2018

Africa Cyber Security Report - Botswana

SERIANU

Cyber Security Skills G ap

United States International University-Africa

ISACA Gaborone Chapter

Africa Cyber Immersion Centre acic Engage | Educate | Empower

African Cyber Security Botswana

SERIANU

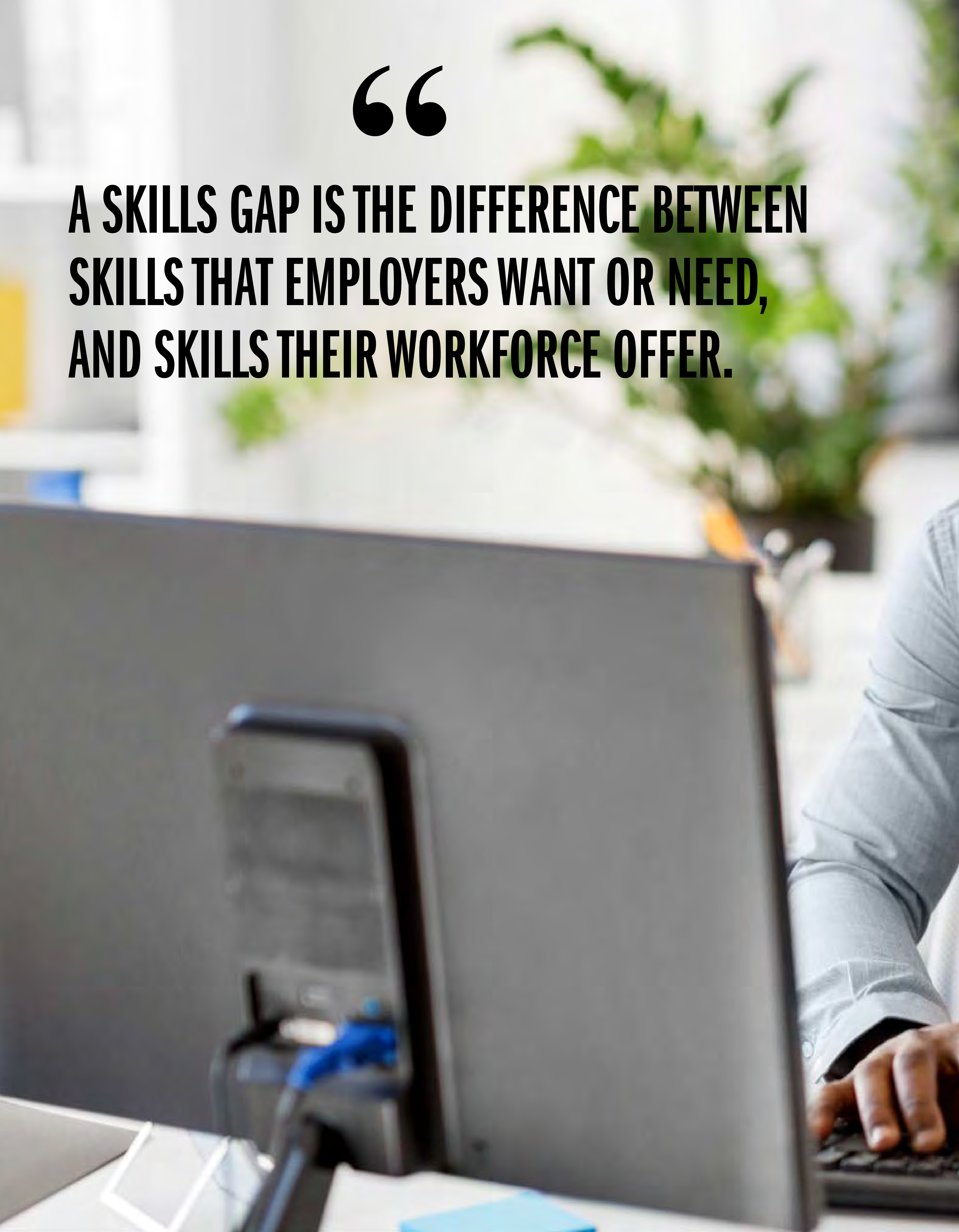
2018

Africa Cyber Security Report - Botswana

Cyber Security Skills Gap

“

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



IN THIS REPORT

EDITOR'S NOTE AND ACKNOWLEDGEMENT

We are extremely pleased to publish the 1st Edition of Botswana 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 Botswana organisations. Our research is broken down into the following key areas:

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

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

Survey Analysis: This section analyses the responses we received from over 150 organisations surveyed within Botswana. It measures the challenges facing Botswana 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 Botswana 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 Botswana organisations and in particular, to gain a better appreciation of the costs to the local economy. We provide an estimate of this cost, which includes direct damage plus post-attack disruption to the normal course of business.

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

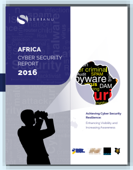
Cyber-risk Visibility and Exposure Quantification Framework (CVEQ Framework): Organisations are now required to quantify their Cyber risk and articulate their Cybersecurity exposures. In this section, we highlights metrics that organisations need to focus on in order to fully quantity, monitor and track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

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

2015

Achieving Enterprise Cyber-resilience Through Situational Awareness

$3tn Cost of cybercrime



2016

Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness

$2b Estimated Cost of Cybercrime in Africa

2017

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 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.
- We also anticipate other industries will rise to the occasion and develop their own specific cyber security guidelines, just as the financial services sector has done.
- Since the skills gap is yet to narrow, outsourcing will continue.

01

DID YOU KNOW?

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

ACKNOWLEDGEMENT

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

USIU AFRICA United States International University-Africa

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

ISACA Gaborone Chapter

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

African Cyber Security

We partnered with African Cyber, a Cybersecurity company focused on offering innovative and holistic Cybersecurity services to organisations. African Cyber provided immense support through research and provision of statistics, survey responses, local intelligence on top issues and trends highlighted in the report.

The Serianu CyberThreat Intelligence Team

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

CO-AUTHORS

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

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

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

Chris Johnson
CEO, African Cyber, Botswana

International Data Corporation (IDC)

Joseph Mathenge
COO, Serianu Limited

Taka Nyahunzvi
President, ISACA-Botswana Chapter

Jaco Viljoen
CEO, First Capital Bank

Emmanuel Thekiso
Information Technology Manager, Botswana Communications Regulatory Authority, BOCRA

Khumo Pule
Managing Director, VAS Group

Dr. Audrey Masizana
Senior Lecturer and Head of Computer Science, University of Botswana

Itumeleng Garebatshabe
CEO of Intellegere Holdings

Senwelo K Modise
Collins Chilisa Consultants

Bungai Muhamu
General Manager, FMRE - Reinsurance

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 Botswana.

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

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

Design, Layout and Production: Tonn Kriation

Disclaimer

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

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

For more information contact:

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

FOREWORD

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

With a rising awareness and understanding of cyber threats, both existing and emerging and with no individual, business or institution being immune; We need to establish multi-stakeholder consortiums that brings together industry, government and academic interests in an effort to improve the state of cyber security on the domestic, regional and international fronts.

As to strive toward the goal of "Knowledge –Based Society" and the aspiration to be a 'High Income Country', we must be aware of the threats and opportunities that Cyber brings. If we up-skill our students and graduates with a collective effort, we have an opportunity to become a regional leader in IT security and create much needed well paid employment.

Throughout the report we highlight the need to raise our level of training, upgrade certifications and even more crucial, build the new talent pipeline by actively skilling high school and technical institute students

Through our responses' to our survey, 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 recent years.

With the passing of the Data Protection Act 2018, this will place an enormous strain on already hard stretched IT departments to implement the appropriate security measures as required by the act. Boards and senior management teams need to assess the impact of this act will have on their operations and have a clear roadmap to ensure compliance with the act.

We estimate that today, Botswana needs at least 1,000 cyber security professionals a year to keep abreast with the number of organisations in need of this critical skill, yet we have observed that each year, just about 20-30 new personnel join the market. In another five years, going by the current rate of technology uptake, we anticipate that the country will need at least 5,000 cyber security professionals.

We urgently need to 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.

With the establishment of 'The Africa Cyber Immersion Centre (ACIC)' this state-of-the-art research, innovation and training facility seeks to address Africa's ongoing and long-term future needs through unique education, training, research, and practical applications, integrating modern, state- of -the -art facilities for on job practical training manned by a pool of highly experienced trainers.

I'm pleased to announce our partnership with Serianu Limited who have now set up offices in Botswana with the the aid of BITC. For the first time in our country, business and organisations will be able to out-source their cyber security to a locally based team of world class cyber professionals.

AS TO STRIVE TOWARD THE GOAL OF "KNOWLEDGE -BASED SOCIETY" AND THE ASPIRATION TO BE A 'HIGH INCOME COUNTRY', WE MUST BE AWARE OF THE THREATS AND OPPORTUNITIES THAT CYBER BRINGS. IF WE UP-SKILL OUR STUDENTS AND GRADUATES AND WITH A COLLECTIVE EFFORT, WE WILL HAVE AN OPPORTUNITY TO BECOME A REGIONAL LEADER IN IT SECURITY AND CREATE MUCH NEEDED WELL PAID EMPLOYMENT.

Chris Johnson
CEO, African Cyber,
Botswana

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

200 Cyber Security Skilled Professionals in Botswana

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 Investments In Information Security

2 Lack of Solid Experience

Increase in organisational spend in cybersecurity in 2017 to 2018

26% of respondents spend above BWP 100,000

$30m cost of cybercrime in Botswana in 2018

97% ↑ Cyber Incidents go unreported or unresolved

5% ↑ successfully prosecuted Cyber crimes

Increased Adoption of Cloud ↑

↑ Increased targeted ATM attacks

↑ Increased Targeted Phishing Attack (Business Email Compromise Attacks)

50% ↑ Increased involvement of Board members on matters cybersecurity

TOP TRENDS FOR 2018

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

MALWARE ATTACKS

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

A close relative of banking malware is crypto mining malware. The rise of Bitcoin and other cryptocurrencies such as Neo, Etheurium etc. took Batswana 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 Batswana 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 Botswana organisations. With the cost of cybercrime increasing every year across Botswana, 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 Botswana - 200 it is clear that businesses are an easy target for both local and international hackers. Some companies in Botswana 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

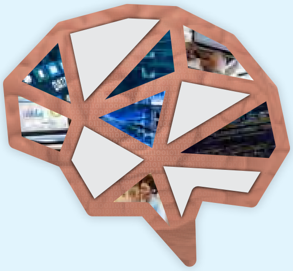
DID YOU KNOW?

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



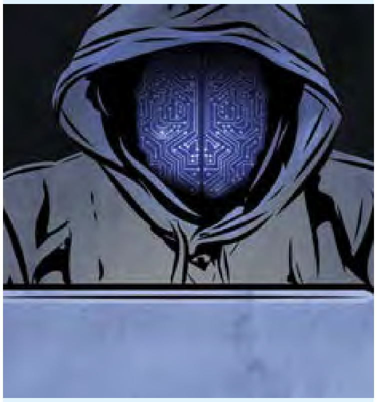
200

Cyber Security Skilled Professionals in Botswana

02

DID YOU KNOW?

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



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

Our analysis also discovered that Botswana 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 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.

INSTANCES OF FAKE NEWS

1

Early September, news spread across different platforms that 87 elephants in Botswana elephant had been killed. However, the government issued a press release calling the story "false and misleading". A physical inspection found just 19 dead elephants, of which six had been killed by poachers.

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

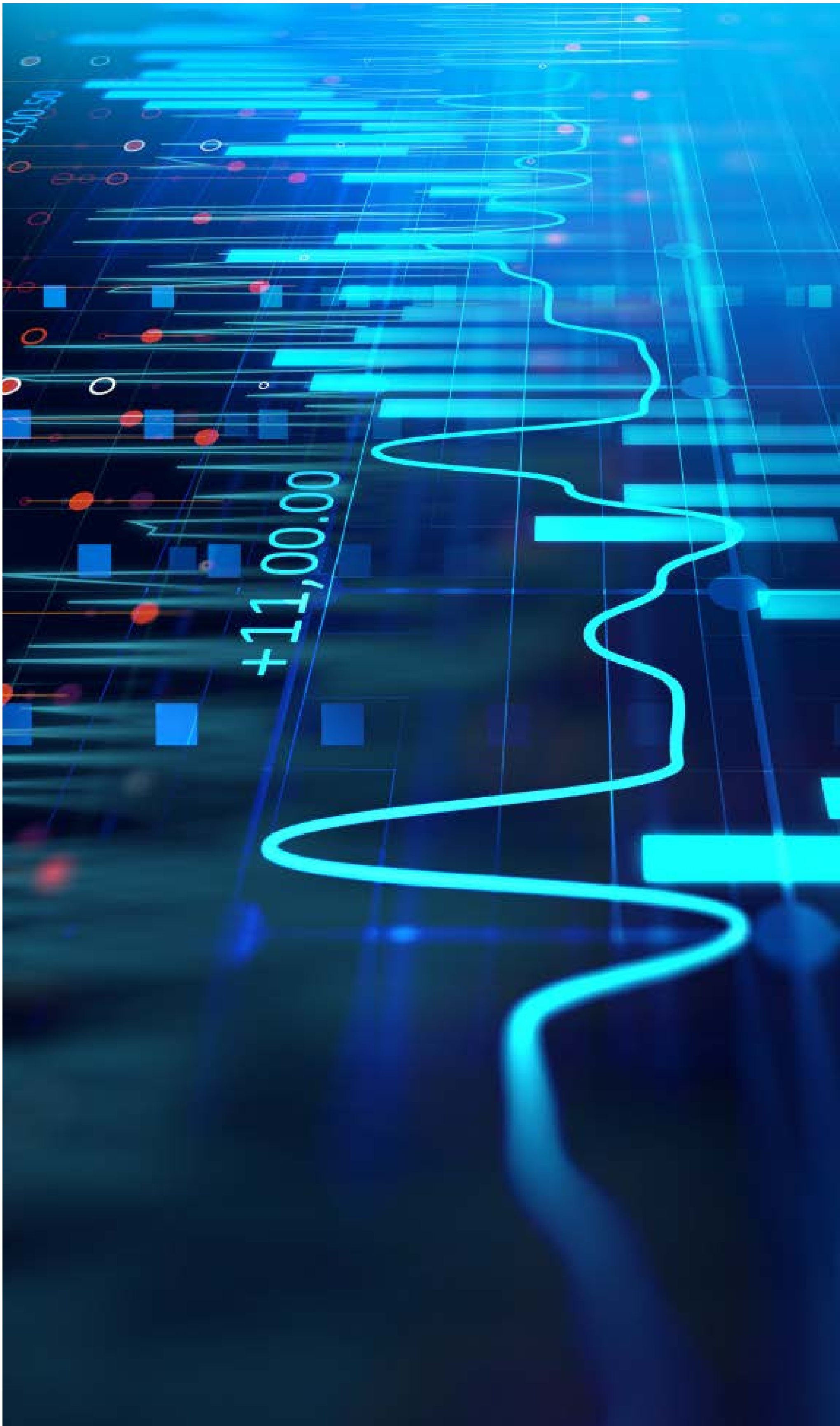
DID YOU KNOW?

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 PERCENT OF THE MEDIA'S COVERAGE OF PRESIDENT TRUMP IS NEGATIVE."A DIRECT CONSEQUENCE OF FAKE NEWS

STATEMENT BY BOTSWANA BANKERS ASSOCIATION



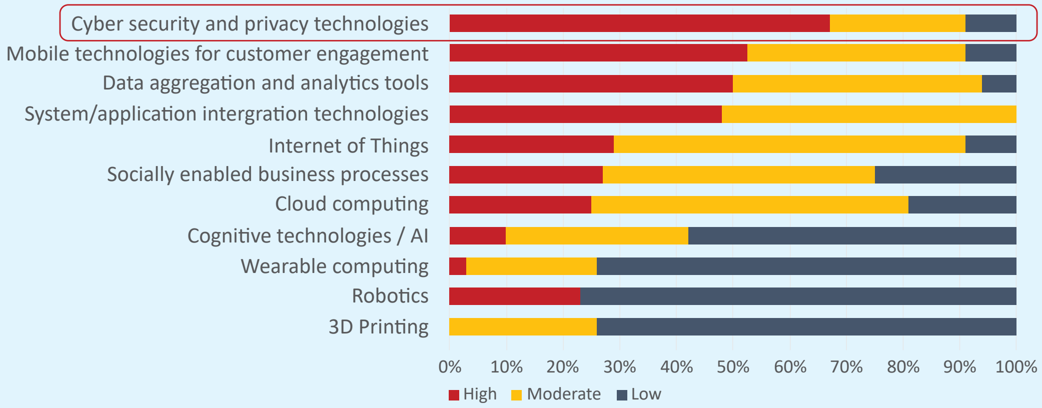
INDUSTRY PLAYER PERSPECTIVE

SUB SAHARAN AFRICA IT SECURITY LANDSCAPE AND TRENDS 2018-2019

SECURITY OUTLOOK 2019

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

CIO PERSPECTIVES OF IT SPENDING AND FOCUS



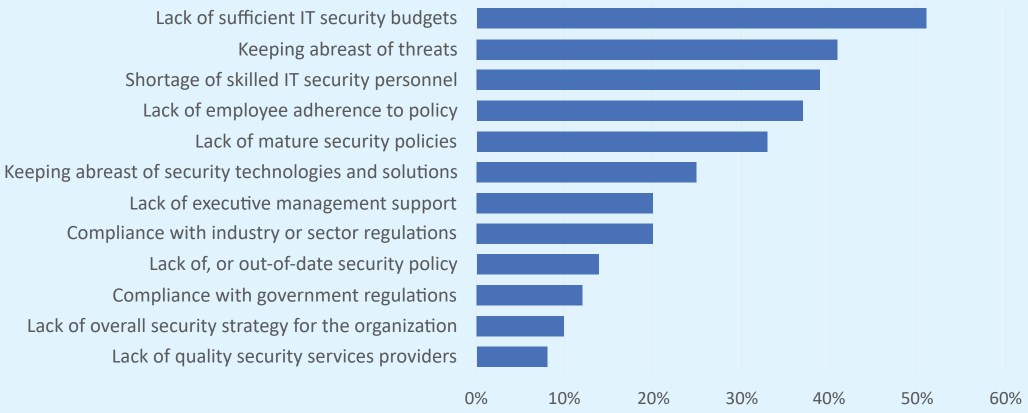
SOURCE 1: IDC

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

Various Dx technologies are hotspots for (in) security:

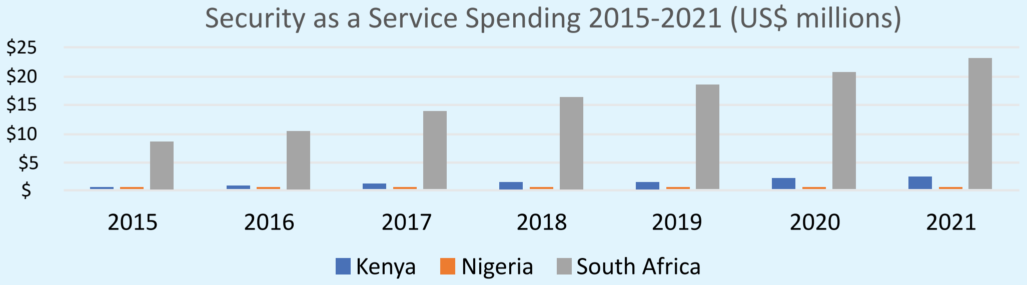
- Cloud (Spectre/Meltdown)
- IoT (auth/poisoning/DoS)
- AI/cognitive (subversion/DoS)
- Shadow IT (leakage/authentication/BC)

CHALLENGES IN MANAGING SECURITY



SOURCE 2: IDC

SECURITY AS A SERVICE SPENDING



SOURCE 3: IDC

- Botswana 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

Communicator

Expert on Security

Trusted Advisor

People Manager

Always Informed

Essential Guidance

Security needs to be at Core of the Transformation Vision

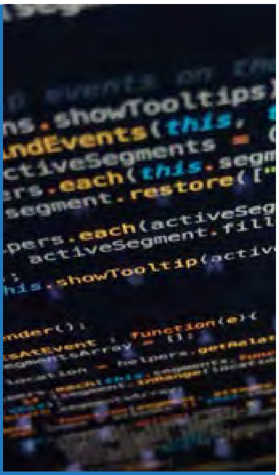
Business needs to fund security and security should be a business problem

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

Increased Stakeholder Management

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

IDC ANALYZE THE FUTURE



ABOUT IDC

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

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

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

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

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

INDUSTRY PLAYER PERSPECTIVE

TAKA NYAHUNZVI

President, ISACA Botswana

WHAT WERE THE BIGGEST TECHNOLOGY AND CYBER SECURITY TRENDS IN BOTSWANA IN THE PAST 12 MONTHS?

