that could cost organisations millions of dollars, or even cost people their lives if in the wrong hands, a case in point being the panama papers. The conversations between legal partners and their clients are confidential. The fact that a third party could intercept these conversations could be the biggest threat a law firm faces. A security architect understands these threats and models a network that has proper segregation of access, data loss prevention and anti-tampering.
- **A biomedical company** focuses all of its effort on researching new pharmaceuticals. The data generated from this research is the nest egg of the organisation, and represents the combined results of the money provided by their investors. Should a competitor gain access to the information, it could potentially cause the entire organisation to fail. The possibility of theft of intellectual property could be the biggest threat faced by this biomedical company.



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



GRAPH 10: RECRUITING CONSTRAINTS.



IF YOU HAVE AN EDUCATION AND NO EXPERIENCE, YOU'RE GOING TO BE HARD-PRESSED TO FIND A CAREER IN THIS FIELD. YOU'VE GOT TO DO WHATEVER IT TAKES TO GET YOURSELF EXPERIENCE. THAT'S MORE IMPORTANT THAN ANYTHING.

KEVIN HAWKINS, PROFESSOR OF IT AND DATABASE ADMINISTRATOR AT HUMANA HEALTH INSURANCE

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

TALENT POACHING

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

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

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



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

CHART 9: IMPORTANCE OF CERTIFICATIONS.



Certifications are a crucial stepping stone for almost any IT career. From our survey results, 96% of the respondents indicated that certificates are important. Clearly, certifications are resume worthy, but are they the end-all be-all?

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

**MOLUPE MOLUPE**

ICT Manager, Lesotho Communications Authority

CYBERSEC ISSUES OF 2017**a. Awareness of users.**

In this country, users of technology are not taking security seriously. People are not really aware of good security practices to follow. This makes them very vulnerable. We have seen a lot happening on social media, information of high confidentiality/ secrecy in government flying around. Employees in government have to be made aware of what it means and why they should follow established best security practices. My only worry is whether they are there within the government.

b. Personal Information.

Here the vulnerability is due to: some people are still not careful with what they put online considering the high attacks on personally owned services on sites as well as identify theft.

c. Mobile money system.

We have heard a lot about attempts to infiltrate authentication system to steal funds from consumers of M-pesa/Eco cash. We see people install apps on their phones unaware that they are exposing themselves to attack of the mobile wallets or otherwise. Operators will have to work tirelessly to ensure that their systems are secure.

FAKE NEWS

Due to release of government information day in day out to social media, it has become difficult to identify fake news.

In this country fake news is ruling. It is more on the political space where people or parties are fighting to topple each other or government of the day.

To me it will be difficult for the Telcos/ISP to

control fake news. This should be responsibility of government and end users. The government has to deploy people who are carefully monitor the social media for such news and act on them.

Regulators should force players like Google and Facebook to improve in technologies that can be used to detect fake news. It may be easy for these players to design and implement algorithms to identify fake news.

Improving user awareness can be achieved by educating users to consider or follow a diversity of people and perspectives. It is important not to limit oneself on the small range of sources of news. It is important to consent all viewpoints in order to get a balanced view. It is also important to promote strong norms on professional journalism and enhance digital literacy among users.

IN AFRICA OR A COUNTRY LIKE LESOTHO, THE HIGHEST RISK IS INABILITY TO USE E-SERVICE.

This is mainly cause by digital illiteracy. People are not e-literate but the GOL has engaged in developing e-services.

Other than that people are still worried that they may be defrauded or their personal information misused.

In Lesotho, some of the services like applications for ID or passport can be introduced online but people who really need this are not familiar with technology or the services are not available at their places.

RANSOMWARE CASES CAN BE REDUCED BY EDUCATING OUR USERS OR PUBLIC IN GENERAL THAT IT IS NOT WISE TO CLICK EVERYTHING. EDUCATION. EDUCATION. EDUCATION.

IN LESOTHO THERE'S NOT MUCH ACTIVITY IN COMBATING CYBER-CRIME. THE WORST THING IS THAT EVEN REGULATION/LAWS ARE NOT PASSING IN PARLIAMENT BUT DRAFTS HAVE BEEN DONE. THE GOVERNMENT IS REACTIVE ON THE ISSUE OF CYBER SECURITY.

So talking about money is something else.

RESEARCH AND DEVELOPMENT IN THE AREA OF CYBER SECURITY IS IMPORTANT. COMING UP WITH MORE APPLICATION EXPERTS TO DEVELOP SOLUTIONS TO PROBLEMS ENCOUNTERED. CREATING RELATIONSHIPS BETWEEN THE INDUSTRY AND UNIVERSITY IS IMPORTANT. THIS IS ALREADY HAPPENING IN EUROPE AND IN THE US. AFRICA HAS TO START CONSIDERING THAT AS CRITICAL.

PRIORITIES FOR 2018

- There's a need to look into mobile money platform as more focus will be on them.
- Countries and organisation alike will need to look into educating their people.
- More focus on the cryptocurrency exchanges.
- As more Apps are coming in, there'll be a need to look into mobile networks, vulnerability of mobile devices with personal/private information.



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 Limited.

AS AFRICA DEVELOPS ITS
SILICON SAVANNA, ONE
QUESTION STILL STANDS,
WHERE ARE THE LADIES?

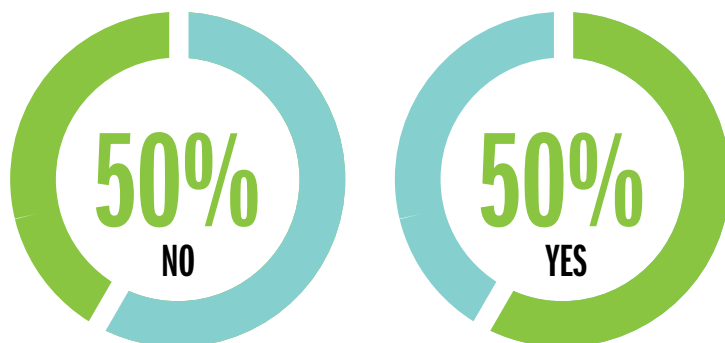
WE ASKED OUR RESPONDENTS
TO PROVIDE THEIR VIEWS.





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

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



Interestingly, we noted a 50/50 response to this statement. It's important to point out that majority of the respondents were male. However, the gender gap discussion is not really one of right versus wrong or men versus women but rather diversity.

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

GENDER GAP ISSUES

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

- Women do not get promoted at the same rate as men are, and
- Women are not getting salary increases at the same rate as men are even though they are asking for and applying at the same rate.

- As a rule, women wait until they accrue required skills before applying for cybersecurity jobs, while men routinely bluff their way through. The men may have none of (the skills) and will still apply.

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

LIES WOMEN TELL THEMSELVES FOR NOT WORKING IN IT:

"I AM NOT GOOD ENOUGH."

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

"THAT'S A MAN'S JOB."

"I AM OKAY WHERE I AM."

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

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

"IT IS THE BOYS CLUB"

"THERE ARE TOO MANY MEN"

"THERE ARE TOO MANY WOMEN"





THE TECHNICAL SKILLS QUESTIONS?