Continued adoption and greater awareness respectively.

Particularly in the mobile space, there has been more and more adoption of technology across all sectors of society. Even in the remote villages, there is mobile connectivity, and this has changed the way that the community lives. This is reflected in the way that businesses are gearing their operations towards being able to conduct business online. The country has an average of over two handsets per person, so a lot of effort is geared towards making products and services available on mobile devices.

Although there is still a long way to go, there has also been increased awareness of the dangers that come with living in the online world that we do. Sharing of profiles and of passwords isn't as prevalent as it was a few years ago. National leaders have been actively encouraging digital development. This message should however be tempered with the need for security to be a paramount consideration on this journey.

THE CYBER SECURITY SKILL GAP IN THE COUNTRY IS HUGE, ESPECIALLY IN THE PRIVATE SECTOR. HOW HAS THIS AFFECTED YOU OR THE INDUSTRY AT LARGE? WHAT SHOULD KEY PLAYERS BE FOCUSING ON TO REDUCE THIS GAP?

The focus has traditionally been on audit, with there being not much need for security. This is reflected in our Chapter membership, in which 70% of the certified members hold the CISA certification.

This has made it necessary to import a lot of skills – for system implementations, maintenance and audits. It comes at a great cost to the country as a whole, and in fact opens the possibility of unscrupulous outsiders taking advantage of whatever confidential information they have had access to.

The focus should therefore be on attracting cyber security practitioners by offering such professionals incentives and by encouraging them to develop themselves. At a corporate level, businesses that specialize in that field should be given registration, tax and other incentives to boost them.

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

Yes it does. The Ministry responsible for ICT has over the past year invited key players to its workshops explaining the cybersecurity roadmap, and to take part in the CMM building.

WHAT KEY CYBERSECURITY COMPETENCIES ARE LACKING WITHIN THE PUBLIC SECTOR? WHAT CAN BE DONE TO ENSURE THAT WE ATTRACT YOUNG TALENT WITHIN GOVERNMENT AND PUBLIC SECTOR?

Investigators and practitioners are lacking. The public at large has little confidence in the capacity of the police force to investigate and prosecute cybercrime. As a result, a lot of it goes unreported. Similarly, there are very few people with the skill to conduct a forensic investigation of a malware attack or system hack.

Law makers and regulators should actively encourage and insist on membership of professional bodies and industry certifications as pre-requisites for ICT-related leadership positions. At the moment, people do this because they want to and not because they have to.

WHICH CYBER SECURITY AREA DO YOU THINK REQUIRES URGENT ATTENTION FROM KEY STAKEHOLDERS: FORENSICS AND INVESTIGATIONS, OPERATIONS AND MONITORING, ASSESSMENTS AND CYBER DEFENSE; RISK AND COMPLIANCE; AUDIT AND ASSURANCE OR RESEARCH AND INNOVATION?

Operations and monitoring cuts across the whole spectrum of people, so should get the most attention. Once the entire user (i.e. operations) and support (i.e. monitoring) base has the right basic habits, the likelihood of elementary lapses occurring will be greatly reduced.

Many things can be automated to help close gaps, but the people at the very end of the chain are the ones most likely to break the system so should be the main focus.

WHICH ONE OF THE FOLLOWING KEY STAKEHOLDERS NEED TO TAKE THE LEAD IN THE CYBER SECURITY DISCUSSION AND IMPLEMENTATION? JUDICIARY, EXECUTIVE, LEGISLATIVE, PRIVATE SECTOR, ACADEMIA OR NATIONAL INTELLIGENCE, MILITARY?

As the people more exposed to its entire spectrum of strengths, weaknesses, opportunities and threats, I feel that the academia and national intelligence should take this lead. This group is best placed to show how the online world completely levels the playing field, making any organisation have the same reach as the next. More than that though, they will be aware of global trends that could just as easily take down not just a company, but an entire industry or even the backbone of a nation due to security vulnerabilities in one organisation.

CURRENTLY THE COUNTRY HAS A NUMBER OF REGULATIONS TO ADDRESS CYBER SECURITY/CRIME IN GENERAL – DATA PROTECTION BILL, ELECTRONIC EVIDENCE BILL AND CYBER CRIME ACT – DO YOU THINK THIS IS SUFFICIENT? IN OTHER COUNTRIES WE HAVE NOTED A NUMBER OF INDUSTRY REGULATORS SETTING UP SECTOR SPECIFIC REGULATORY FRAMEWORK. HOW COME THIS IS NOT THE CASE IN BOTSWANA?

It wouldn't be beneficial to introduce a raft of legislation before the country is ready for it. This is from the angle of both the legislators also the general population. Those making the laws must understand what they are enacting, and the law enforcement agents should also understand what they are supposed to uphold and how to enforce and investigate it. This is a gradual process which although moving slowly is gathering pace.

Sector-specific regulations are definitely lagging behind when compared to other jurisdictions. In the same way that accountants, auditors, engineers and other groups have their professional bodies with compulsory membership, the ICT sector should have a similar requirement in place to ensure that proper ethical and governance standards are adhered to.

OUR CURRENT EDUCATION/ACADEMIC CURRICULUM DOES NOT ADDRESS CYBER SECURITY TRAINING. WHAT HAVE YOU IN YOUR CAPACITY AS THE ISACA BOTSWANA DONE TO CURB THE ISSUE OF CYBER SECURITY SKILL GAP FROM GRADUATES?

In 2017, we as a Chapter held a two-day cybersecurity essentials workshop for fourth year students at the University of Botswana. We went on to offer sponsorship for the writing of the CSX Fundamentals exam to any student who achieved a certain grade in the end-of-workshop quiz, and thereafter sponsored one student to write the exam – which she passed.

We will be hosting this as a bi-annual event, and will be working with other educational institutions as well.

SURVEY ANALYSIS

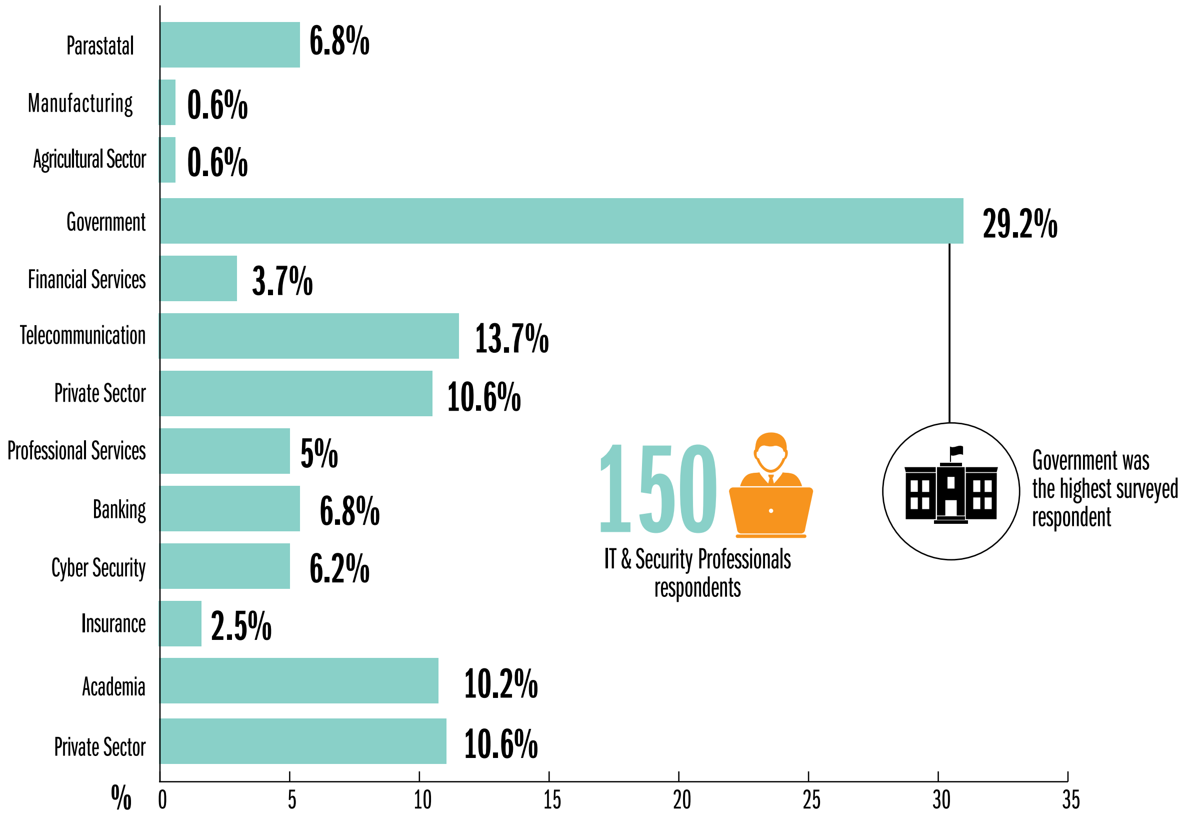
The 2018 Cybersecurity Survey provides insight into what Botswana organisations are doing to protect their information and assets, in light of increasing cyber-attacks and compromises impacting them.

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

RESPONDENTS PROFILE

INDUSTRIES SURVEYED

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



GRAPH 1: INDUSTRIES SURVEYED.

BYOD, CLOUD AND IOT

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

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

CHART 1: BYOD USAGE.

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

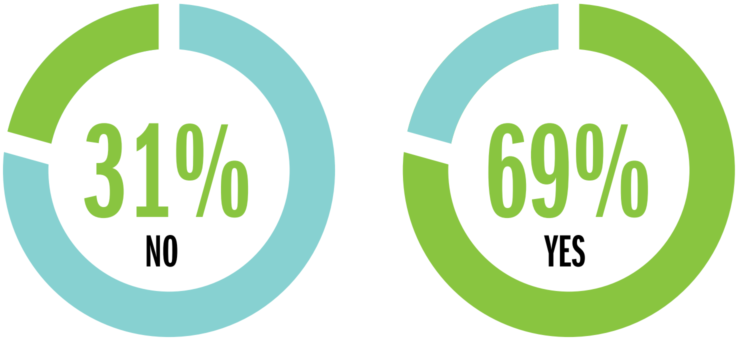
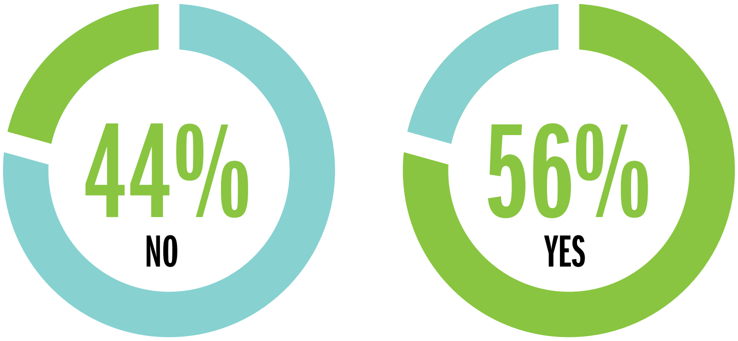


CHART 2: CLOUD SERVICES/ IOT USAGE.

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



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

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

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

BYOD, CLOUD POLICIES

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

CHART 3: BYOD POLICY

Does your organisation have a best practice policy for BYOD?

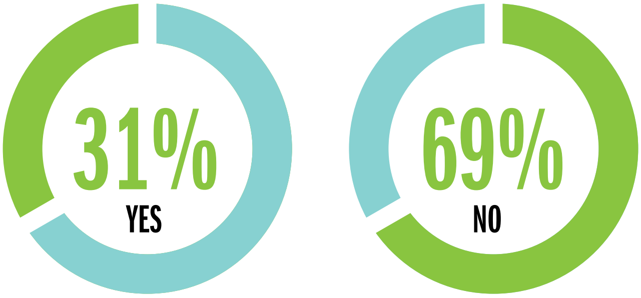
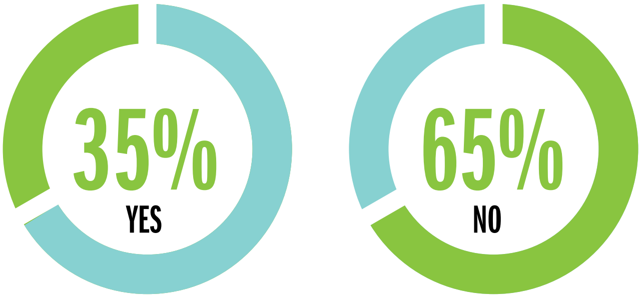


CHART 4: IOT AND CLOUD SERVICES BEST PRACTICE

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



BYOD/IoT present the following challenges:

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

Key challenges in integrating data sources

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

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

RECOMMENDATIONS

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

04

DID YOU KNOW?

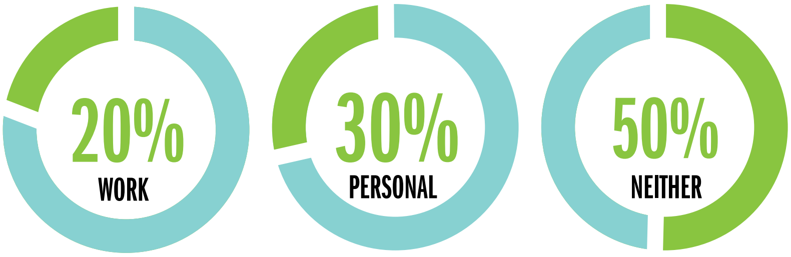
ATTACKERS ARE TAKING ADVANTAGE OF THE INCREASED USE AND LACK OF MONITORING OF PERSONAL DEVICES WITHIN ORGANISATIONS TO INTRODUCE ROGUE DEVICES THAT ARE THEN USED TO COMPROMISE THE NETWORK.

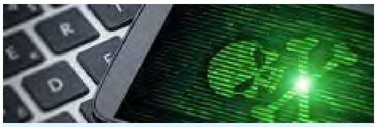
CYBER CRIME

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

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

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





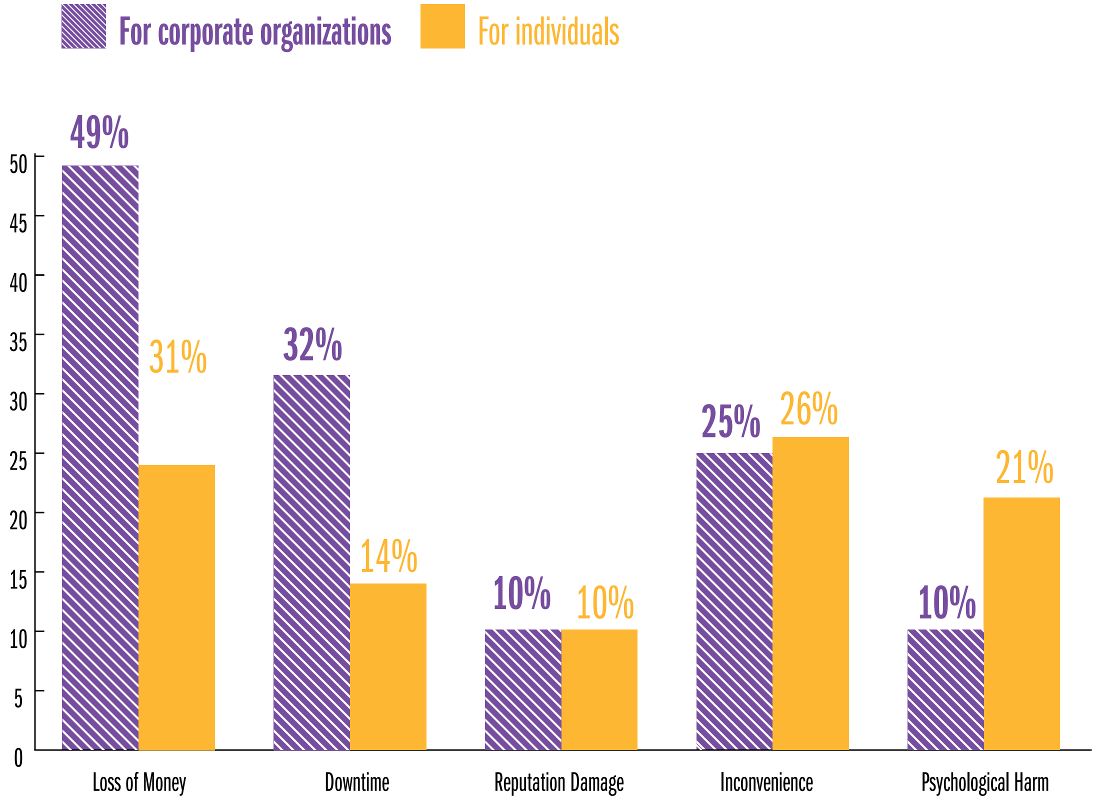
> ON AVERAGE, ORGANISATIONS VICTIMIZED BY CEO FRAUD ATTACKS LOSE BETWEEN $25,000 AND $75,000.
>
> FBI ALERT 2016

WHY YOU ARE A TARGET

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

IMPACT OF CYBER CRIME

When asked about the business impact of cybercrime, loss of money, system downtime and reputation damage were highlighted as having the biggest impact for corporates. Inconvenience and Psychological harm were the biggest impact for Individuals.