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

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

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

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





STATE OF CYBER INSURANCE IN AFRICA

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

Lack of Awareness. Digital technology in Lesotho 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 Lesotho 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 identifying and assessing all risks, implementing controls to mitigate the risks, verifying 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 organisation does not have skilled professionals to help determine the organisations cyber risk exposure, they can always use a third-party to conduct the analysis.

WHAT FUTURE TRENDS SHOULD WE ANTICIPATE WITHIN CYBER INSURANCE SECTOR?

Cyber Insurance is expected to grow exponentially. As various legislations are implemented, the uptake of Cyber Insurance will increase.

MANY ORGANISATIONS IN AFRICA 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.



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: SKILLS MATRIX.

0

Not Applicable

1

General Knowledge

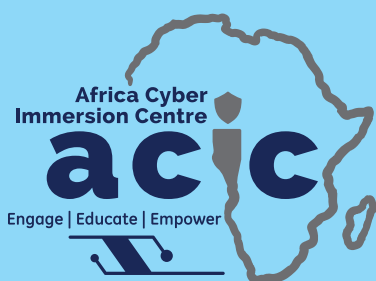


Skills Mismatch - Are You Hiring The Right Person, For The Right Job?

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



AFRICA CYBER IMMERSION CENTRE



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:

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.

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

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

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 Lesotho 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 HUMBLLED AND EXTEND OUR SINCERE ARM OF APPRECIATION AND GRATITUDE.



STUDENT, KAPSABET BOYS HIGH SCHOOL



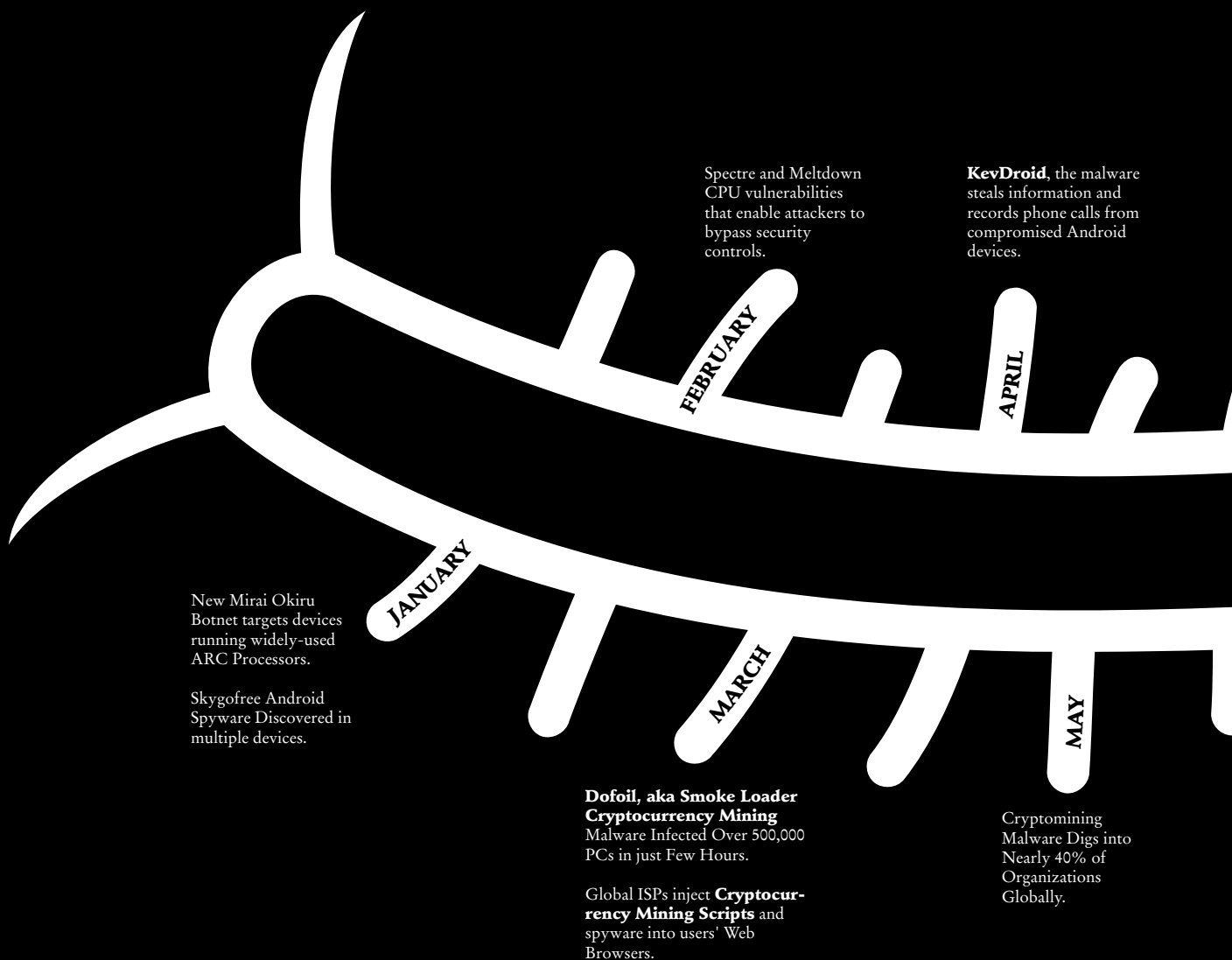






CYBER INTELLIGENCE

LATEST MALWARE VIRUSES THAT WERE RELEASED AND CAPTURED IN 2018.





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: f05a31ac604e4ea844e8130e45d30f01

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.

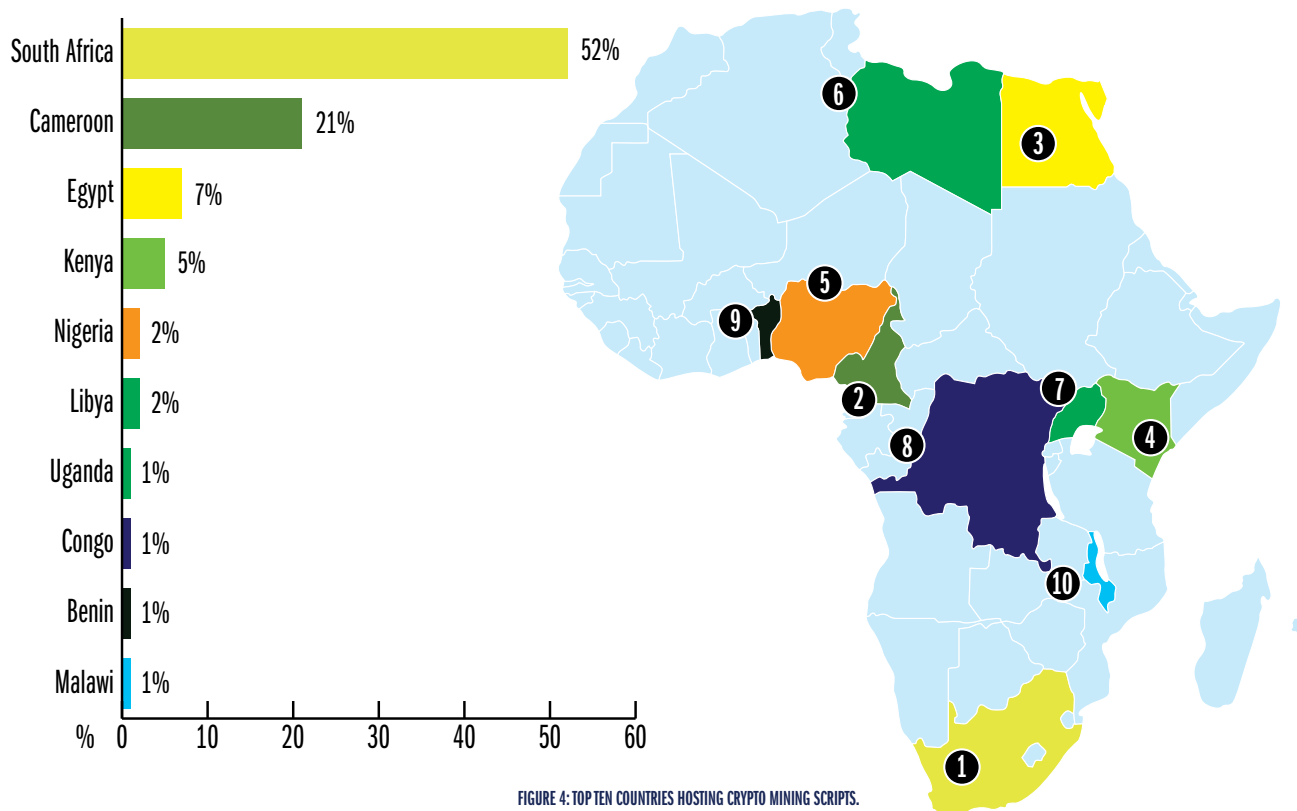
DarkPulsar typically affected Windows 2003/2008 servers. It runs malicious code



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.



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 external 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

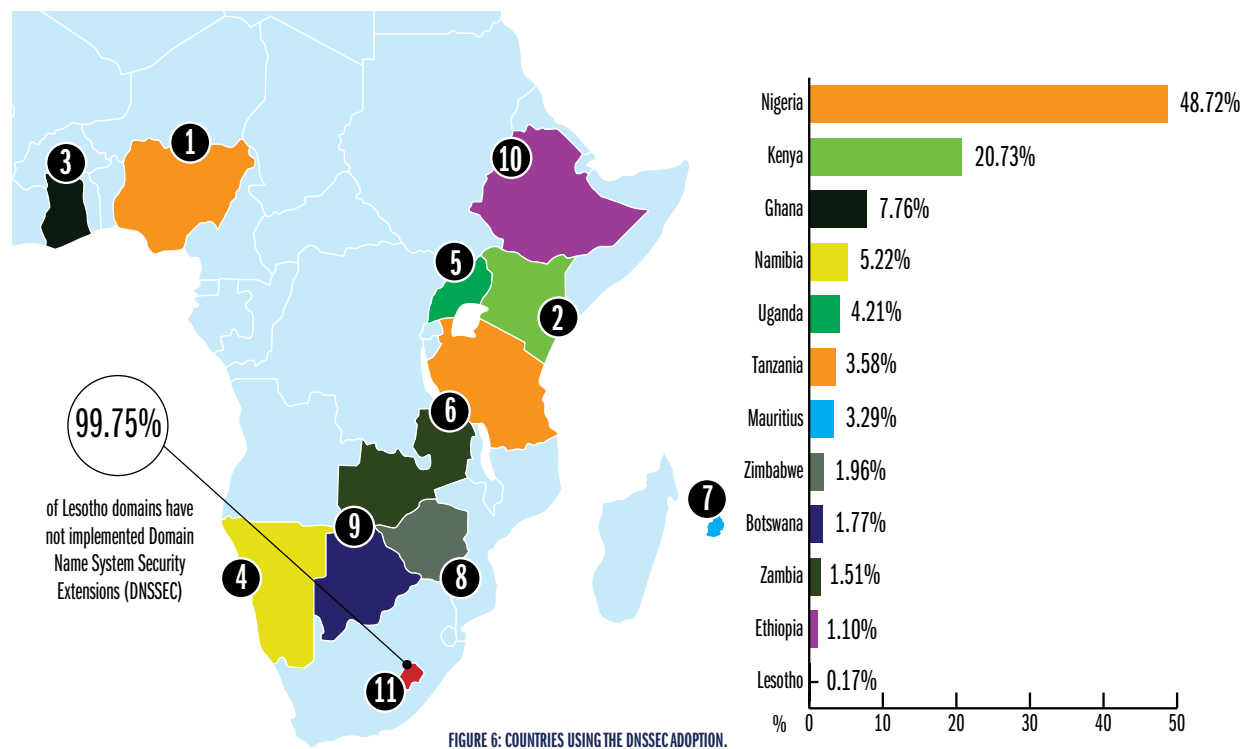
RASPBERRY PI

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:



DNSSEC ADOPTION





INDUSTRY PLAYER PERSPECTIVE

**MAKHELE MOLEFE**

Senior Systems Support Officer,
National Manpower Secretariat

KINDLY HIGHLIGHT SOME OF THE TOP CYBER SECURITY ISSUES OF 2017 AND HOW THESE ISSUES IMPACTED YOU PERSONALLY, YOUR ORGANIZATION OR COUNTRY?

Pyramid schemes running over internet.

A. DO YOU THINK FAKE NEWS IS A MAJOR PROBLEM IN YOUR COUNTRY/AFRICA? IF YES, WHO SHOULD BE RESPONSIBLE FOR CONTROLLING THE CREATION AND DISTRIBUTION OF FAKE NEWS (GOVERNMENT, END USERS, TELCOS/ISPS OR CONTENT OWNERS)?

Yes it is. Government, Telcos/ISPs.

B. SHOULD REGULATORS FORCE INFLUENTIAL PLATFORMS LIKE GOOGLE AND FACEBOOK TO REMOVE FAKE NEWS AND OTHER EXTREME FORMS OF CONTENT FROM THEIR PLATFORMS?

They can remove the fake news but also affected people can correct and give what is correct news.

C. WHAT CAN BE DONE TO IMPROVE THE GENERAL USER AWARENESS ON THE DETECTION OF FAKE NEWS IN THE COUNTRY?

General users can be trained on how to look at features of credible and reliable news/information.

A. MANY GOVERNMENTS IN AFRICA ARE INVESTING IN E-SERVICES (E-GOVERNMENT, E-VOTING, E-TAX SYSTEMS AND MANY OTHER PORTALS. DO YOU THINK THE AFRICAN CITIZENRY IS READY TO CONSUME AND UTILIZE THESE SYSTEMS WITHOUT THE WORRY OF PRIVACY, SECURITY AND FRAUD?

No.

B. WHAT ARE SOME OF THE RISKS WE FACE WITH THE INTRODUCTION OF GOVERNMENT DRIVEN E-SERVICES AND DO YOU HAVE ANY EXAMPLES OF THESE CASES IN YOUR COUNTRY?

There are people who hack systems and they want to make fraudulent payments for themselves.