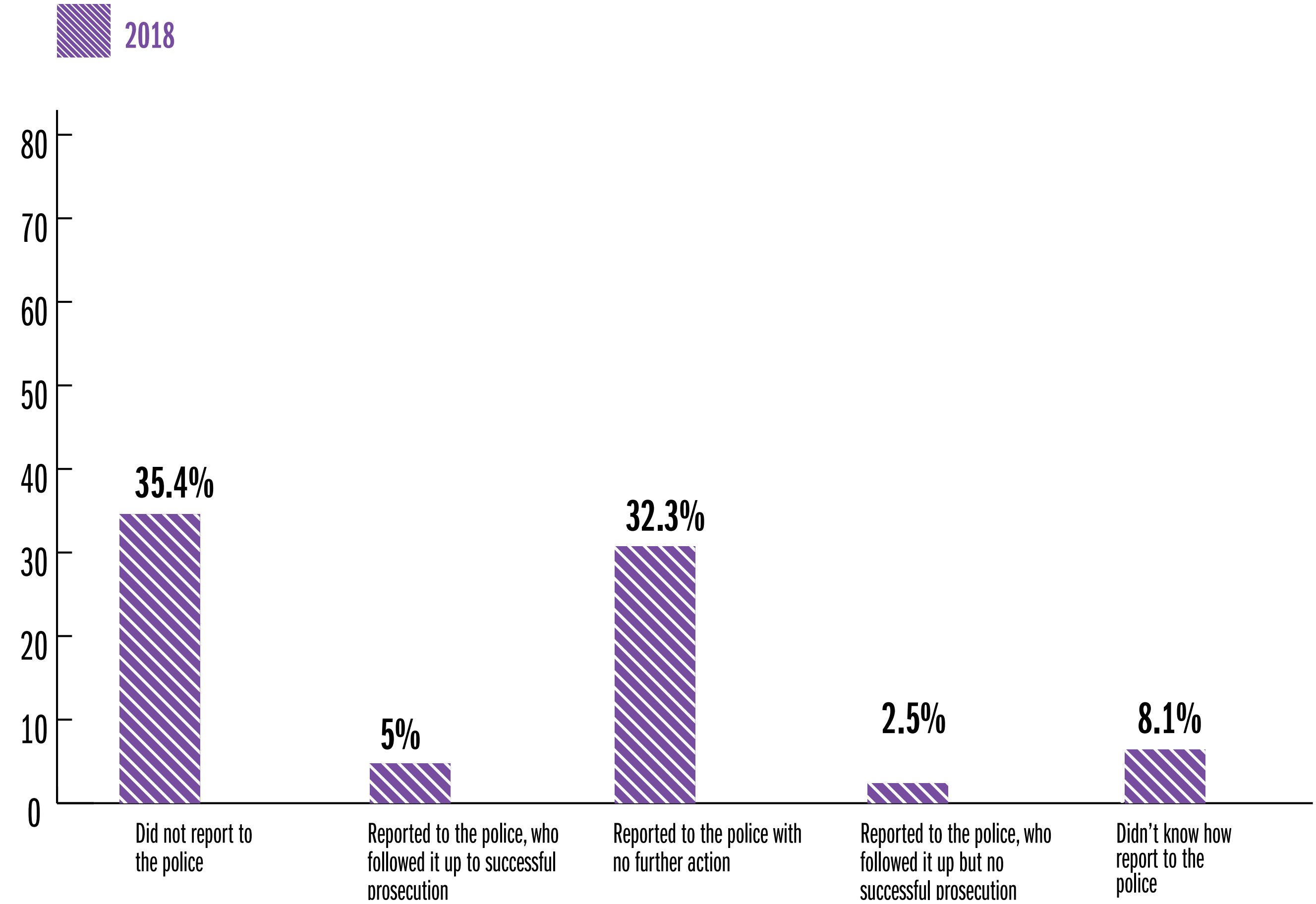
GRAPH 2: IMPACTS OF CYBERCRIME: CORPORATE VS INDIVIDUALS.

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?



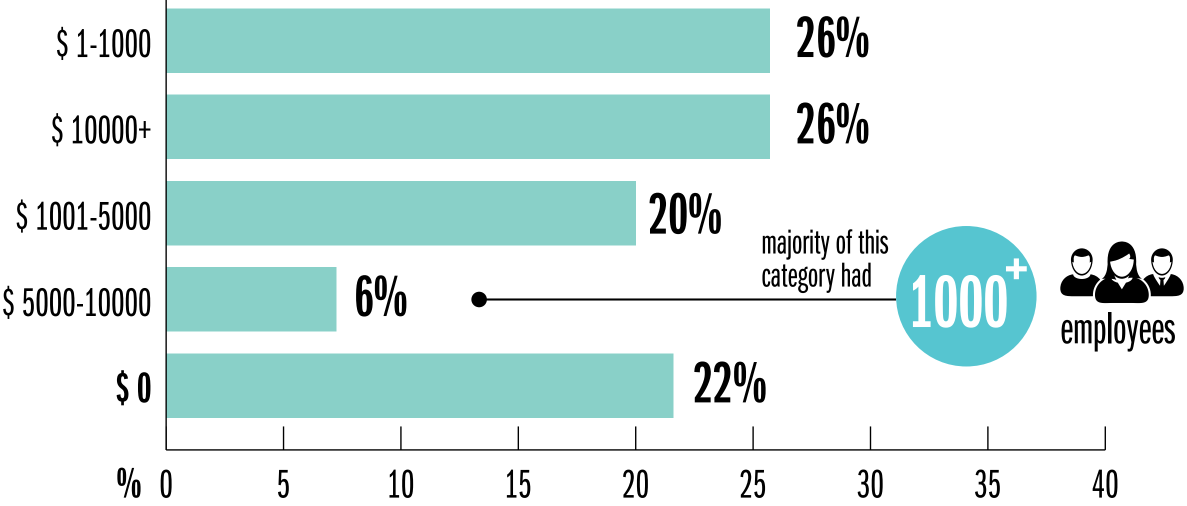
GRAPH 3: REPORTING OF CYBERCRIME .

- 35% of cyber-crime that happens in Botswana end up unreported to the police and 33% of those that were reported to the police, no further action was taken
- 5% in the number of successfully prosecuted Cybersecurity incidents.

CYBER SECURITY SPENDING

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

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

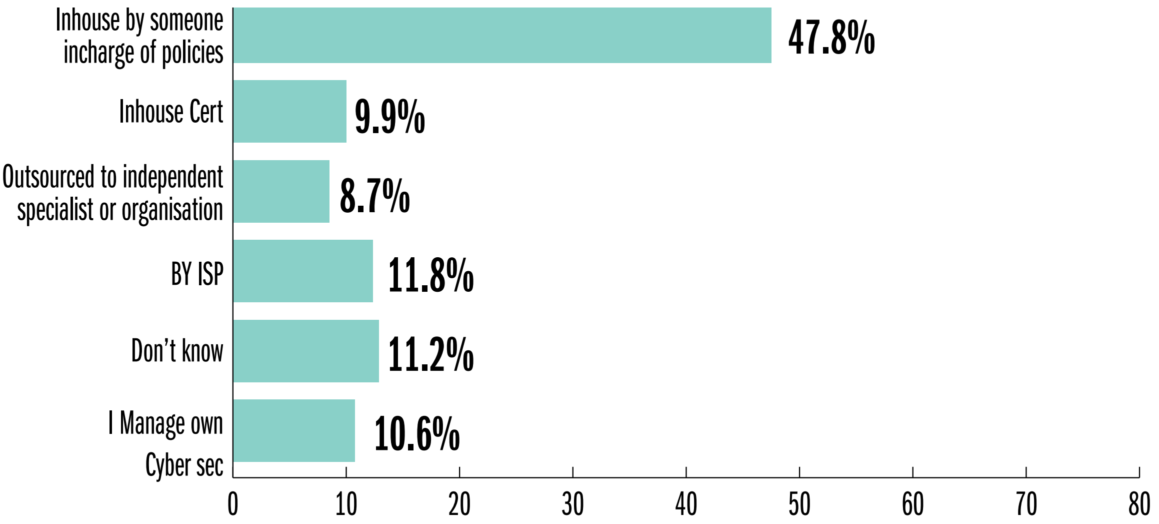


GRAPH 4: CYBERSECURITY SPEND.

MANAGING CYBER SECURITY

68% of organisations manage their cyber security inhouse while 20.5% have oursourced these services to an external party (MSSP or ISP). More companies are now developing inhouse capabilities to manage cyber security, this is the case with Banking, Saccos and financial institutions.

HOW IS YOUR ORGANISATION'S CYBER SECURITY MANAGED?

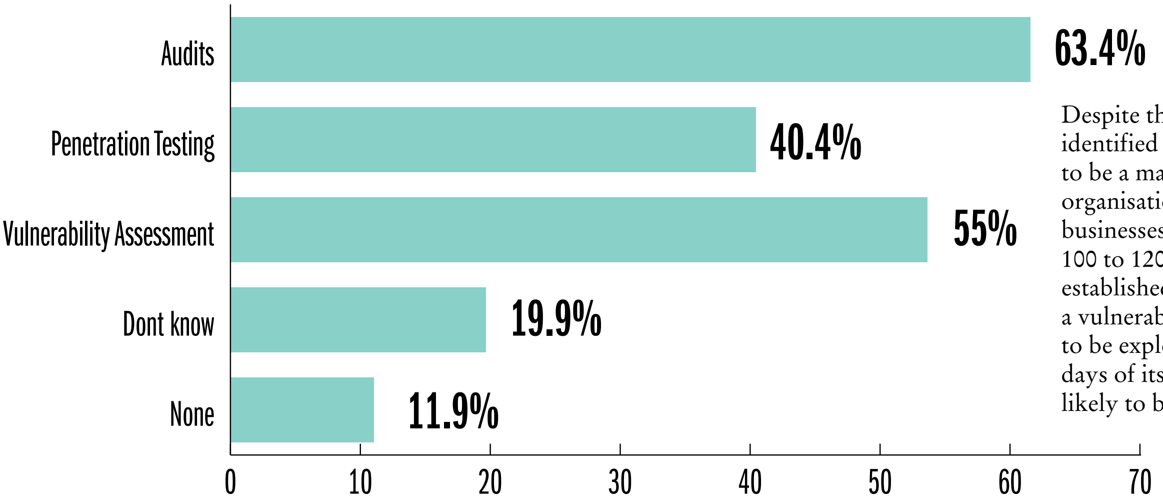


GRAPH 5: CYBERSECURITY MANAGEMENT.

CYBER SECURITY TESTING TECHNIQUES

Security testing is a process that is performed with the intention of revealing flaws in security mechanisms and finding the vulnerabilities or weaknesses in the environment. Recent security breaches of systems underscore the importance of ensuring that your security testing efforts are up to date. From the survey, 63% of respondents perform audits. 40% perform penetration testing while 55% perform Vulnerability Assessment. All these testing techniques work best when applied concurrently.

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



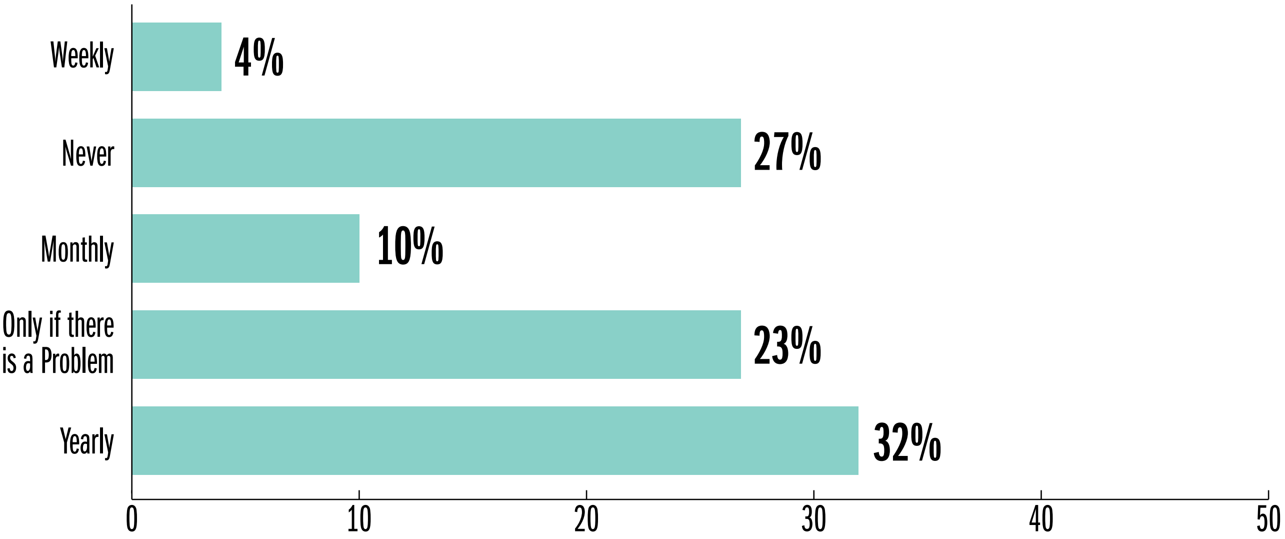
Despite these statistics, fixing identified gaps was found to be a major challenge for organisations. On average, businesses took between 100 to 120 days to fix an established vulnerability. Yet, a vulnerability is most likely to be exploited in the first 60 days of its release — and 90% likely to be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

GRAPH 6: SECURITY TESTING TECHNIQUES.

CYBER SECURITY AWARENESS

The level of cybersecurity awareness in Botswana is still low with 27% of organisations not having an established cyber security training program. Most organisations (23%) are also still very reactive when it comes to cyber security training, these organisations train their staff only when there is an incident or problem. This is worrying considering 20% of all cyber attacks reported in the survey was through work. Having said that, important to point out that 46% of respondents reported to have a regular training program in place. The importance of having regular security training for employees cannot be over emphasised.

HOW OFTEN ARE STAFF TRAINED ON CYBERSECURITY RISKS?



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

EMMANUEL THEKISO

Information Technology Manager, Botswana Communications Regulatory Authority, BOCRA

“

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

- The arrival and availability of new technologies, such as Internet of Things (IoT) is enabling operators to address new opportunities in industrial and consumer markets.
- The variety and quality of services from telecom companies and internet service providers (ISP) are increasing;
- Profit margins are decreasing;
- Billing becoming increasingly complex, provisioning and assurance, fraud management
- the lines between telecom companies and technology vendors are blurring.
- Competition from Over the Top services and Internet of things (other new Technologies);
- decline in revenue and lot of pressure on telcos to develop a converged platform that is sufficiently functional to support the full weight of the IoT;
- Operators have spent years facing the dual challenges of spiraling data traffic volumes and intense competition leading to pressure on pricing, which has taken a massive toll on profitability.
- New technology requires more bandwidth. Examples 5G is just requires increased network efficiency and the potential to offer high-value, differentiated services to enterprises and consumers.
- Massive volumes of data from multiple sources;
- Quality of services from telecom companies and internet service providers (ISP) are increasing

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

- Telecoms Companies must take a fresh look at the level of ICT innovation and adapt their organisation to digital transformation by creating strong cross-functional interfaces and seeking tools for maintaining organisational flexibility.
- Telecommunication providers need to upgrade their IT and connectivity infrastructure and focus on providing data and voice services that are high quality, reliable, and affordable.
- Security of the networks has become a major priority for the telcos and they are facing challenges with the emergence of new threats that are powered by new technologies.
- Telecoms’ companies must Create a focused offering, with clear positioning, well-defined value proposition, and a carefully targeted customer segment. Such an offering should rely on standardized IT products and services and existing platforms where possible.
- Develop platform-based solutions in disruptive technology areas that are close to the core business.
- Telecom companies should also consider how to derive additional value from their existing assets and competitive advantages.
- Minimize costs in production and delivery by using automated and “low touch” processes to avoid building in extensive personnel requirements and increasing speed to market with a product that is not fully integrated in existing legacy systems and potentially running on a separate infrastructure.

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

- No Information reported on Swim Swap in 2018

WHAT NEW INITIATIVES HAVE DEVELOPED IN THE TELCO SECTOR OVER THE LAST 3 YEARS? (5G ETC) HAVE THESE BEEN TARGETED BY ATTACKERS RECENTLY?

- Network upgrades. fiber and 4G upgrades or other networking technologies
- Infrastructure, sufficiently flexible to handle new and profitable monetization opportunities.
- Network enhancements to take back the technological advantage from OTT providers.

HOW CAN CONSUMERS OF TELCO PRODUCTS SUCH AS ROUTERS SECURE THEMSELVES FROM EXPLOITATION OF VULNERABILITIES WITHIN THESE DEVICES?

- Service misconfiguration: In many cases, the hardware used by the telecommunications industry carries configuration interfaces that can be accessed openly via HTTP, SSH, FTP or telnet. This means that if the firewall or router is not configured correctly, the hardware in question becomes an easy target for unauthorized access. Dangers of wireless routers are real.

- Hackers could easily be using your router to conduct many types of malicious attacks, like sending harmful spam to unsuspecting victims or using phishing sites to steal passwords, if the routers do not update themselves.
- Another thing these hackers can do with someone else's router is conduct DDoS attacks, which are simply "distributed denial of service" problems that happen when a bunch of computing devices are taken over and used in concert to send massive amounts of data to a server or an internet access point, more than it can handle.

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

- Regulation : While the company may pursue unregulated business opportunities, telecom service provisioning remains a highly regulated enterprise.
- Market Intelligence : Tech-savvy consumers expect more from their service providers than ever before – more bandwidth, more applications support, better service quality, superior customer support
- Senior leaders need to keep their fingers on the pulse of the market forces that impact their current and future success. They need to stay abreast of federal regulation and legislative priorities to assess the impact on their service offerings, profitability and sources of funds.
- They need a grass roots understanding of their customers' evolving needs and preferences to plan for future product and service offerings and ward off competitive incursions.
- Financial Expertise: Market intelligence goes hand-in-hand with strong financial management skills. Strategic investments in new or existing businesses require a detailed understanding of the underlying economics.
- Technology Knowledge : Today's executive must have personal knowledge of the sea of technology deployed in the modern communications network and the bench strength to provide that level of expertise.Multi-Generational Organisational Skills

Q) Analytical Skills : Despite the need to evolve with changing environments, astute executives continue to render dispassionate assessments of all new business opportunities. Market demand for new products and services as well as the competitive in which they will be offered.

Financial stability of the affected entities and the impact of the new venture.

Emerging leaders make sure their organisations have the right internal control systems and data analytics capability to manage their operations efficiently and effectively. They define performance metrics consistent with their business strategy and use them to make tactical adjustments, as needed. They also take cybersecurity very seriously and institute the appropriate protections and processes to minimize their risk of attack.

The ever-changing landscape of communications poses a challenge for many organisations, but when addressed with the right capabilities, these challenges become opportunities for growth. By excelling in the competencies above, organisations can stay relevant and become an example of next generation leadership in their industry.

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

The top threats from both sides include:

- Social engineering, phishing or malware aimed at subscribers
- Distributed Denial of Service (DDoS) attacks
- Insider threats
- Exploitation of vulnerabilities within network and consumer devices
- Credit card and identity theft
- Service interruption
- Website damage
- Loss of reputation: If a major network is unavailable, a telecom provider is unable to operate, and brand reputation suffers. Further, the compromise of sensitive employee and customer data can put valuable relationships at risk.

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

Botswana laws such as Cyber Crime and Computer related needs to be alone updated and aligned with EU Convention and Malabo Convention. Botswana should introduce laws which specifically which deals with cybercrime.
More cybersecurity professionals should be developed. More research on cybersecurity.

WHAT ARE YOUR EXPECTATIONS FOR 2018?

- Introduction of latest technology such 5G.
- Improved bandwidth
- Improved quality of service
- Companies in this turbulent sector must address the risks and disruptive potential of their products and services.

COST OF CYBERCRIME IN BOTSWANA

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.

P300m
estimated cost of cybercrime

Direct Cost
$10m

Indirect Costs
$20m

MOST AFFECTED INDUSTRIES

1. Banking
2. Public Sector
3. Microfinance
4. Hospitality and Retail
5. Others

DIRECT AND INDIRECT 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)	6,232,450.00	• SIEM • Network Access Controls • IPS/IDS • Active Directory • Vulnerability Management • Solutions • PAM • Antivirus • HIDS • Proxy • WAF • Load Balancer	• Penetration Testing • Audit • Forensic Investigations • Risk Assessment • Compliance Review • Post-Implementation • Review • BCP/DR Testing and • Review	• General Awareness Training • Technical Training • Board Training • Business Managers • Training
Public Sector (Utilities)	5,777,235.00			
Service Providers (Telcos, Fin-tech, and Financial apps)	4,648,915.00			
Manufacturing, Healthcare, Hospitality and Retail	677,965.00			
Others	2,663,435.00			

Total Indirect Cost is $20,00,000.00

DIRECT COSTS	Estimated Direct Cost (USD)	Activities
Financial Services (Banking, Insurance, Saccos and MFI)	3,163,835.00	• Data hijacking (ransomware attack) • Money lost • Fines from regulators • Law suits • Claims and Cyber Insurance • Forensic Investigations
Public Sector	2,881,335.00	
Service Providers (Telcos, Fin-tech, Betting, Financial apps)	2,259,915.00	
Manufacturing, Healthcare, Hospitality and Retail	339,000.00	
Others	1,355,915.00	

Direct Costs is $10,000,000.00

INDUSTRY PLAYER PERSPECTIVE

JACO VILJOEN

CEO, First Capital Bank

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

There are many challenges facing the banking sector in Botswana. The cost of technology is one of them and coupled with that IT security.

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

General awareness about cyber security amongst staff and customers alike is perhaps one of the most important initiatives that can reduce the risk. Banks specifically should of course ensure that their IT security is up to date and continuously spend money on monitoring and improvements.

THERE WERE MANY REPORTED CASES OF ATM ATTACKS IN 2018, WHY IS THIS?

My personal view is that the man/woman on the street is too trusting and not aware of the risks using an ATM. The thieves are aware of this and therefore started targeting Botswana.

HOW CAN BANKS SECURE THESE INFRASTRUCTURES?

There are many things to be done. It starts with awareness and monitoring. Furthermore the latest IT security software, firewalls, etc is critical.

WHAT INITIATIVES HAVE DEVELOPED IN THE BANKING SECTOR OVER THE LAST 3 YEARS? (VIRTUAL BANKING, E-WALLET, BITCOINS, MOBILE APPLICATIONS ETC)

The biggest initiatives was linked to electronic banking, specifically using cellphones to make payments.

HOW WILL CRYPTOCURRENCY AFFECT THE BANKING SECTOR?

I think all currencies will ultimately become cryptocurrencies. For now it actually assists “ethical” banking since there is a perception that cryptocurrency is used for money laundering.

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

I think a lot of focus goes towards securing the core banking systems, which is correct; but I believe more focus should be given to the areas where payment systems interface with the core banking systems, for example POS payments.

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

What is the typical organisation structure for Cybersecurity in banking sector?

The banking sector needs specialists for information security. Most banks rely on their groups to support given the cost and complexity to replicate the competencies in each country.

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

Attacks on banks moved away from cash to electronic cash. All technology in Banks are therefore under threat. Payment systems are perhaps under threat the most, including local and foreign payment systems.

HOW DO THE LOCAL LAWS AND REGULATIONS ADDRESS THE ISSUE OF CYBER SECURITY IN THE BANKING SECTOR? (ORG STRUCTURE/ROLES AND RESPONSIBILITIES, TECHNOLOGIES, TRAINING,) WHAT WOULD YOU RECOMMEND?

The laws are outdated to the best of my knowledge and need to be updated since it is difficult to prosecute someone who stole money electronically.

WHAT WAS THE BIGGEST ATTACK (LOCALLY OR GLOBALLY) IN YOUR INDUSTRY? WHAT KEY LEARNINGS DID YOU DRAW FROM IT?

One of the challenges is that attacks are not shared. This is most probably due to the fear of shame. Attacks happen fairly regular though, even in Botswana. My key learning from attacks in Botswana the past five years is that support is available to resolve and fix it fairly easy and the sooner you report it the less the losses are.

WHAT ARE YOUR EXPECTATIONS FOR 2019?

I hope that the Country will prosper and that the Banking industry will be able to assist in that growth.

INDUSTRY PLAYER PERSPECTIVE

KHUMO PULE

Managing Director, VAS Group

WHAT WERE THE BIGGEST TECHNOLOGY AND CYBER SECURITY TRENDS IN BOTSWANA IN THE PAST 12 MONTHS?

On the technology side we have seen remarkable growth in the national fibre infrastructure, which translates to a lot of businesses and hoseholds using fibre for their internet needs. For the cyber security part, the biggest cyber security trend has been a crisis in security talent, as cyber-crime increases, so does the demand for security professionals.

THE CYBER SECURITY SKILL GAP IN THE COUNTRY IS HUGE, ESPECIALLY IN THE PRIVATE SECTOR. HOW HAS THIS AFFECTED YOU OR THE INDUSTRY AT LARGE? WHAT SHOULD KEY PLAYERS BE FOCUSING ON TO REDUCE THIS GAP?

The issue of skill gap in cyber security has had a huge impact on the country's cybersecurity maturity including the ability to detect security breaches / respond to security breaches effectively and efficiently, this goes for both the private and the public sector. There has been one too many significant breaches, majority of which resulted in massive financial losses and loss of sensitive customer data.

Key players should be focusing on capacity building in this space, especially in an era where as a country we are transitioning to a knowledge-based economy.

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

The Government does engage the private sector and academia in its cybersecurity work through inclusion in their workshops and seminars, albeit more often than not, the Government fails to provide information/ updates on progress on cybersecurity initiatives.

WHAT KEY CYBERSECURITY COMPETENCIES ARE LACKING WITHIN THE PUBLIC SECTOR? WHAT CAN BE DONE TO ENSURE THAT WE ATTRACT YOUNG TALENT WITHIN GOVERNMENT AND PUBLIC SECTOR?

Both Technical and Cyber Risk Management competencies lack within the public sector, but more of Technical. A lot of practical education 'hands-on learning programmes' could generate massive interest amongst the young generation.

WHICH CYBER SECURITY AREA DO YOU THINK REQUIRES URGENT ATTENTION FROM KEY STAKEHOLDERS: FORENSICS AND INVESTIGATIONS, OPERATIONS AND MONITORING, ASSESSMENTS AND CYBER DEFENSE; RISK AND COMPLIANCE; AUDIT AND ASSURANCE OR RESEARCH AND INNOVATION?

Assessments and cyber defense

WHICH ONE OF THE FOLLOWING KEY STAKEHOLDERS NEED TO TAKE THE LEAD IN THE CYBER SECURITY DISCUSSION AND IMPLEMENTATION? JUDICIARY, EXECUTIVE, LEGISLATIVE, PRIVATE SECTOR, ACADEMIA OR NATIONAL INTELLIGENCE, MILITARY?

Legislature, and have the rest follow

CURRENTLY THE COUNTRY HAS A NUMBER OF REGULATIONS TO ADDRESS CYBER SECURITY/CRIME IN GENERAL – DATA PROTECTION BILL, ELECTRONIC EVIDENCE BILL AND CYBER CRIME ACT – DO YOU THINK THIS IS SUFFICIENT? IN OTHER COUNTRIES WE HAVE NOTED A NUMBER OF INDUSTRY REGULATORS SETTING UP SECTOR SPECIFIC REGULATORY FRAMEWORK. HOW COME THIS IS NOT THE CASE IN BOTSWANA?

As a starting point, these acts/ bills could be said to be sufficient if they were implemented, with supporting structures and the like. In my opinion, it's better to ensure implementation/ enforcement of passed acts/ bills before considering addition of any work and/or effort

OUR CURRENT EDUCATION/ACADEMIC CURRICULUM DOES NOT ADDRESS CYBER SECURITY TRAINING. WHAT HAVE YOU IN YOUR CAPACITY AS A MANAGING DIRECTOR OF A BUSINESS IN THE CYBER SPACE DONE TO CURB THE ISSUE OF CYBER SECURITY SKILL GAP FROM GRADUATES?

As a training and consultancy institute, we are currently working on developing 'job-readiness' short learning programmes for graduates and soon to graduate scholars.

CYBER SECURITY SKILLS GAP

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

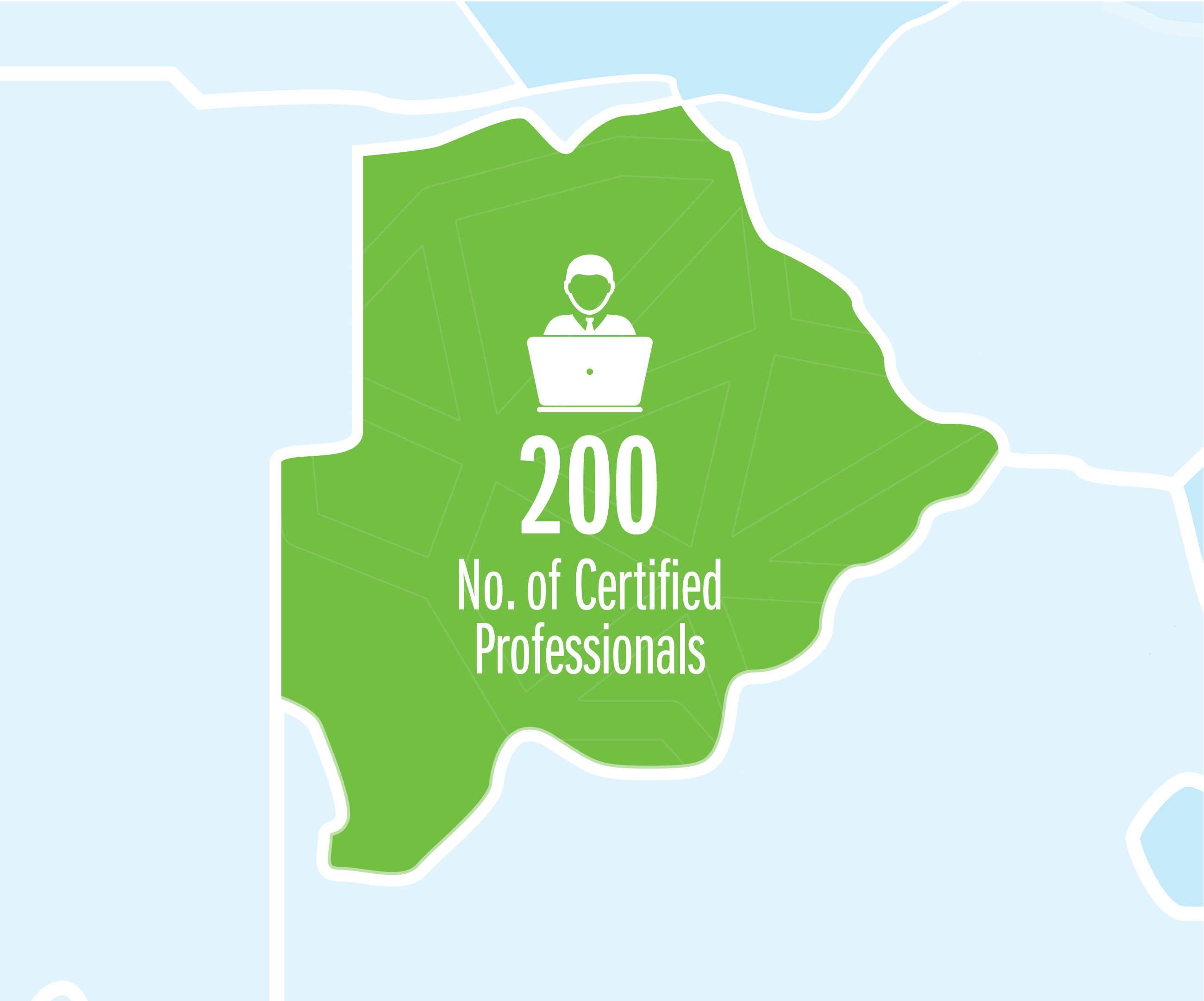
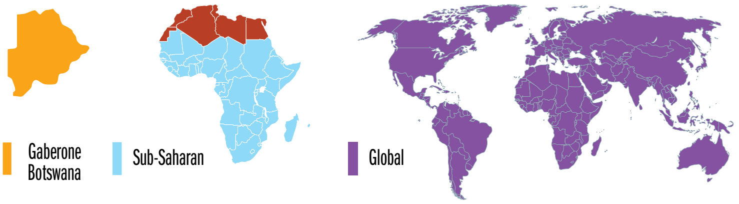


FIGURE 1: OBIS QUAS ACERCHILIT FUGITAE CUM VOLE.

No. of Skilled Professionals in 2018



		Gaberone Botswana	Sub-Saharan	Global
ISACA® Trust in, and value from, information systems	CISA Certified Information Systems Auditor	61	3795	84,484
	CRISC Certified in Risk and Information Systems Control	9	646	19,163
	CISM Certified Information Security Manager	13	945	32,233
	CGEIT Certified in the Governance of Enterprise IT +Others	3	324	5749
(ISC)²	CISSP Certified Information Systems Security Professional	9	844	*
CEH Certified Ethical Hacker CompTIA	CHFI Computer Hacking Forensic Investigator Offensive Security OSCP CCNP Cisco Certified OTHERS	151	6554	*
	TOTAL	250	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.

INDUSTRY PLAYER PERSPECTIVE

ITUMELENG GAREBATSHABE

CEO, Intellegere Holdings

WHAT WERE THE BIGGEST TECHNOLOGY AND CYBER SECURITY TRENDS IN BOTSWANA IN THE PAST 12 MONTHS?

Beyond the international trends such as data privacy and cloud security, Botswana relatively doesn't have a lot of trends because of the growing number of people using the internet. Some trends mostly related to consumers has been issues of cyber fraud and cyber bullying.

THE CYBER SECURITY SKILL GAP IN THE COUNTRY IS HUGE, ESPECIALLY IN THE PRIVATE SECTOR. HOW HAS THIS AFFECTED YOU OR THE INDUSTRY AT LARGE? WHAT SHOULD KEY PLAYERS BE FOCUSING ON TO REDUCE THIS GAP?

The skills gap as adversely affected the industry by not being able to resolve cyber-crime activities well in time especially looking at law enforcement and other stakeholders. Because of the skills gap majority of companies both SMEs and Corporate operate with high risk of attacks. Institutions need to provide the market with versatile graduates who have a practical grasp of Cyber Security. Companies also need to invest in up skilling their personnel to be more cyber aware.

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

Am not sure about Academia but from private sector perspective there is no engagement on cyber issues from government at all.

WHAT KEY CYBERSECURITY COMPETENCIES ARE LACKING WITHIN THE PUBLIC SECTOR? WHAT CAN BE DONE TO ENSURE THAT WE ATTRACT YOUNG TALENT WITHIN GOVERNMENT AND PUBLIC SECTOR?

We need more digital/computer forensic professionals, security assurers, risk analysts, researchers, policy developers. We seem to be focusing on more technical skills like Ethical Hacking and Network Engineering than these critical components of Cyber Security.

To attract young talent we need to have conducive working environments with open minded leadership because the young talent is eager to make a difference but they are mostly frustrated by senior management.

WHICH CYBER SECURITY AREA DO YOU THINK REQUIRES URGENT ATTENTION FROM KEY STAKEHOLDERS: FORENSICS AND INVESTIGATIONS, OPERATIONS AND MONITORING, ASSESSMENTS AND CYBER DEFENSE; RISK AND COMPLIANCE; AUDIT AND ASSURANCE OR RESEARCH AND INNOVATION?

All of them as we still have a massive skills gap amongst all. We need to deliberately train talent in these fields to ensure we keep a balance approached and avoid redundancy of skills

WHICH ONE OF THE FOLLOWING KEY STAKEHOLDERS NEED TO TAKE THE LEAD IN THE CYBER SECURITY DISCUSSION AND IMPLEMENTATION? JUDICIARY, EXECUTIVE, LEGISLATIVE, PRIVATE SECTOR, ACADEMIA OR NATIONAL INTELLIGENCE, MILITARY?

All the above stakeholders need to take part as they all complement each other. We need a holistic approach to cyber security to ensure that policies and frameworks are seamless and we can have proper KPIs.

CURRENTLY THE COUNTRY HAS A NUMBER OF REGULATIONS TO ADDRESS CYBER SECURITY/CRIME IN GENERAL – DATA PROTECTION BILL, ELECTRONIC EVIDENCE BILL AND CYBER CRIME ACT – DO YOU THINK THIS IS SUFFICIENT? IN OTHER COUNTRIES WE HAVE NOTED A NUMBER OF INDUSTRY REGULATORS SETTING UP SECTOR SPECIFIC REGULATORY FRAMEWORK. HOW COME THIS IS NOT THE CASE IN BOTSWANA?

I feel they are still not sufficient and yes setting up sector specific regulatory frameworks can go a long way helping the Botswana in the ever changing Cyber Space. We are still lagging behind mainly due to Cyber Security being a new phenomenon to Botswana and also lacking a lot of skill and knowledgeable framework developers.

OUR CURRENT EDUCATION/ACADEMIC CURRICULUM DOES NOT ADDRESS CYBER SECURITY TRAINING. WHAT HAVE YOU AND YOUR INSTITUTION DONE TO CURB THE ISSUE OF CYBER SECURITY SKILL GAP FROM GRADUATES?

We are currently running an independent self-financed project dubbed Cyber Defence Hub. CDH is a program that nurtures skills across all Cyber Security disciplines. One of the key objectives is to upskill students before they graduate with vigorous mental and technical skills to make them ready for the market. We are currently setting up what would be the first independent professional C.E.R.T

CYBER DEFENCE HUB

This is an independent self-financed project. CDH is a program that nurtures skills across all Cyber Security disciplines. One of the key objectives is to upskill students before they graduate with vigorous mental and technical skills to make them ready for the market. We are currently setting up what would be the first independent professional C.E.R.T

Comments From The Cyber Defence Hub Students

KEORAPETSE

the Cyber Defense Hub, is quite a dope place to hang around. Having great minds around me, actually made me change my view on other things like appointing of roles its criticality when settings tasks. The sense of one man one mission goal didn't work for me when it comes to our field. But having a team allowed me grow from point A to B.

RONN

I joined the Hub with a strong belief that with our continued collaboration in the field of Cyber Security, it will enable us to one day defend our nation when the need arises, as well as be able to transform the communities which we exist within. I believe in this establishment!

GEORGE

I joined the cyber defense hub because I believe in the power of collaboration among like-minded peers. Presenting a united front dramatically increases the odds of success, particularly in an emerging field that not well understood. By networking with individuals in both technical and non-technical roles, I will gain a broader perspective in general that I would not otherwise attain, working alone.