IN 2017, WE HAD SEVERAL CASES OF CYBER SECURITY ATTACKS INCLUDING RANSOMWARE ATTACKS ACROSS THE WORLD-WERE YOU IMPACTED BY THESE ATTACKS?

No

IF YES, HOW DID YOU (COMPANY OR COUNTRY) RESPOND TO THESE CASES?

N/A

CONSIDERING THE SHORTAGE OF SKILLED RESOURCES IN AFRICA, HOW CAN WE LIMIT THE IMPACT OF RANSOMWARE CASES?

We need to train people intensively on cyber security and all that they need to provide proper security for companies and government departments.

DO YOU THINK ORGANIZATIONS ARE SPENDING ENOUGH MONEY ON COMBATING CYBER-CRIME?

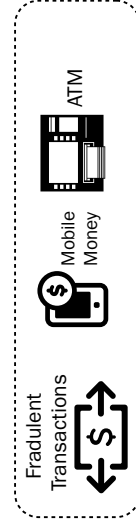
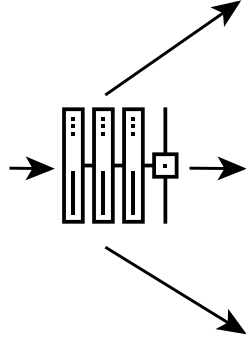
No.

WHAT CAN BE DONE TO ENCOURAGE MORE SPENDING ON CYBER SECURITY ISSUES?

Top management needs to be made aware of what is going on online, its benefits and the associated risks. This should motivate them to train their technicians on cyber-security.

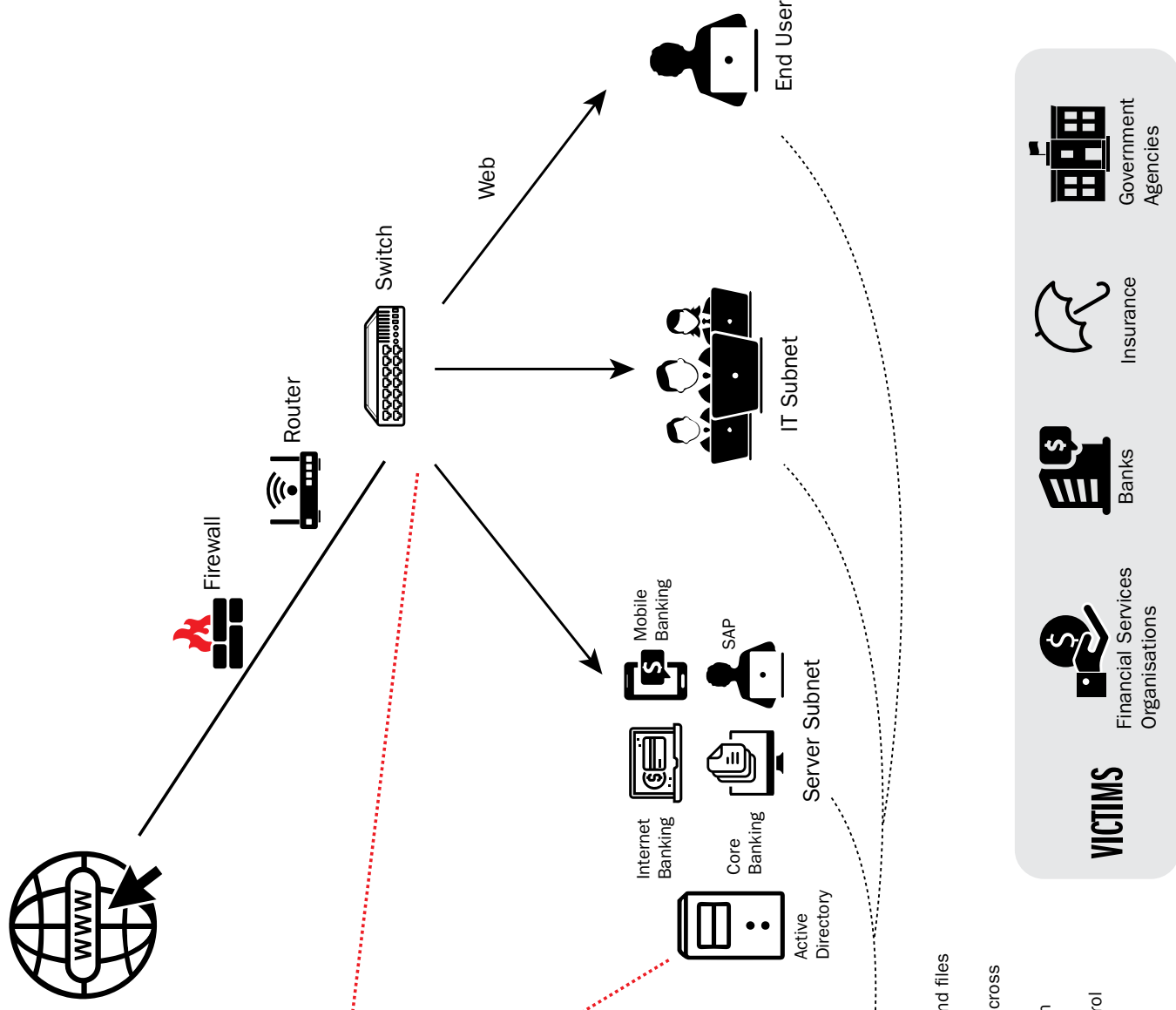
ANATOMY OF A CYBER HEIST

Attack Vectors



ATTACK PROCESS

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

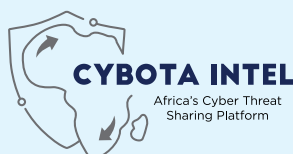




INFORMATION SHARING GAP

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.

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.



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.

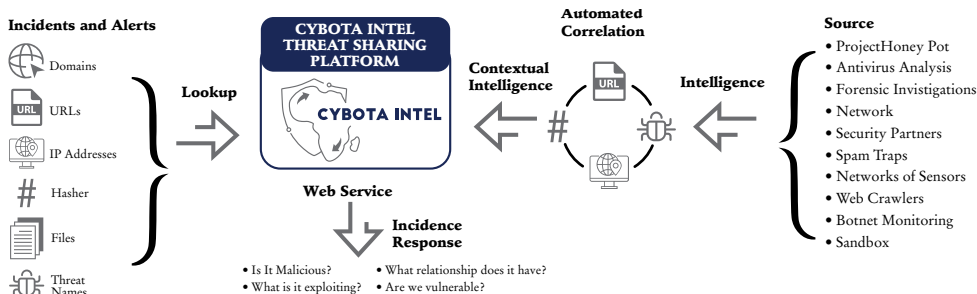


Prevention:
Through applying of patches and fixes shared through the platform.



Improved Eco-system:
Through information sharing.

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

ACADEMIA SECTOR

**U. EBISOH**

Limkokwing University, Maseru

KINDLY HIGHLIGHT SOME OF THE TOP CYBER SECURITY ISSUES OF 2017 AND HOW THESE ISSUES IMPACTED YOU PERSONALLY, YOUR ORGANISATION OR COUNTRY?