JURINEE

I recently joined Cyber Defense Hub because it really caught my attention in matters relating to cyber. We are living in a world that is quickly changing to a more digital world and so we ought to gain knowledge about the changes that will occur in and around the cyber world and I believe Cyber Defense Hub will expose us to such knowledge.

TSHEPO

Basically I joined the group to broaden my knowledge computer related field learning from bright minds from different field of computer study such networking, mobile computing and computing. Learning more about hacking, knowing vulnerabilities with different perspectives of computing minds will broaden my learning.

GERALD

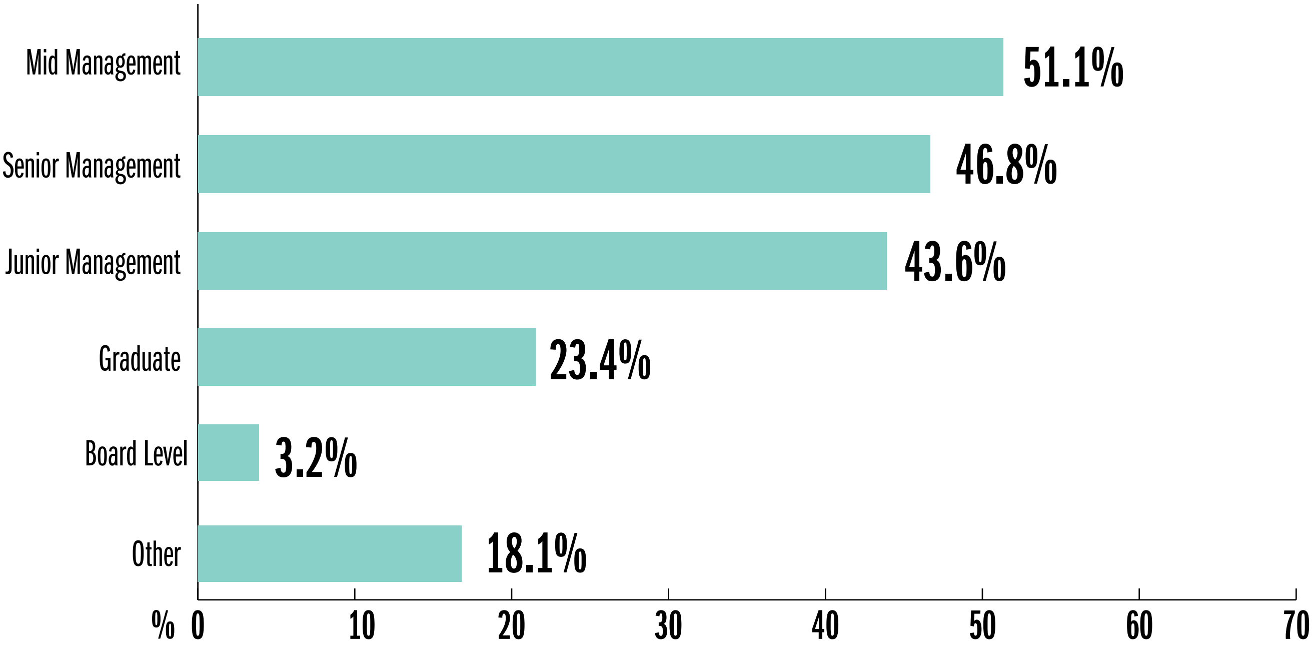
I became a part of the cyber defence hub so as to broaden my network and work with like-minded intellectuals. This initiative been a finesse grooming platform as it is gives me exposure and experience in my field and other fields.

MINNAH

I joined Cyber Defense Hub to share and learn computer skills. The good thing about the hub is that it caters for everyone both in and outside the computer field and it is always great when we meet and get to learn from each other.

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

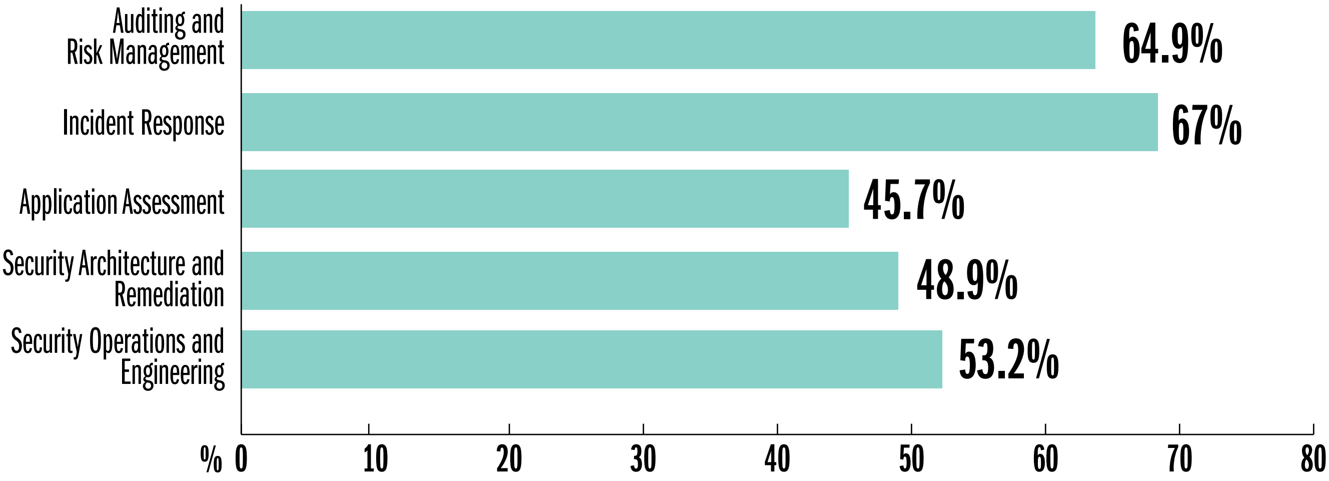
AT WHICH LEVEL DOES YOUR ORGANISATION FIND THE SKILLS SHORTAGE TO BE THE MOST ACUTE?



GRAPH 8: SKILLS SHORTAGE PAIN POINT.

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

05

DID YOU KNOW?

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

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

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

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

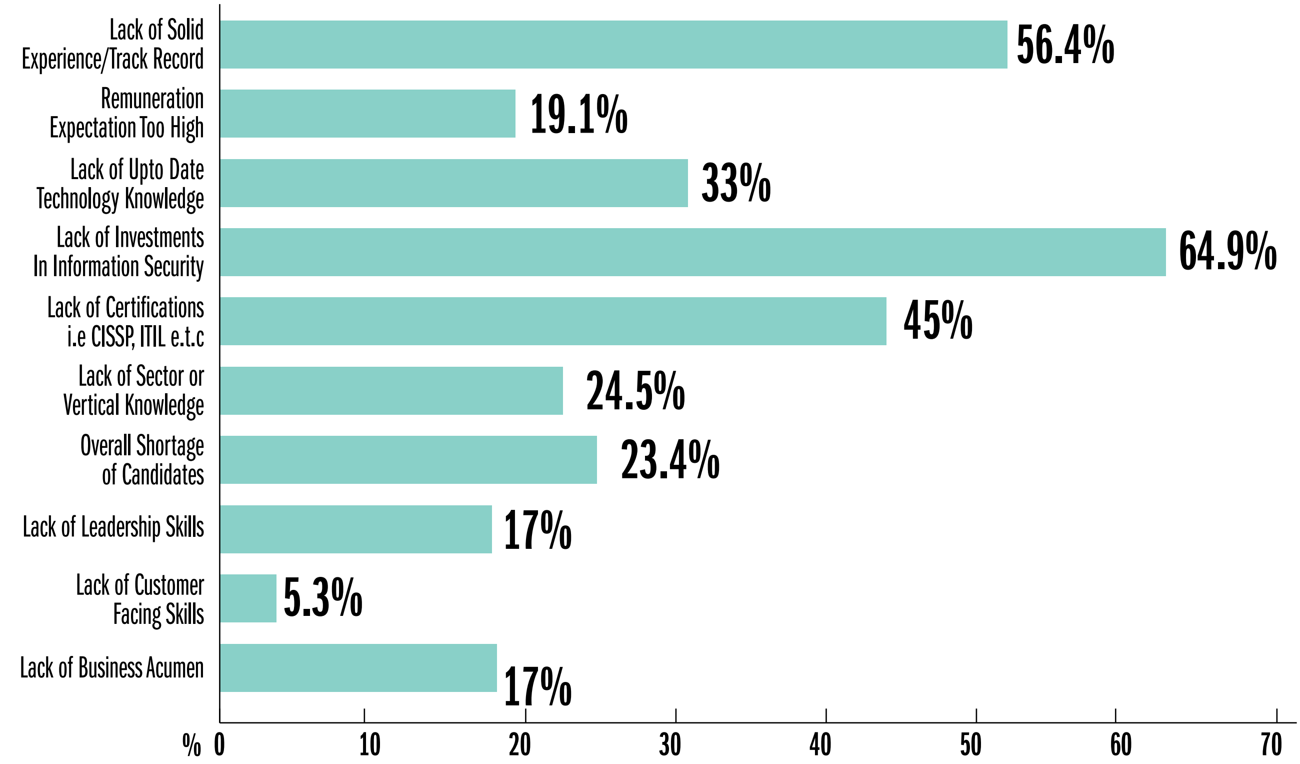
- A top notch cybersecurity manager will not be efficient if the organisation structure limits his mandate by having him report to e.g. finance.
- Investing in a SIEM will not add value if the network has not been properly segmented and baseline of activities (determining what's normal) established.

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

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

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

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



GRAPH 10: RECRUITING CONSTRAINTS.

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

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

TALENT POACHING

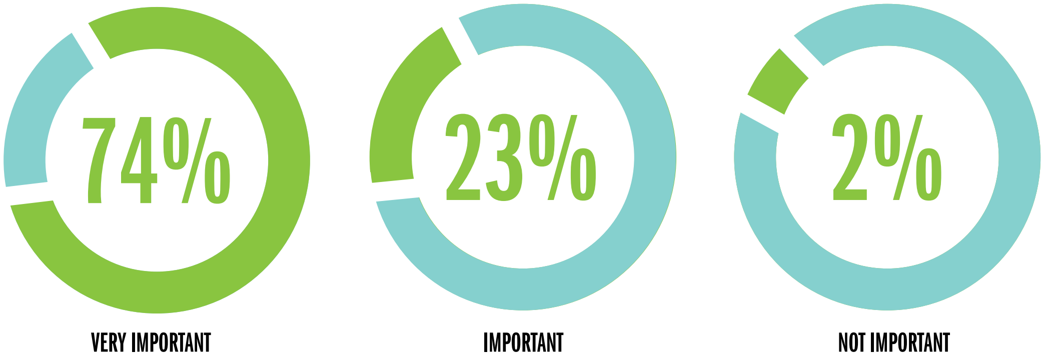
It is exceedingly difficult to hire new experienced professionals in an organisation. Why? Experienced cybersecurity professionals are in high demand, so organisations are engaged in a battle royale to coax them away from their present employers and outbid others for their services.

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

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

CONCLUSIONS FROM THE SURVEY RESULTS.

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

INDUSTRY PLAYER PERSPECTIVE

ADDRESSING CYBER SECURITY SKILLS GAP IN THE ENTERPRISE ENVIRONMENT

JOSEPH MATHENGE

Chief Operations Officer, Serianu Limited

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

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

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

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

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

I will discuss these concepts in brief.

1. Attract the right candidate.

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

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

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

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

2. Total compensation and benefits package.

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

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

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

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

3. Retain the talent.

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

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

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

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

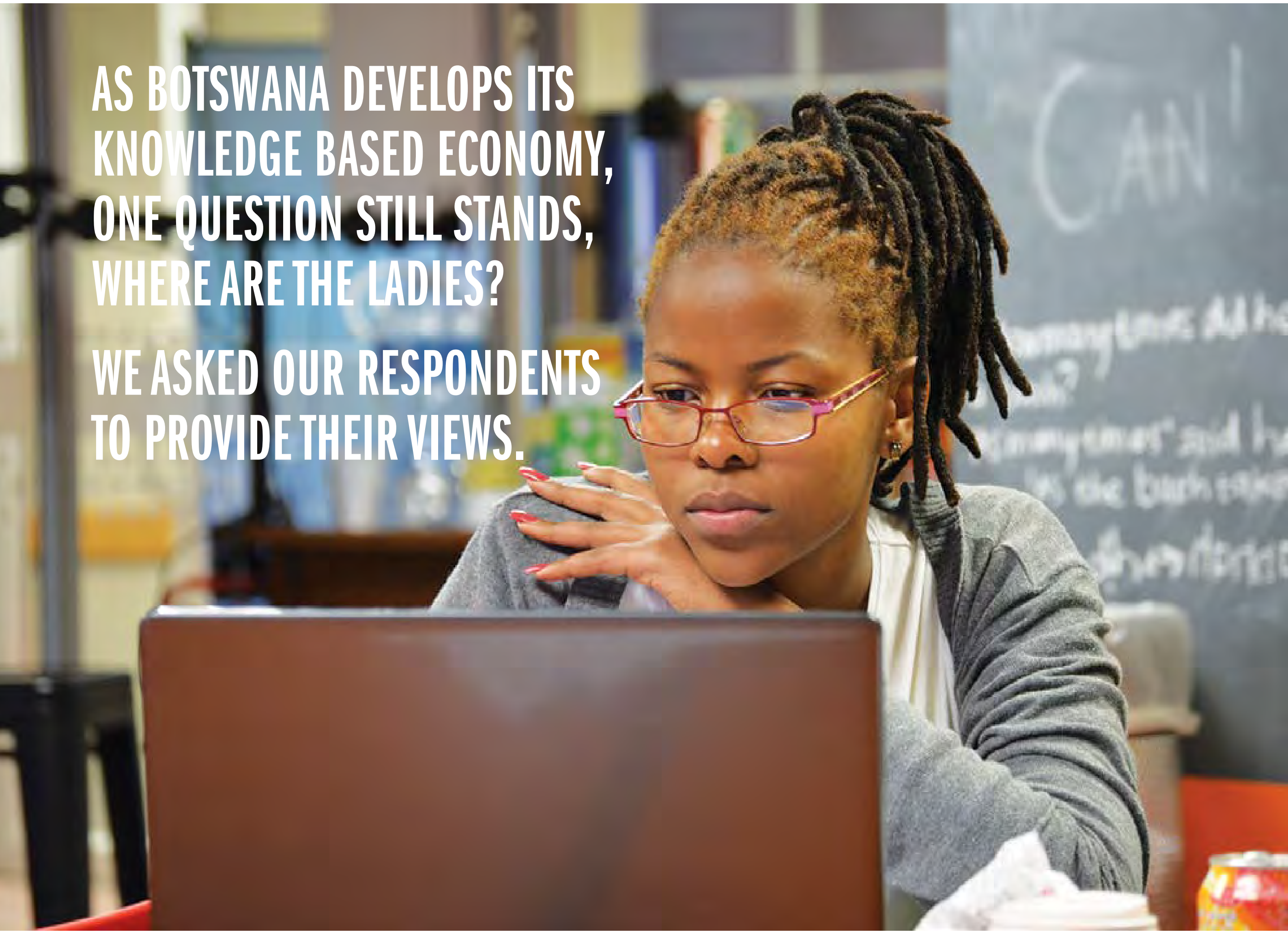
4. Be willing to let go.

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

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

THE GENDER GAP

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

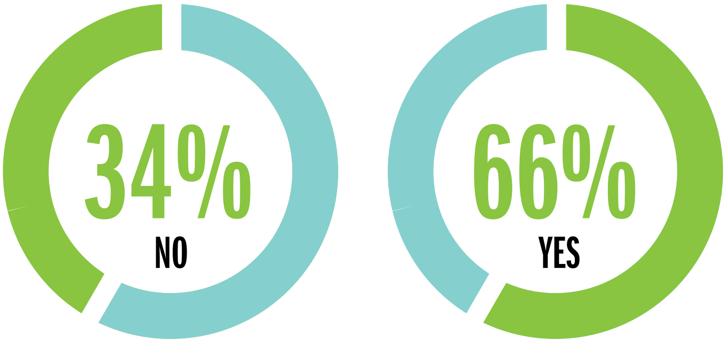


AS BOTSWANA DEVELOPS ITS KNOWLEDGE BASED ECONOMY, ONE QUESTION STILL STANDS, WHERE ARE THE LADIES?

WE ASKED OUR RESPONDENTS TO PROVIDE THEIR VIEWS.

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

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



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

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

GENDER GAP ISSUES

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

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

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

LIES WOMEN TELL THEMSELVES FOR NOT WORKING IN IT:

"I AM NOT GOOD ENOUGH."

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

"THAT'S A MAN'S JOB."

"I AM OKAY WHERE I AM."

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

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

"IT IS THE BOYS CLUB"

"THERE ARE TOO MANY MEN"

"THERE ARE TOO MANY WOMEN"

.

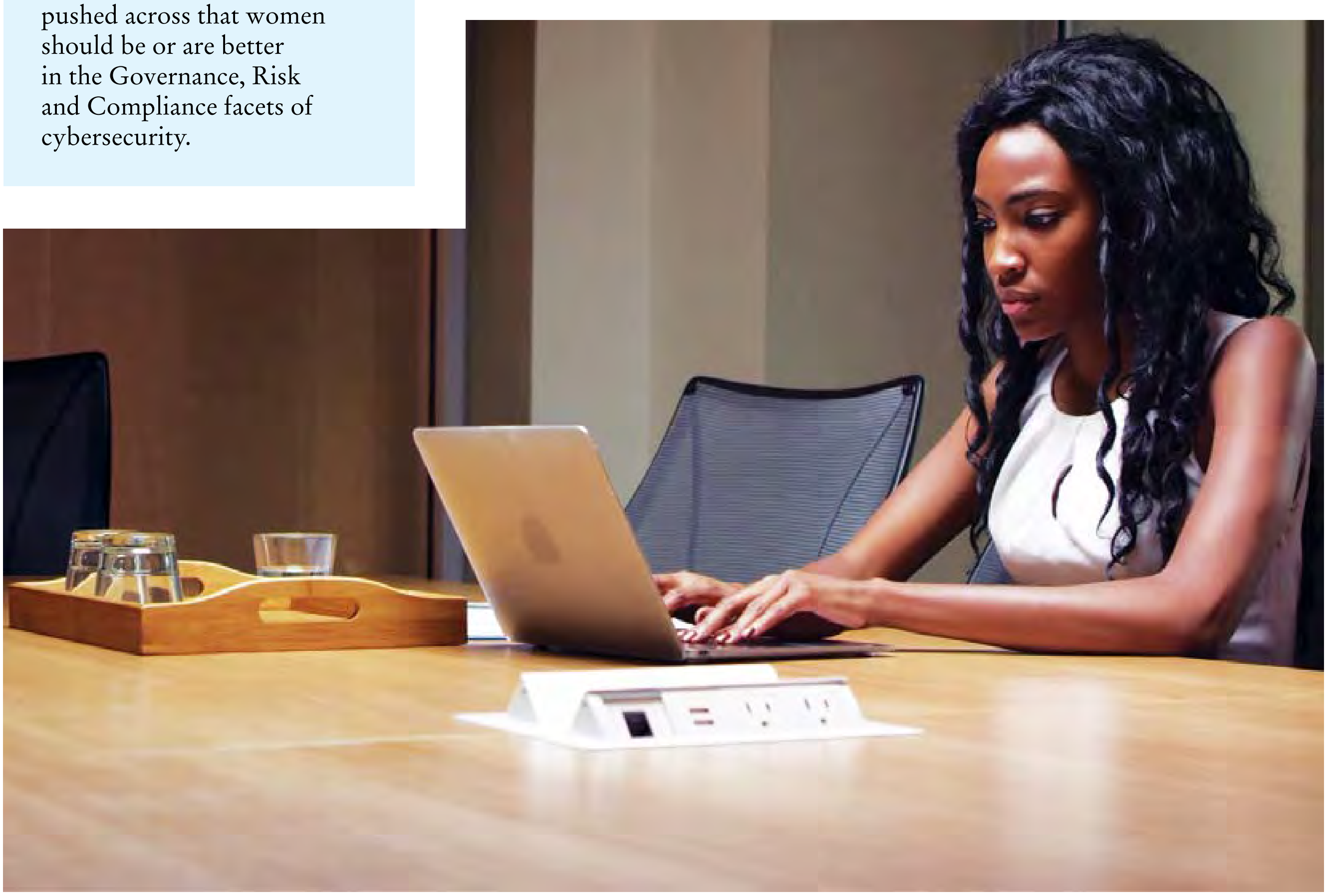
THE TECHNICAL SKILLS QUESTIONS?

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

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

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

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



INDUSTRY PLAYER PERSPECTIVE

THE REQUIREMENT TO KEEP INFORMATION SECURE: HOW CYBERSECURITY ATTAINED THE STATUS OF BEING A LEGAL OBLIGATION IN BOTSWANA

SENWELO K. MODISE
Collins Chilisa Consultants

In 2000, only 15000 people used the internet in Botswana. The internet is now used by some 65% of the population according to the Global Information Technology Report, which ranked Botswana 101 out of 139 in its Networked Readiness Index. The internet, good and convenient as it may be is a fertile environment for crime, and crimes committed through or enabled by the internet are complex and ever-evolving. In order to combat crimes dependent on the internet and computers, Botswana enacted a Cybercrime and Computer Related Crimes Act in 2007.

The Act was amended in 2018 to catch up with the pace of evolving challenges presented by the internet. Botswana's legislative framework is predominately substantive and procedural; it fails to provide for one important aspect of dealing with cybercrime. It is substantive in the sense that it defines what constitutes a cybercrime, among the statutory prohibited acts are unauthorized access to a computer system or service, access with the intent to commit an offence, unauthorized interference and interception of data or network, offensive electronic communication and child pornography. It also covers the procedural aspect in the sense that it provides for the process to be employed to investigate cybercrimes.

The Act fails to provide for the preventative aspect of dealing with cybercrime, which is largely achieved through cybersecurity. Combating cybercrime is a multi-disciplinary affair that spans hardware and software through to policy and people, all of it aimed at both preventing cybercrime occurring in the first place, and minimizing its impact when it does. This is the practice of cybersecurity.

Cybersecurity, also referred to as information security, refers to the practice of ensuring the integrity, confidentiality, and availability of information. Elements of cybersecurity encompass network security, application security, endpoint security, data security, identity management, database and infrastructure security, cloud security, mobile security, disaster recovery/business continuity planning, end-user education and the choice of which element to focus on depends on the organisation and its operations.

Throughout the years, cybersecurity has not been given the attention it deserves by those that ought to have taken it into consideration. According to the Africa Cybersecurity Report of 2016 security professionals are struggling to demonstrate business value of cybersecurity to senior management because they are providing very technical operational metrics whereas business managers are looking for more business-oriented metrics. One other reason why security professionals struggle with demonstrating the business value of cybersecurity is due to the fact that it is not a legal obligation; it is not mandatory, it is incidental and seems optional. The good news is that it has attained the status of being compulsory all thanks to the legislative development in data protection and privacy. Cybersecurity is one the data protection principles enshrined in the recently enacted Data Protection Act of 2018, which has been promulgated to ensure the protection of personal data and privacy of the individual.

The Act is on notice pending the setting up of a regulatory authority established therein. Section 14(f) of the Act provides that a data controller shall ensure that personal data is protected by reasonable security safeguards against risks such as loss, unauthorized access, destruction, use, modification or disclosure.

This means that both governmental and non-governmental entities are now compelled to adopt information security policies and progress as a matter of compliance with the law. Section 32 of the Act provides that a data controller shall take appropriate technical and organisational security measures necessary to protect personal data. The appropriate level of security is ensured taking into account the technological development of processing personal data and the costs for implementing the security measure as well as the nature of the personal data to be protected and the potential risks involved in processing.

Compliance with this aspect of the law will require an information security program with a lifecycle that is monitored and evaluated. The information security policies and programs used to protect personal data are in as good a position to protect other information assets of the company such as intellectual property and trade secrets therefore can be applied across board. Preceding the adoption of an information security program would be a data protection impact assessment involving data inventory and mapping, identifying both personal data and sensitive personal data, identifying the risks of processing and ways to mitigate the risks.

Following the adoptation of an information security program would be regular information security audits and data privacy audits to ensure effectiveness of the program throughout its lifecycle. The challenge likely to be faced in light of this new legal obligation is the skills gap. There are not many cybersecurity and data protection professionals in Botswana, even though at the heart of combating cybercrime are these professionals however there is light at the end of the tunnel.

INDUSTRY PLAYER PERSPECTIVE

DOES THE GOVERNMENT ENGAGE THE PRIVATE SECTOR OR ACADEMIA IN ITS CYBERSECURITY WORK? HOW EFFECTIVE ARE THESE PARTNERSHIPS?

DR. AUDREY MASIZANA

Senior Lecturer and Head of Computer Science, University of Botswana

The role of academia and those in education sectors is to assist in capacity and awareness building to produce human capital with mission-critical skills in cyber security and ethical hacking.

Development of curricula for cyber security is a fairly new function in the educational arena worldwide and most institutions, including at tertiary level, are just beginning to integrate programs in cyber security as a part of their academic qualifications. This clearly is a case here in Botswana. The most prestigious professional associations in computing – ACM and IEEE 2017, established a joint force to develop a cyber-security model curricula which covers a wide range of areas such as data security, software security, component security, connection security, system security, human security, organisational security, and societal security. The body of knowledge recognises that education in cyber security should address not only the technology, but also issues relating to the people, policy, information and processes. Hence this calls for a multi-disciplinary approach to cyber security education that emphasises on inclusive delivery that relies on partnerships amongst role players.

In addition, academic institutions within the country have to aggressively engage with industry, and government to produce basic and cutting edge research validated solutions towards challenges in security faced by the society. In this country there exist next to none of such collaborations explicitly established for this purpose, which is a serious and worrisome gap. Existing research efforts conducted in the various institutions, are in isolation and barely demonstrate significant impact on the county's real life security problems. There is an urgent need to address these concerns as part of the national strategy.

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

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

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

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

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

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

COMPONENTS OF ACIC’S COMPETENCY MATRIX

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

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

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

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

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

ACIC'S COMPETENCY MATRIX

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

TABLE 2: OBIS QUAS ACERCHILIT FUGITAE CUM VOLE.

0 Not Applicable   1 General Knowledge

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

● 2 Good Understanding ● 3 Expert Understanding

AFRICA CYBER IMMERSION CENTRE

Africa Cyber Immersion Centre
acic
Engage | Educate | Empower

Bridging the Skills Gap

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

PARENTAL CONTROL

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

TIPS FOR ENSURING MY KID'S ONLINE BEHAVIOR?

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

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

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

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

WHAT PARENTAL SOFTWARE CAN I USE?

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

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

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

Engage, Educate & Empower

MASTERING THE FOUNDATION

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

WAY-FORWARD

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

GOVERNMENT

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

The government should be alive to the realities of cyberwars.

ACADEMIA

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

EMPLOYERS

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

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

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

STUDENT, KAPSABET BOYS HIGH SCHOOL

acic

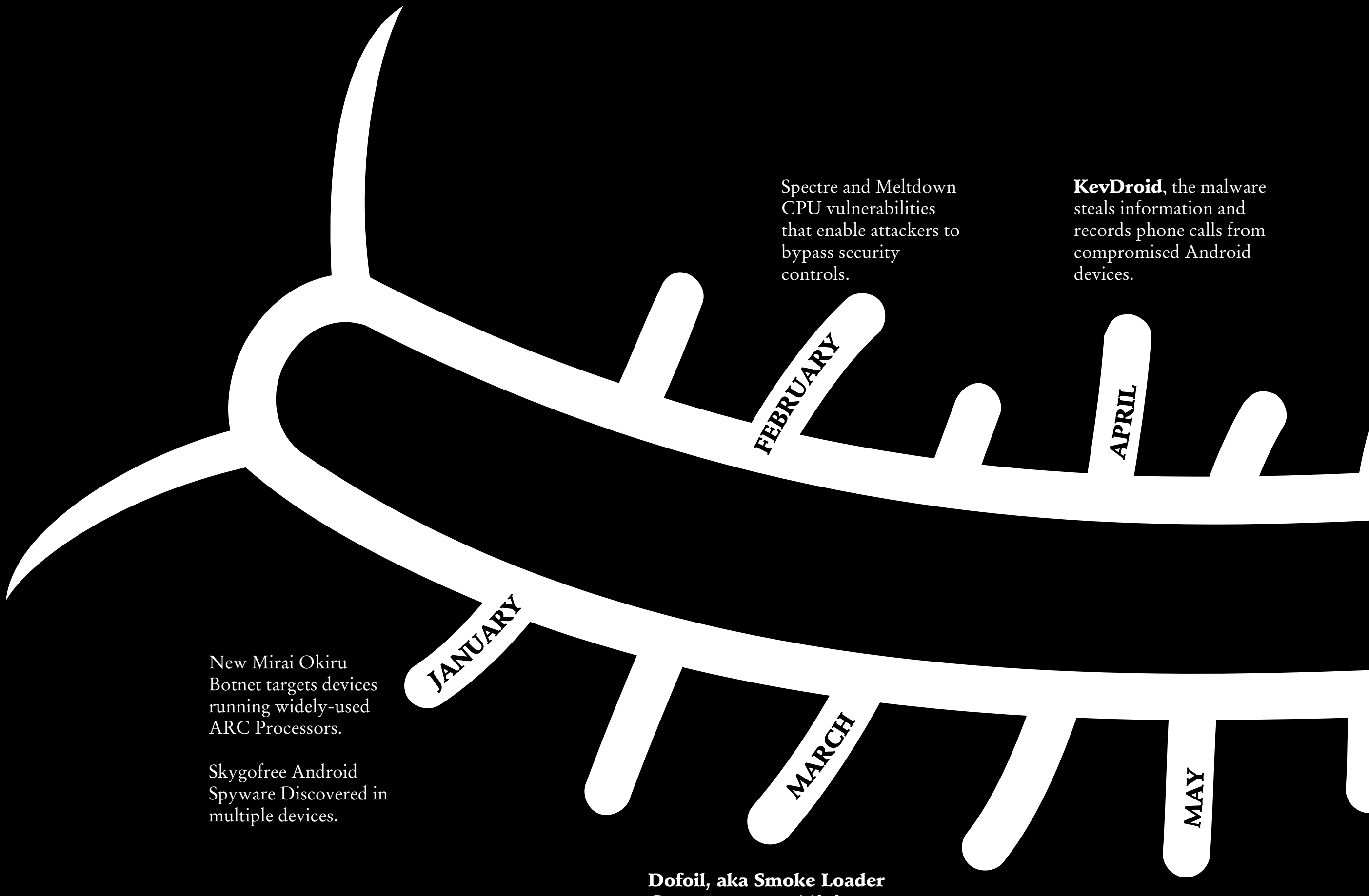
SCIENCE
LABORATORIES

NOVA PH

KAPSABET HIGH SCHOOL

CYBER INTELLIGENCE

LATEST MALWARE VIRUSES THAT WERE RELEASED AND CAPTURED IN 2018.



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

Skygofree Android Spyware Discovered in multiple devices.

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

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

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

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

Cryptomining Malware Digs into Nearly 40% of Organizations Globally.

Locally re- engineered Malware discovered by the ACIC team;

Betaversion Malware
MD5 hash value: e86c626878a0c693d3727024d55ff882

Scr.exe Malware:
MD5 hash value: f05a31ae604e4ea844e8130e45d30f01

Taskrun Malware:
MD5 hash value: f2223193031768286296c5c70990d63d

Scvhost.exe Malware:
MD5 hash value: f2223193031768286296c5c70990d63d

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

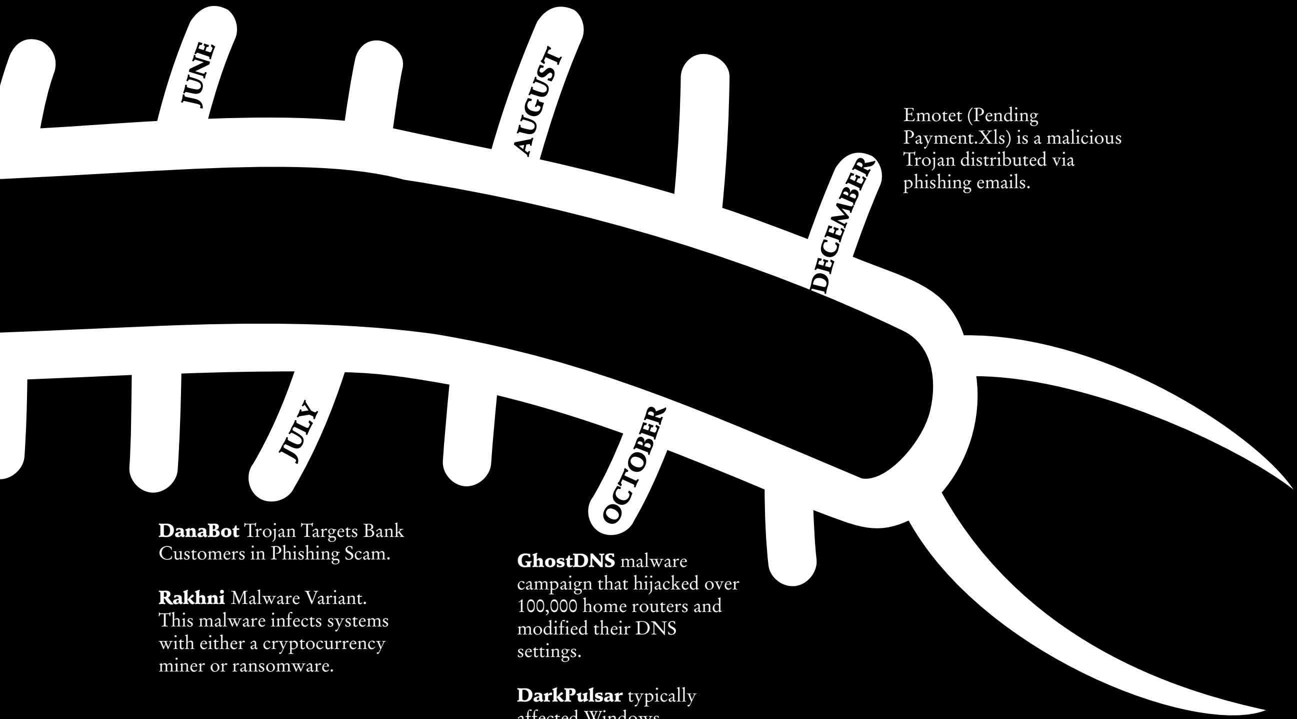
MyloBot – Highly Sophisticated Botnet Shutdowns Windows Defender and windows update.

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.



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

DanaBot Trojan Targets Bank Customers in Phishing Scam.

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

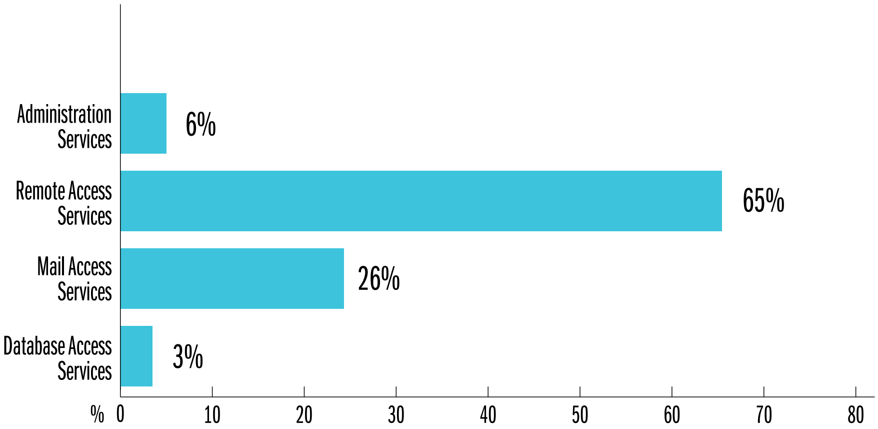
GhostDNS malware campaign that hijacked over 100,000 home routers and modified their DNS settings.

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

OPEN PORTS

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

We classified them into the following categories::

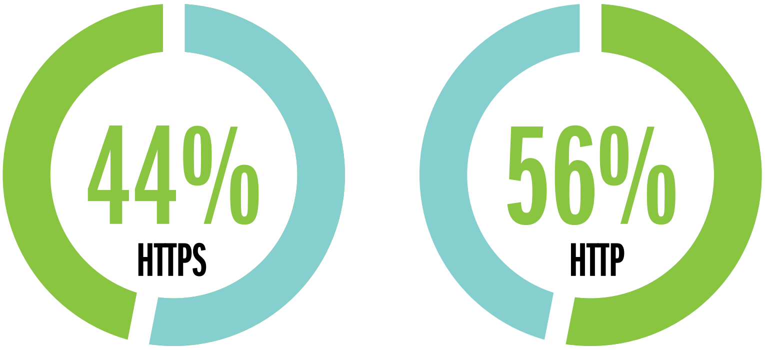


GRAPH 12: EXTERNALLY ACCESSIBLE SERVICES.

WEB SERVICES

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

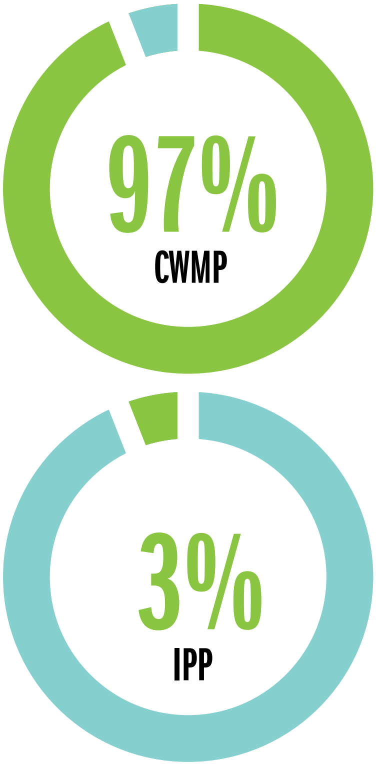
CHART 11: WEB SERVICES.