- Identity Theft
- Online Predators

DO YOU THINK FAKE NEWS IS A MAJOR PROBLEM IN YOUR COUNTRY/ AFRICA?

Yes, it is!

IF YES, WHO SHOULD BE RESPONSIBLE FOR CONTROLLING THE CREATION AND DISTRIBUTION OF FAKE NEWS (GOVERNMENT, END USERS, TELCOS/ISPS OR CONTENT OWNERS)?

All stakeholders, if possible

SHOULD REGULATORS FORCE INFLUENTIAL PLATFORMS LIKE GOOGLE AND FACEBOOK TO REMOVE FAKE NEWS AND OTHER EXTREME FORMS OF CONTENT FROM THEIR PLATFORMS?

No.

WHAT CAN BE DONE TO IMPROVE THE GENERAL USER AWARENESS ON THE DETECTION OF FAKE NEWS IN THE COUNTRY?

1. Using social media. However, for workers who are not familiar with social media, formal or informal training may be needed.
2. Knowledge management could take place in traditional settings (such as coffeehouses and ice cream parlours) just by using the owner-proprietor's memory of his key customers, their preferences, and their client-service expectations or typically use a range of digital tools to track, monitor and analyze the huge streams of data their businesses are generating, a process called "data mining".

MANY GOVERNMENTS IN AFRICA ARE INVESTING IN E-SERVICES (E-GOVERNMENT, E-VOTING, E-TAX SYSTEMS AND MANY OTHER PORTALS.) DO YOU THINK THE AFRICAN CITIZENRY IS READY TO CONSUME AND UTILIZE THESE SYSTEMS WITHOUT THE WORRY OF PRIVACY, SECURITY AND FRAUD?

Yes and No.

WHAT ARE SOME OF THE RISKS WE FACE WITH THE INTRODUCTION OF GOVERNMENT DRIVEN E-SERVICES AND DO YOU HAVE ANY EXAMPLES OF THESE CASES IN YOUR COUNTRY?

No.

- There is lack of trust
- Security concerns
- Obsolete technologies in use
- Inability to adapt to changes
- Not enough technology literacy

IN 2017, WE HAD SEVERAL CASES OF CYBER SECURITY ATTACKS INCLUDING RANSOMWARE ATTACKS ACROSS THE WORLD - WERE YOU IMPACTED BY THESE ATTACKS?

No.

DO YOU THINK ORGANISATIONS ARE SPENDING ENOUGH MONEY ON COMBATING CYBER-CRIME?

Yes.

WHAT CAN BE DONE TO ENCOURAGE MORE SPENDING ON CYBER SECURITY ISSUES?

Proper budgeting allocations.

IN YOUR OPINION, WHAT SHOULD AFRICAN COUNTRIES/UNIVERSITIES FOCUS ON TO ENCOURAGE INNOVATION IN THE DEVELOPMENT OF CYBER SECURITY SOLUTIONS?

African countries should focus on new and more sophisticated digital processes which should be introduced online with impacts on the efficient management of our network.

WHAT ROLE CAN THE PRIVATE SECTOR AND CONSUMERS OF IMPORTED CYBER SECURITY PRODUCTS PLAY TO ENSURE WE CAN ENCOURAGE LOCAL PLAYERS TO START DEVELOPING AFRICAN GROWN CYBER SECURITY PRODUCTS/SOLUTIONS OR EVEN SERVICES?

More coordinated standards, procedures, methods and agreements for the digital exchange of information on networks

IN YOUR OPINION AND FROM AN AFRICAN CONTEXT, WHAT ARE THE TOP 2018 CYBER SECURITY PRIORITIES FOR AFRICAN COUNTRIES AND ORGANISATIONS?

Identity Theft

Online Predators





COMPUTER CRIME AND CYBERCRIME BILL LESOTHO



06

OBJECTIVES

- Act provides a legal framework for the criminalisation of computer and network related offences.
- Principal aims are to criminalize certain illegal content in line with regional and international best practices, provide the necessary specific procedural instruments for the investigation of such offences and define the liability of service providers.

PROVISIONS

- Draft Bill divided into nine parts – All provisions of Model law on cybercrime transposed and expanded as appropriate to suit Lesotho situation;
- Terms used and provisions other than those peculiar to Lesotho law defined;
- Proposed Bill, drafted using technology neutral language.

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 Crime and Cybercrime Bill Lesotho

Part 1

- Provides definitions and sets the objective of the Act, scope/application and the date when the Act will come into force;
- Defines terms such as “computer system”, “access provider” and “hinder” etc., using sufficiently broad wording and where possible illustrative examples. eg “Computer system” or “information system” - a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function;
- Sec. 3 (1) - term “access provider” can be both a legal person as well as a natural person. In light of this, even the operator of a private network can therefore be considered an access provider.
- “Hinder” - (includes cutting the electricity supply to a computer system; and causing electromagnetic interference to a computer system; and corrupting a computer system by any means; and inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data;
- “Critical infrastructure” - computer systems, devices, networks, computer programs, computer data, so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters



Part II	<ul style="list-style-type: none"> Purpose of Sections 4 24 of the Act is to improve means to prevent and address computer and network related crime by defining a common minimum standard of relevant offences based on best practice prevailing within the region as well as international standards. (eg CoECC, C/wealth Model Law) Ss.4 25 therefore provides minimum standards and therefore allows for more extensive criminalisation should the country so desire. all offences established in this Act, require that offender is carrying out the offences intentionally. Reckless acts are therefore not covered. “person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification...” eg Section 5 requires that the offender is carrying out the offences intentionally. Reckless acts are not covered. Provides a set of substantive criminal law provisions that criminalise certain offences - eg illegally accessing and remaining logged into a computer system without lawful excuse or justification, obstructing, interrupting or interfering with the lawful use of computer data and disclosing details of a cybercrime investigation Other than interfering with computer data and data espionage (Penal Code Act S.62), harassment, and to some, degree, interception and system interference (Communications Act S.44) none of these acts are currently legislated against by existing legislation in Lesotho.
Part III	<ul style="list-style-type: none"> Provides procedures to determine jurisdiction over criminal offences enumerated in Sections 4 24 Jurisdiction territorial and extra-territorial (ship/aircraft registered in enacting country, citizen etc) S.25 (1)- Territorial jurisdiction applicable if <ul style="list-style-type: none"> - both person attacking computer system and victim system are located within same territory or country. - computer system attacked is within its territory, even if the attacker is not. S25(2) – applies if a national commits an offence abroad, and conduct is also an offence under law of state in which it was committed or conduct has taken place outside territorial jurisdiction of any State
Part IV	<p>Electronic evidence</p> <p>Deals with admissibility of electronic evidence and incorporates by reference law dealing with electronic transactions & communication to apply</p>
Part V	<p>Procedural law</p> <ul style="list-style-type: none"> Provides a set of procedural instruments necessary to investigate Cybercrime; Identification of offenders, protection of integrity of computer data during an investigation contains several inherently unique challenges for law enforcement authorities. Purpose is to improve national procedural instruments by defining common minimum standards based on best practices within the region as well as international standards. - definition of standards will help national lawmakers to discover possible gaps in the domestic procedural law. Sections 28 35 only define minimum Standards and therefore do not preclude creation of more extensive criminalization at national level introduces new investigation instruments (eg. Section 35) and also aims to adapt traditional procedural measures (such as Section 28). All instruments referred to aim at permitting obtaining and/or collection of data for purpose of conducting specific criminal investigations or proceedings. instruments described in Part V to be used in both traditional computer crime investigation and in any investigation that involves computer data and computer systems
Part VI	<p>Liability (Service Providers)</p> <ul style="list-style-type: none"> Defines limitations of liability of Internet service providers. Responsibility of certain Internet Service Providers are limited in Act, if their ability to prevent users from committing crimes is limited. It was therefore necessary to differentiate between the different types of providers Without clear regulation, uncertainty created as to whether there is an obligation to monitor activities and, whether providers could be prosecuted based on a violation of the obligation to monitor users' activities Apart from possible conflicts with data protection regulations and secrecy of telecommunication, such obligation would especially cause difficulties for hosting providers that store significant number of websites. To avoid these conflicts S. 36 excludes general obligation to monitor transmitted or stored information. Limits liability of providers to criminal liability.
Part VII	<ul style="list-style-type: none"> General Provisions – administration of Act - includes issuance of Regulations eg interception of computer data (security, functional and technical requirements for interception, etc), critical information infrastructure (identification, securing integrity and authenticity of, registration and other procedures relating to critical information infrastructure, etc)