ADMINISTRATION SERVICES

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

CHART 12: ADMINISTRATION SERVICES.



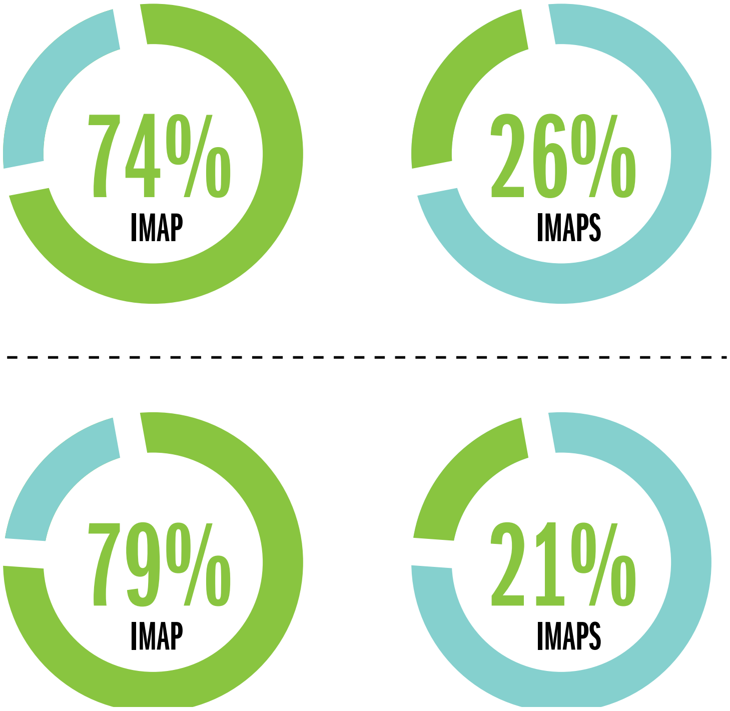
CUPS manages print jobs and queues and provides network printing while CWMP protocol enables devices to be remotely configured through the use of SOAP based Remote Procedure Calls (RPC).

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

MAIL ACCESS SERVICES

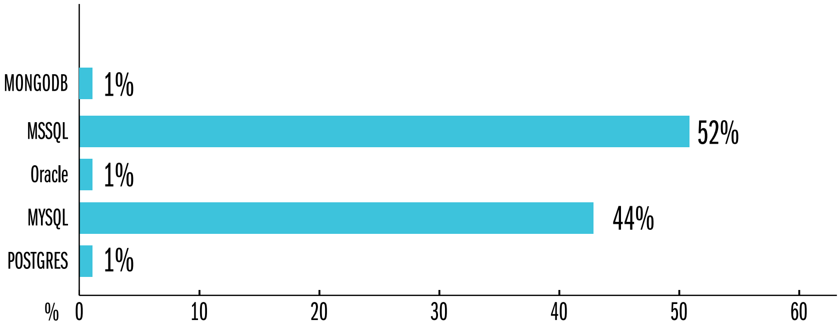
BOTSWANA

CHART 13: MAIL ACCESS SERVICES.



DATABASE ACCESS SERVICES

BOTSWANA



CRYPTO MINING

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

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

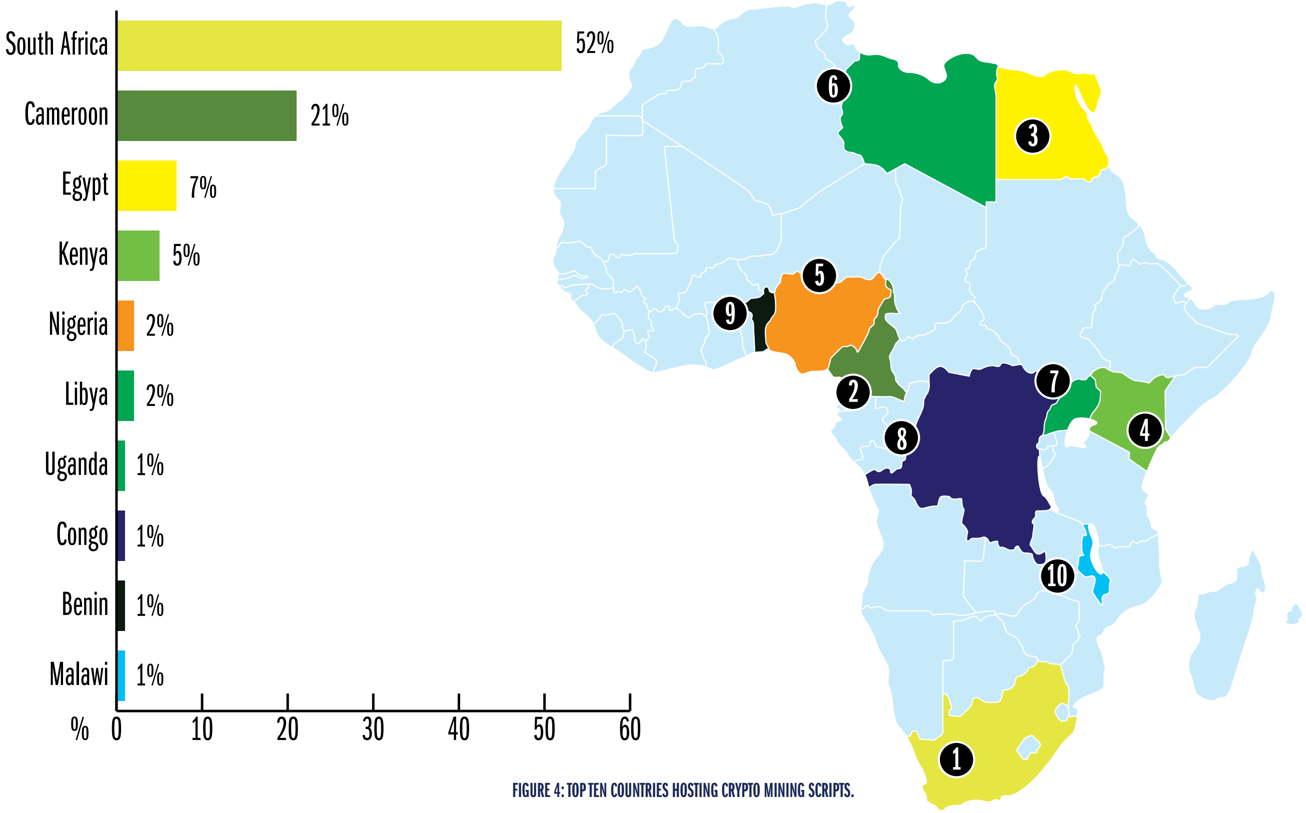


FIGURE 4: TOP TEN COUNTRIES HOSTING CRYPTO MINING SCRIPTS.

RASPBIAN ADOPTION

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

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

RASPBERRY PI

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

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

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

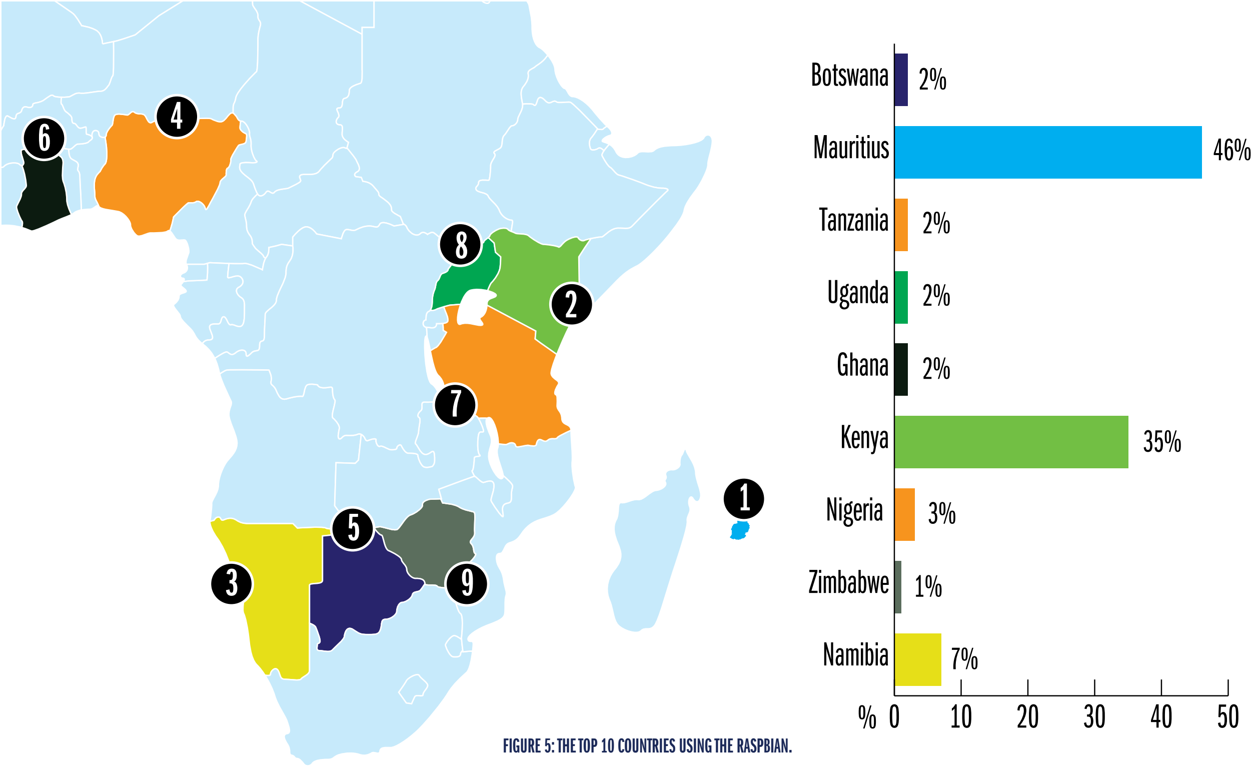
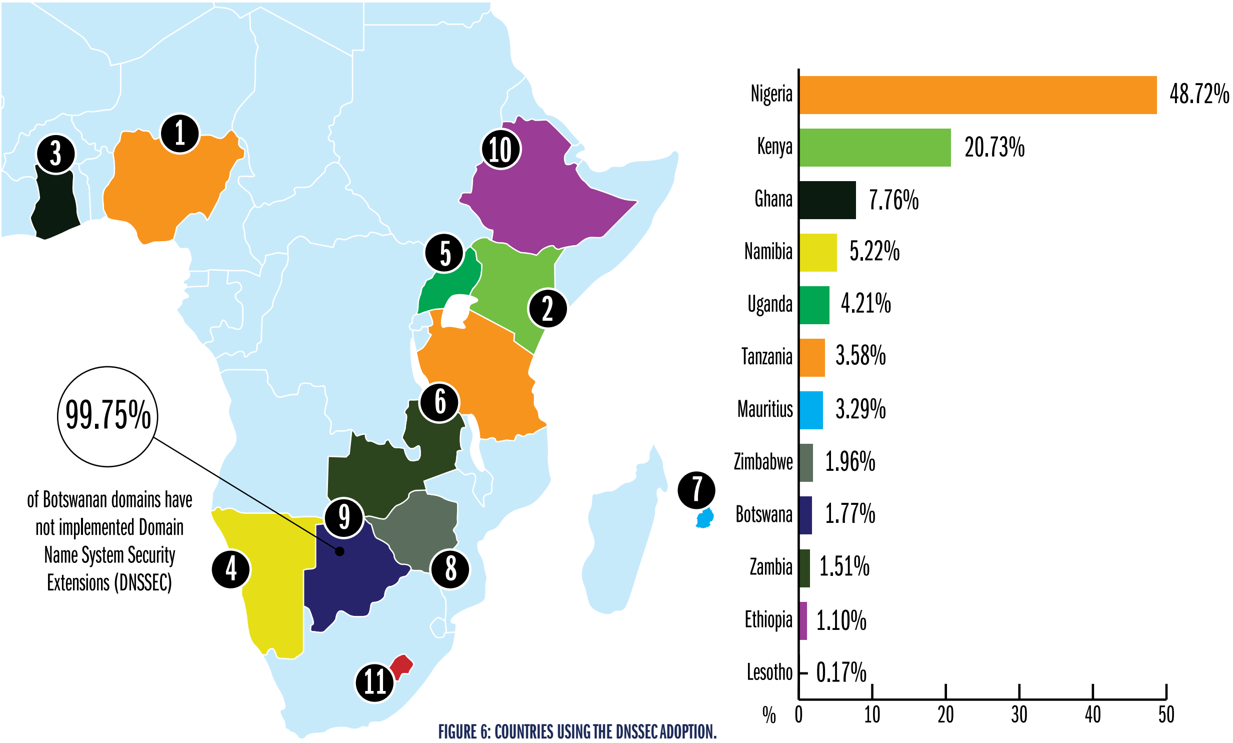


FIGURE 5: THE TOP 10 COUNTRIES USING THE RASPBIAN.

DNSSEC ADOPTION



99.75%

of Botswanan domains have not implemented Domain Name System Security Extensions (DNSSEC)

FIGURE 6: COUNTRIES USING THE DNSSEC ADOPTION.

INDUSTRY PLAYER PERSPECTIVE

BUNGAI MUHAMU

General Manager, FMRE - Reinsurance

WHAT IS THE UPTAKE OF CYBER INSURANCE IN BOTSWANA?

Despite the increasing incidence of cyber security breaches, the growth in cyber insurance premium has been lagging behind. Nonetheless, there has been an increasing number of companies especially in the financial and retail sector requesting covers of late. Whilst cyber insurance penetration and per capita expenditure or insurance density are a bit low, we expect a soar in demand in the next few years as risk posed by cyber continue to explode.

WHAT ARE THE BENEFITS OF CYBER INSURANCE?

The cost of cyber attacks alone in 2018 was more than $45 billion globally and to put it into perspective, this is almost double the size of the Botswana economy. These costs relate to both first party expenses and third party liability claims. Cyber threats are a growing and rapidly changing threat to businesses of all types and sizes. Whilst companies can have incident response plan, disaster recovery plan, and a business continuity plan, dealing with a cyber breach can be expensive and cyber insurance coverage is designed to help cover the costs associated with the breach. Beyond the direct costs of dealing with and recovering from a cyber attack or data breach, there are also other costs that are harder to quantify. Insurance is meant to protect the business against these unexpected costs.

In modern day business, data is the most important asset a company has and it's critical to have insurance for it.

HOW DO YOU CALCULATE CYBER INSURANCE PREMIUMS?

We consider quite a number of risk factors in pricing cyber insurance and the broad categories include the insured's nature of business, the people, the network, the website, the data as well as cyber risk management programme. We also insist on conducting penetration testing, vulnerability assessment, and employee training in order to arrive at an optimal risk premium. Nonetheless, there are always challenges in pricing cyber risk for example there is no geographical limitation of the risk as compared to our conventional property risks, the significance of the human element, correlation of attacks, risk of aggregation and dynamic of technological evolution. If there is something certain and constant about technology is that it will not stop changing. So then how you model this change in pricing is always difficult and we have to constantly change our pricing models.

HOW ARE CYBER CLAIMS HANDLED AND ASSESSED?

Cyber claims handling expertise normally comes at a premium because assessing and calculating damages in a cyber breach claim can be complex. To help customers, in case of an attack, we focus on three areas: Understand the complexities of the particular attack waged and the technology behind it; determine whether coverage is available under the applicable policy; and identify the claims handling needs associated with the coverages and particular attention to the reputational risk and emotional aspects of the attack is important. Each cyber insurance policy issued will state the Public Relations Consultants and IT Experts in case of a claim and these coordinate with the insurers in handling the claim.

DOES CYBER INSURANCE REPLACE CYBER SECURITY?

Just like the traditional insurance protection, cyber insurance does not in any way replace cyber security. One of the most prominent principle of insurance is that the client has to act as if they are not insured and insurance should come in when your control systems fail. In the same vein, cyber insurance is usually the last layer of protection to cover unexpected losses and in this case breaches. We expect our clients to maintain robust systems and implement the six Ds of cyber defense strategies which are Deter, Detect, Defend, Deflect, Document, and Delay.

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

Yes, there is the Data Protection Act of 2018 in Botswana which is very elaborate on data collection, handling and protection. This is still a new law and there is a lot that needs to be done to make our clients aware of the implications of the Act to their business. I am sure a few companies have done an impact assessment of this Act and we always highlight it in our discussions with Compliance Officers.

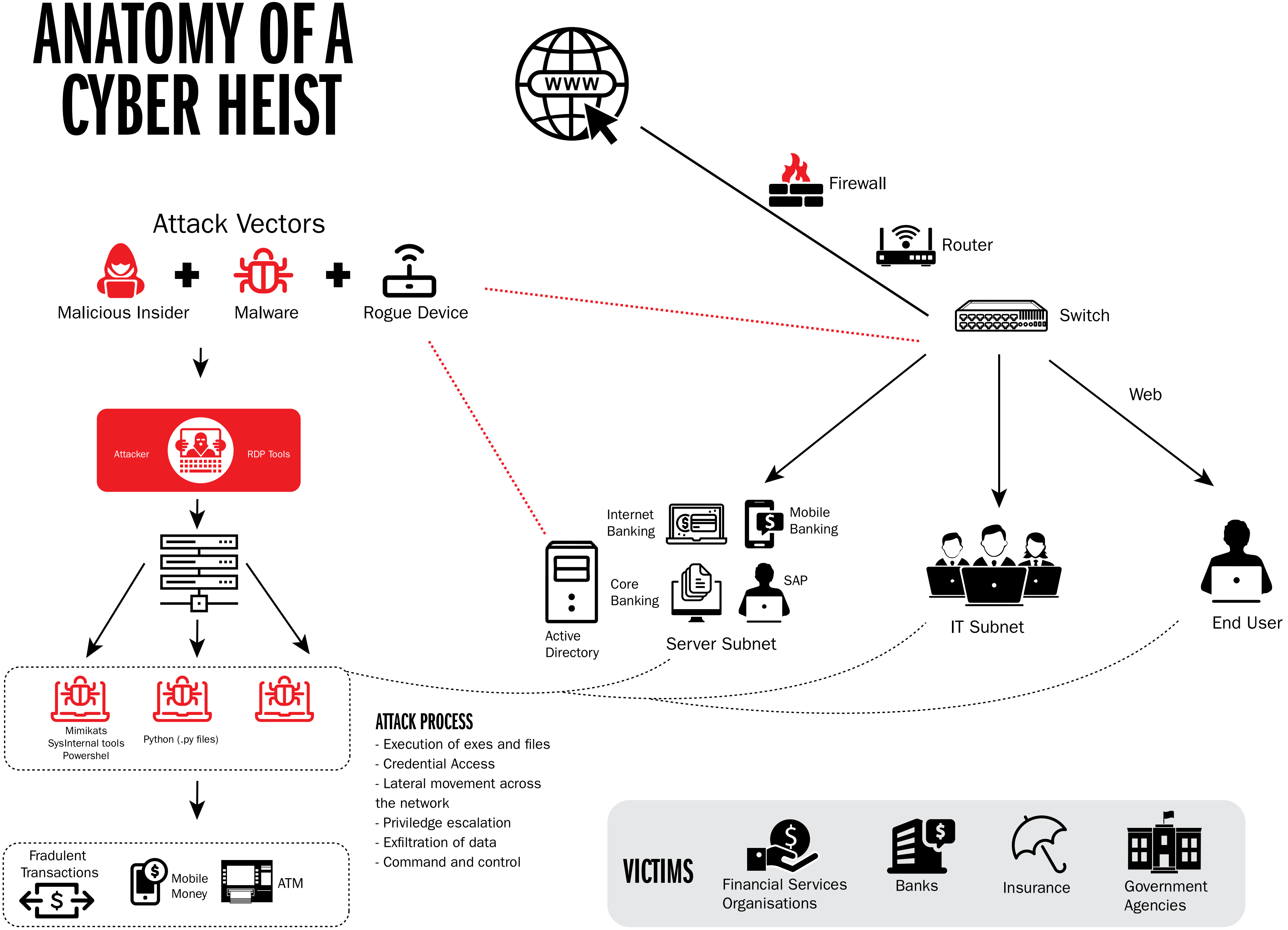
WHAT OPPORTUNITIES DOES CYBER INSURANCE PROVIDE TO ORGANISATIONS?