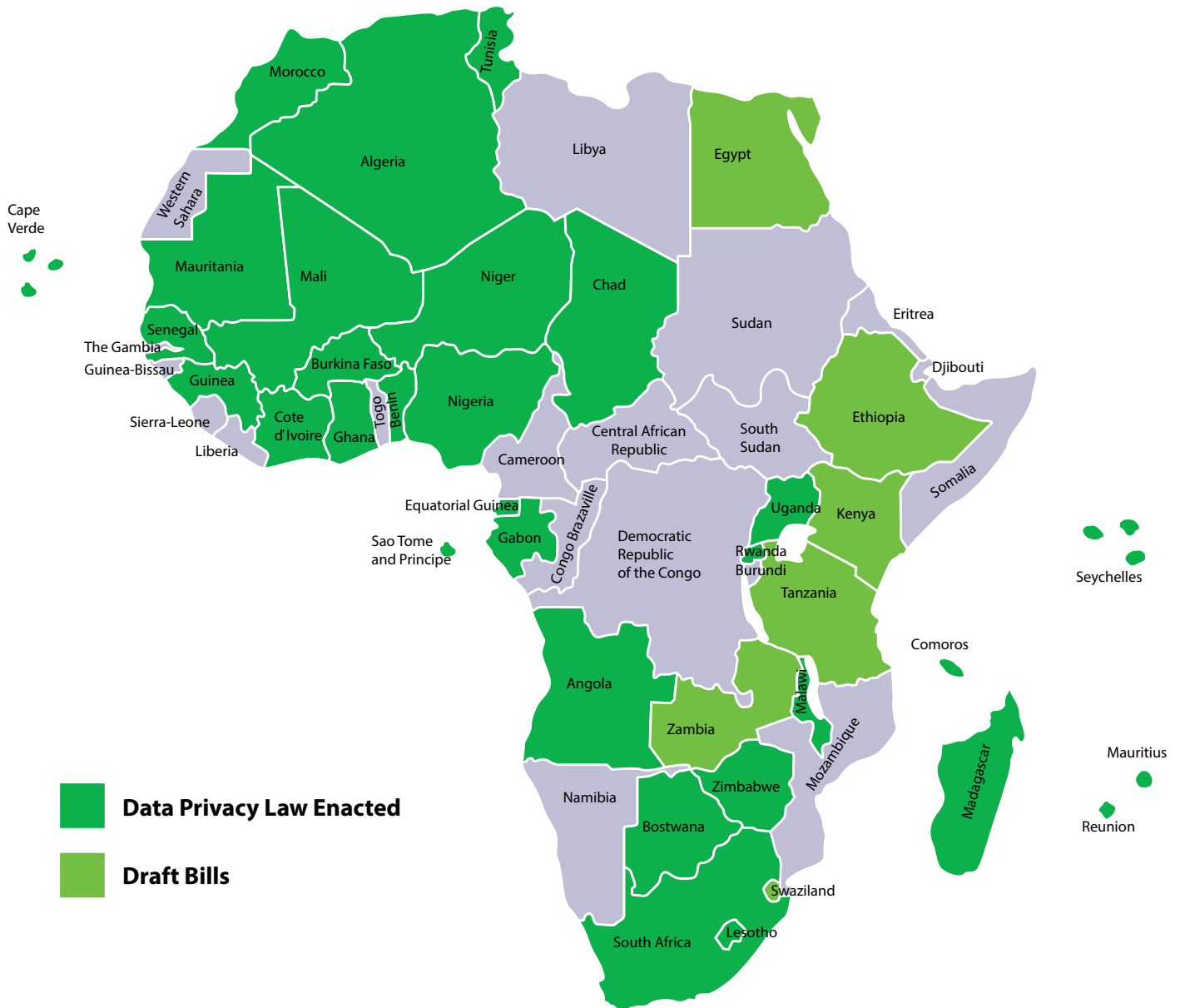
Part VIII	Consequential Amendments and Savings <ul style="list-style-type: none"> • of legislation needing to be amended for purposes of bringing it in line with draft Bill ie • Communications Act, No. 4 of 2012 • Amendment of Section 44 – removal of provisions on, harassment, interfering with computer data / computer system, interception,
Part IX	Penal Code No. 30 of 2012 <ul style="list-style-type: none"> • Amendment of Section 62 - removal of provisions on interfering with computer / storage device/ computer data, and data espionage

Offences

1. Illegal Access	9. Computer-related Fraud	16. SPAM
2. Illegal Remaining	10. Child Pornography	17. Disclosure of details of an investigation
3. Illegal Interception	11. Pornography	18. Failure to permit assistance
4. Illegal Data Interference	12. Identity-related crimes	19. Harassment utilizing means of electronic communication
5. Data Espionage	13. Racist and Xenophobic Material	20. Violation of Intellectual property rights
6. Illegal System Interference	14. Racist and Xenophobic Motivated Insult	21. Attempt, abetment and Conspiracy
7. Illegal Devices	15. Genocide and Crimes Against Humanity	
8. Computer-related Forgery		

Part III	<ul style="list-style-type: none"> • Jurisdiction • Extradition 	
Part IV	ELECTRONIC EVIDENCE Admissibility of Electronic Evidence	
Part V	Procedural Law <ul style="list-style-type: none"> • Search and Seizure • Assistance • Production Order • Expedited preservation 	<ul style="list-style-type: none"> • Partial Disclosure of traffic data • Collection of traffic data • Interception of content data • Forensic Tool
Part VI	Liability <ul style="list-style-type: none"> • No Monitoring Obligation • Access Provider • Hosting Provider 	<ul style="list-style-type: none"> • Caching Provider • Hyperlinks Provider • Search Engine Provider
Part VII	General Provisions <ul style="list-style-type: none"> • Limitation of Liability • Forfeiture of Assets • General Provision on Cybercrimes • Regulations 	<ul style="list-style-type: none"> • Offence by body corporate or un-incorporate • Prosecutions • Compounding of Offences
Part VIII	Consequential AMENDMENTS AND SAVINGS <ul style="list-style-type: none"> • Communications Act, 2012 • Construction • Amendment of Section 44 (harassment, interfering with computer data / computer system, interception) 	
Part IX	Penal Code Act 2012 <ul style="list-style-type: none"> • Construction • Amendment of Section 62 (interfering with computer/ storage device/computer data, data espionage). 	

Data Privacy and Bills - Africa



Source: Graham Greenlead
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



LAND ADMINISTRATION AUTHORITY

KINDLY HIGHLIGHT SOME OF THE TOP CYBER SECURITY ISSUES OF 2017 AND HOW THESE ISSUES IMPACTED YOU PERSONALLY, YOUR ORGANISATION OR COUNTRY?

- Ransomware
- Fake news is a major problem in Lesotho. Both government and content owners (freedom of expression, freedom comes with responsibility (compliance)
- Platforms like google and Facebook have some mechanisms in place to remove content that is classified as harmful, offensive or fake.

MANY GOVERNMENTS IN AFRICA ARE INVESTING IN E-SERVICES (E-GOVERNMENT, E-VOTING, E-TAX SYSTEMS AND MANY OTHER PORTALS. DO YOU THINK THE AFRICAN CITIZENRY IS READY TO CONSUME AND UTILIZE THESE SYSTEMS WITHOUT THE WORRY OF PRIVACY, SECURITY AND FRAUD?

African citizenry is ready to adopt the e-services to a certain extend.

WHAT ARE SOME OF THE RISKS WE FACE WITH THE INTRODUCTION OF GOVERNMENT DRIVEN E-SERVICES AND DO YOU HAVE ANY EXAMPLES OF THESE CASES IN YOUR COUNTRY?

Risks associated with e-services are trust, security.

4. IN 2017, WE HAD SEVERAL CASES OF CYBER SECURITY ATTACKS INCLUDING

RANSOMWARE ATTACKS ACROSS THE WORLD-WERE YOU IMPACTED BY THESE ATTACKS?

Yes, there was a single case of ransomware:

IF YES, HOW DID YOU (COMPANY OR COUNTRY) RESPOND TO THESE CASES?

We had to recover from backups, security awareness and investing in security can help limit the impact of ransom ware.

DO YOU THINK ORGANISATIONS ARE SPENDING ENOUGH MONEY ON COMBATING CYBER-CRIME?

We believe that organisations are spending some money on cyber-crime: security courses be standardized.

BASED ON OUR RESEARCH THE AFRICAN CYBER SECURITY MARKET WILL BE WORTH USD 2 BILLION BY 2020. DESPITE THIS OPPORTUNITY, AFRICA HAS NOT PRODUCED A SINGLE COMMERCIALY VIABLE CYBER SECURITY PRODUCT/ SOLUTION. IN YOUR OPINION, WHAT SHOULD AFRICAN COUNTRIES/UNIVERSITIES FOCUS ON TO ENCOURAGE INNOVATION IN THE DEVELOPMENT OF CYBER SECURITY SOLUTIONS?

African Universities should focus on promotion of cybersecurity research; Private sector can sponsor cybersecurity research.



TOP TRENDS AND PRIORITIES FOR 2019

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



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

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

GROWTH IN LETHAL AND TARGETED MALWARE

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

ATTACK-REPLICATION

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

INCREASED USE OF OUTSOURCED/ MANAGED SECURITY SERVICES

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

USE OF THIRD PARTIES TO EXPLOIT TARGET ORGANISATIONS

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





CONTINUED ENGAGEMENT FROM BOARD AND SHAREHOLDERS

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

GROWTH IN CYBER INSURANCE OFFERINGS

The global cyber insurance market is expected to expand globally and projected to grow to \$5bn in annual premiums by 2018 and at least \$7.5bn by 2020. AoN, one of the top insurance companies in Africa, 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 MEASURABLE 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.



Today, organisations 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 organisation'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 organisation. The degree of losses from cyber fraud and the scale of attacks are rising with every passing year. Indeed, available data shows that African organisations 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 organisation. 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 organisations, 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 organisation.

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 organisation, 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 organisation's attention to and readiness for cybersecurity risks. In order to understand and appreciate the state of their organisation'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, Lesotho 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, Lesotho 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.

INDUSTRY PLAYER PERSPECTIVE

NABIHAH RISHAD

Senior Risk Consultant, Serianu Limited



FRAUD EXPOSURES

FRAUD EXPOSURES

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

IP THEFT EXPOSURES

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

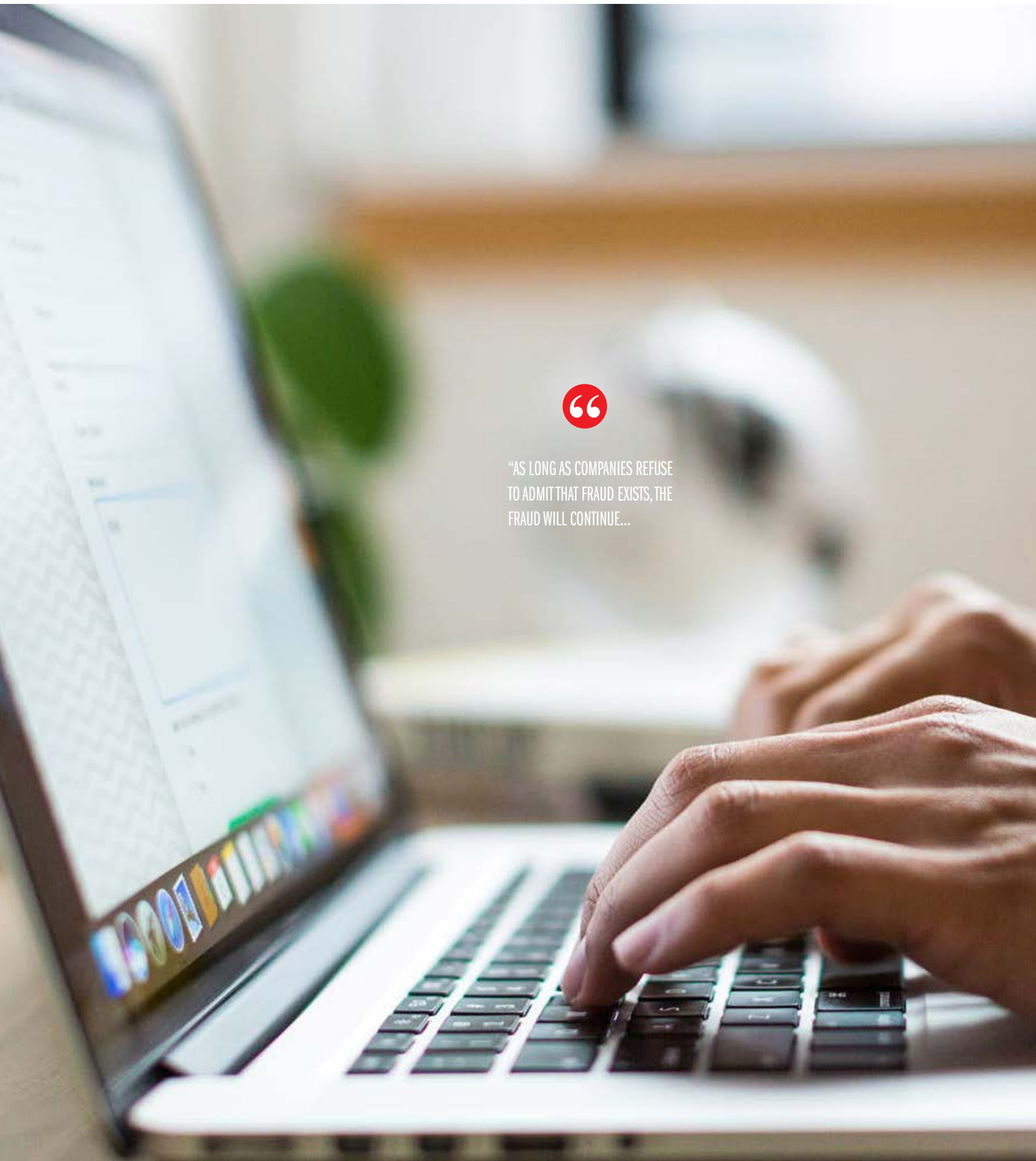
SABOTAGE EXPOSURES

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





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





CYBER VISIBILITY AND EXPOSURE QUANTIFICATION (CVEQ™) FRAMEWORK

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

Serianu CVEQ™ Framework



08

DID YOU KNOW?

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 assess 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:

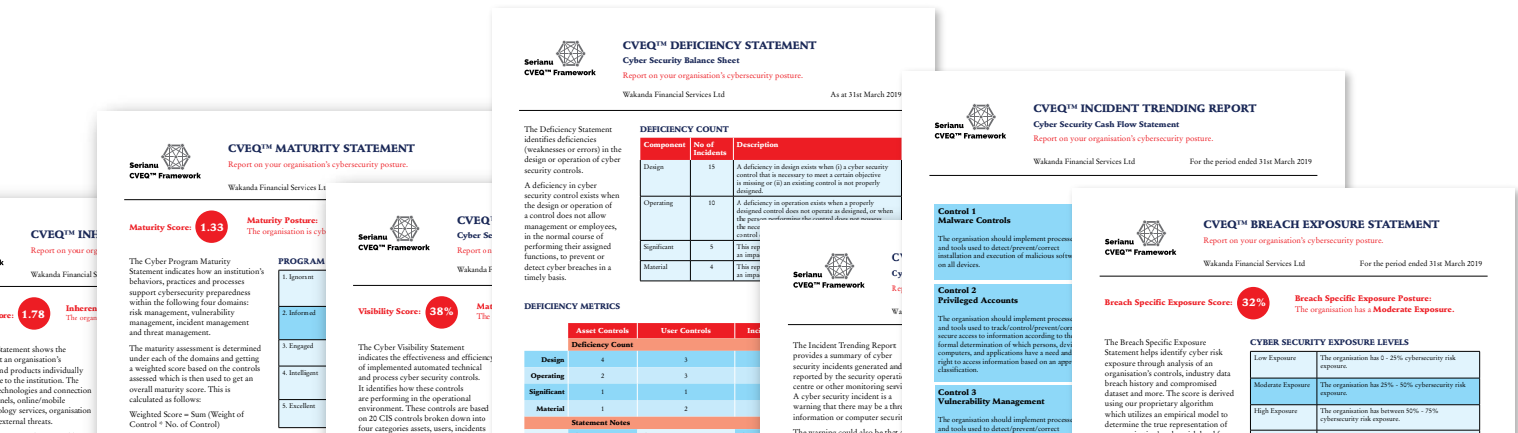
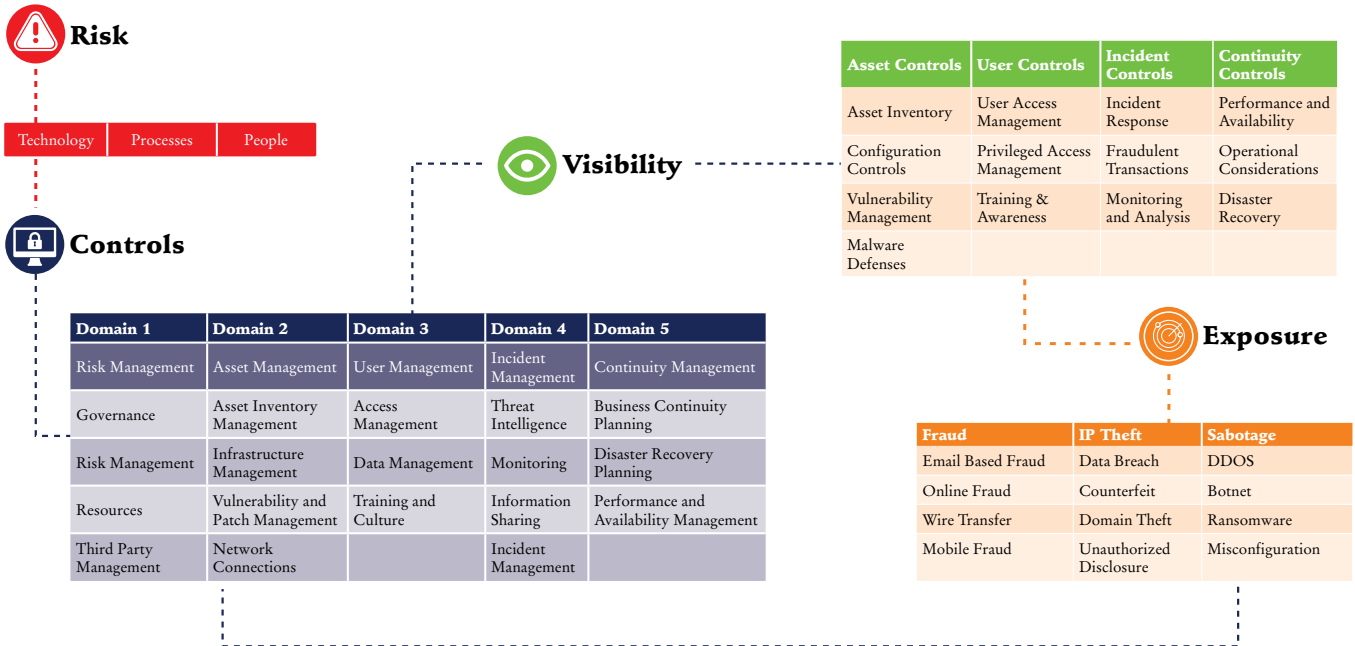
- Inherent Risk Statement
- Maturity Statement
- Visibility Statement
- Deficiency Statement
- Incident Monitoring Statement
- Exposure Statement





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**.



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

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

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



REFERENCES

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

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

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

The Cybersecurity Workforce Gap William Crumpler & James A. Lewis

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

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

CUE. (2018, November). Approved Academic Programmes Offered Universities in Lesotho. 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/usiuafrica-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>



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>