Its common cause that technology has brought in unprecedent levels of connectedness, automation, convenience and mobility. However, this is also tied with exceptional potential for cyber-related catastrophe and aggregation of risk from the connected life. Cyber insurance will allow companies to leverage on the inherent opportunities being presented by technology without worrying about the adverse risks associated with it. On the other hand, from an insurer perspective, as the scope, frequency and severity of cyber risks continue to spike, huge new opportunities exist for insurers who make a first mover advantage and position themselves for growth in the cyber insurance market.

WHAT FUTURE TRENDS SHOULD WE ANTICIPATE WITHIN CYBER INSURANCE SECTOR?

When I joined the insurance market, about 16 years ago, insurance for technology related business was restricted to physical digital assets only. Things have changed a lot since then especially in the past 5 years. Insurers have increased the boundaries of insurability and this being driven the Lloyds of London market to include insurance of the intangible cyber assets. Insurers will continue to enhance their cyber capabilities and disentangle the complexity of pricing in order to provide a full spectrum of services. Therefore an expected future development of cyber insurance could include damage to intangible assets with non-cyber perils, such as crisis communication coverage, consultancy services, reputational harm which are rarely covered by traditional insurance.

ANATOMY OF A CYBER HEIST



ATTACK PROCESS

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

VICTIMS

Financial Services Organisations

Banks

Insurance

Government Agencies

INFORMATION SHARING GAP

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

CYBOTA INTEL
Africa's Cyber Threat Sharing Platform

OBJECTIVES OF SERIANU'S INFORMATION SHARING PLATFORM

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

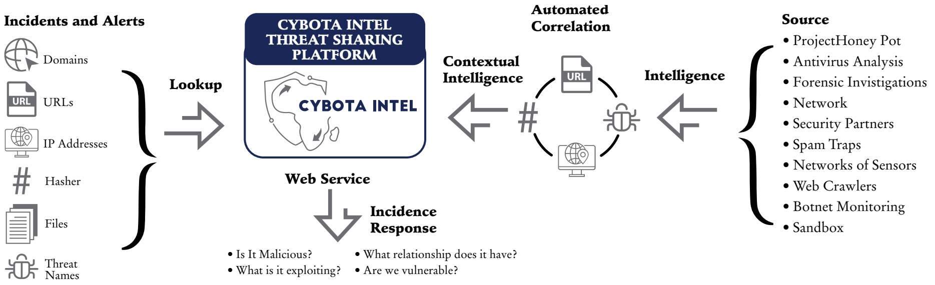
Rapid Response: Early detection leading to rapid incident response.

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

Improved Eco-system: Through information sharing.

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

HOW IT WORKS



WHY JOIN?

ORGANISATION

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

SECURITY AND TECHNICAL TEAMS

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

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

CYBER LAWS IN BOTSWANA

06

DID YOU KNOW?

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

WIKIPEDIA

UNAUTHORIZED ACCESS TO A COMPUTER OR COMPUTER SYSTEM

Accesses the whole or any part of a computer or computer system, knowing that the access he or she intends to secure is unauthorized; or causes a computer or computer system to perform any function as a result or unauthorized access to such system, commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to

Imprisonment for a term not exceeding six months, or to both.

A person shall not be liable under subsection (1) where the person-

- Is a person with a right to control the operation or use of the computer or computer
- System and exercises such right in good faith;
- Has the express or implied consent of a person empowered to authorize him or her to?
- Have access to the computer or computer system;
- Has reasonable grounds to believe that he or she had such consent as specified in
- Subparagraph (b);
- Is acting pursuant to measures that may be taken under Part III of this Act; or
- Is acting in reliance of any statutory power arising under any enactment or a power?

Conferred under any Act, for the purpose of-

- Obtaining information, or
- Taking possession of any document or other property.

A person's access to a computer or computer system is unauthorized where the person-

- Is not himself or herself entitled to access of the kind in question;
- Does not have consent, from any person who is so entitled, to access of the kind in
- Question; or
- Exceeds the access he or she is authorized.

For the purposes of this section, it is immaterial that the unauthorized access is not directed at

- A particular programme or data;
- A programme or data of any kind; or
- A programme or data held in any particular computer or computer system

UNAUTHORIZED ACCESS TO COMPUTER SERVICE

Subject to subsection (5), a person commits an offence where such person, knowingly and by any means, without authorization or exceeding the authorization he or she is given-

- Secures access to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service; or
- Intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within, a computer or computer system.

A person who commits an offence under subsection (1) shall on conviction be liable to a fine not exceeding P20, 000 or to imprisonment for a term not exceeding one year, or to both.

Where, as a result of the commission of an offence under subsection (1), the operation

Of a computer or computer system is impaired, or data contained in the computer or computer

System is suppressed or modified, a person shall on conviction be liable to a fine not

Exceeding P40, 000 or to imprisonment for a term not exceeding two years, or to both.

For the purposes of this section, it is immaterial that the unauthorized access or

Interception in subsection (1) is not directed at-

- A particular programme or data;
- A programme or data of any kind; or
- A programme or data held in any particular computer or computer system.

A person shall not be liable under subsection (1) where he or she-

- Has the express or implied consent of both the person who sent the data and the Intended recipient of such data; or
- Is acting in reliance of a statutory power arising under any enactment or a power Conferred under any Act

ACCESS WITH INTENT TO COMMIT AN OFFENCE

A person who, with intent to commit an offence under any other enactment, causes a Computer or computer system to perform any function for the purpose of securing access to-

- Any programme or data held in a computer or computer system; or
- A computer service, commits an offence and shall on conviction be liable to a fine not Copyright Government of Botswana exceeding P10, 000 or to imprisonment for a term not exceeding six months, or to Both.

For the purposes of this section it is immaterial that-

- The access referred to under subsection (1) is authorized or unauthorized; or
- The further offence to which this section applies is committed at the same time as when the access is secured or at any other time.

UNLAWFUL POSSESSION OF DEVICES OR DATA

- A person who intentionally, without lawful excuse or justification, manufactures, sells procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.
- A person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1), commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.
- A person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

FOR THE PURPOSES OF SUBSECTION (3), "POSSESSION OF ANY DATA OR PROGRAMME" INCLUDES-

- Having possession of a computer or computer system or data storage device that holds or contains the data or programme;
- Having possession of a document in which the data or programme is recorded; and
- Having control of the data or programme that is in the possession of another person

CYBER EXTORTION

A person who performs or threatens to perform any of the acts described under this Part for the purposes of obtaining any unlawful advantage by-

- Undertaking to cease or desist from such actions; or
- Undertaking to restore any damage caused as a result of those actions,
- Commits an offence and shall on conviction be liable to a fine not exceeding P10,000 or to imprisonment for a term not exceeding six months, or to both.

CYBER FRAUD

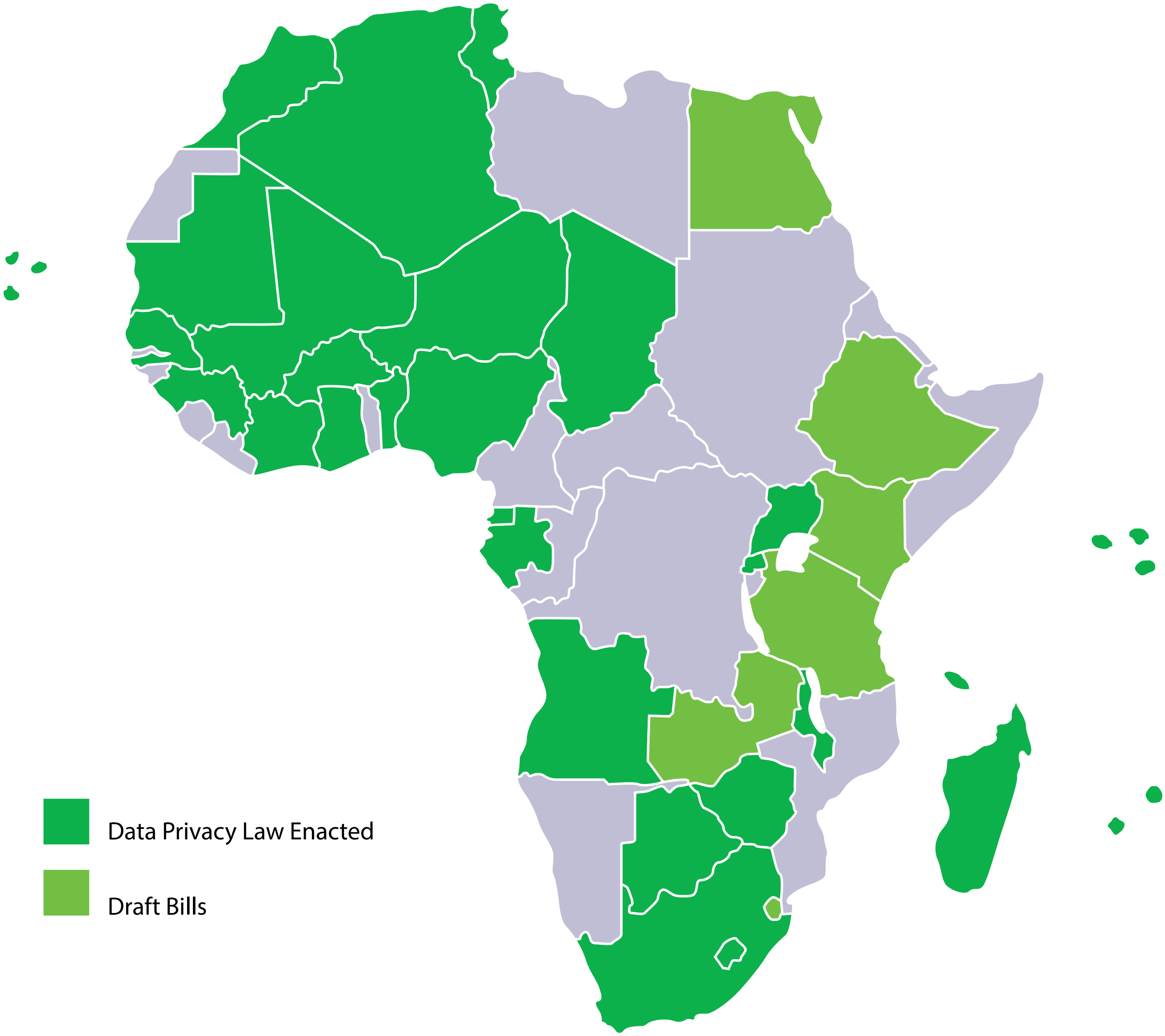
A person who performs any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

A person who, with intent to procure any advantage for himself or herself or another person, fraudulently causes loss of property to another person by-

- Any input, alteration, deletion or suppression of data; or
- Any interference with the functioning of a computer or computer system,

Commits an offence and shall on conviction be liable to a fine not exceeding P20,000 or to imprisonment for a term not exceeding one year, or to both.

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

TOP TRENDS AND PRIORITIES FOR 2019

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

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

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

GROWTH IN LETHAL AND TARGETED MALWARE

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

ATTACK-REPLICATION

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

INCREASED USE OF OUTSOURCED/ MANAGED SECURITY SERVICES

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

USE OF THIRD PARTIES TO EXPLOIT TARGET ORGANISATIONS

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

CONTINUED ENGAGEMENT FROM BOARD AND SHAREHOLDERS

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

GROWTH IN CYBER INSURANCE OFFERINGS

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

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

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

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

Top Priorities for 2019

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

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

BOARD ENGAGEMENT: PROACTIVE MONITORING AND TRACKING OF CYBERSECURITY METRICS.

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

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

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

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

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

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

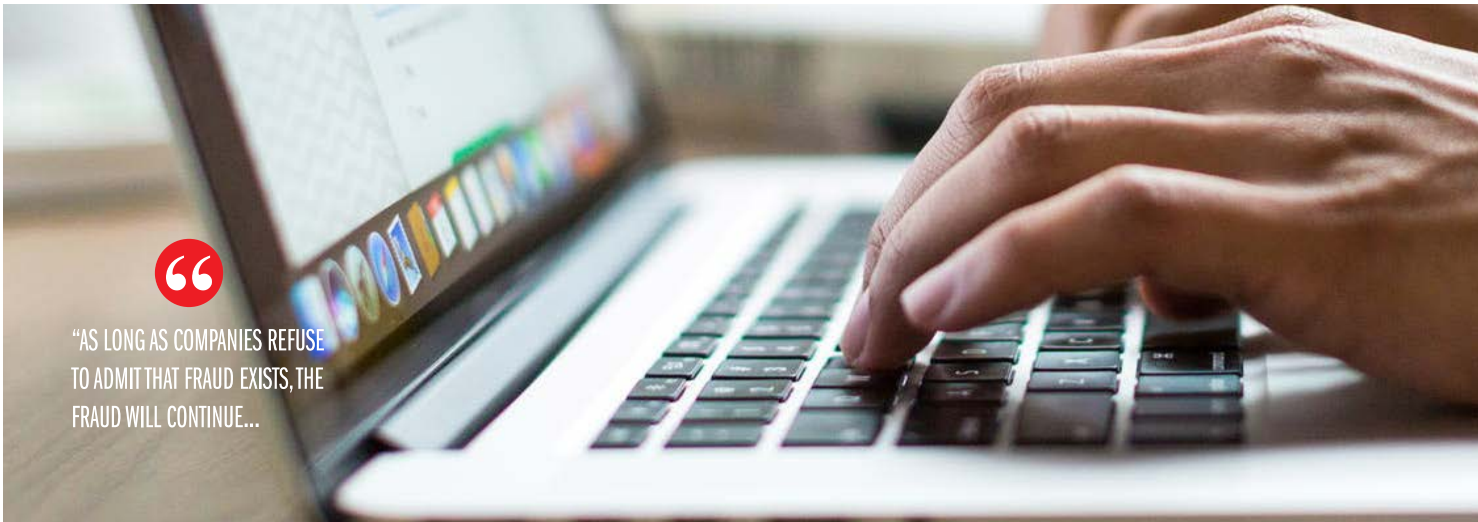
POLICY IMPLEMENTATION: ENFORCING SPECIFIC ACTIONS DOCUMENTED WITHIN COMPANY POLICY.

FRAUD EXPOSURES

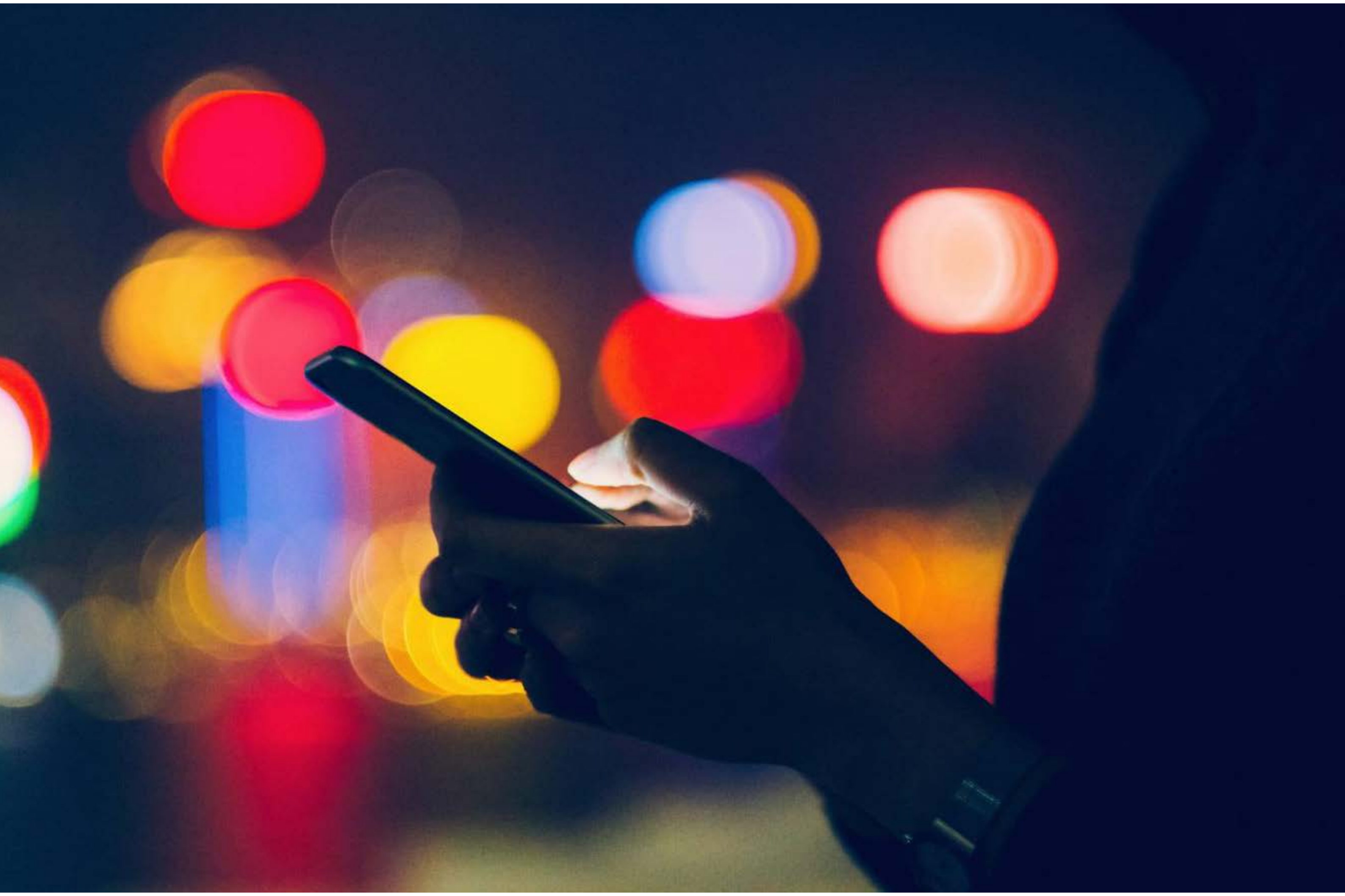
FRAUD EXPOSURES	
Mobile Fraud	Sim swaps, account takeovers,
Email Fraud	Spoofing, Phishing, bogus offers and business email compromise.
Transfer Fraud	Unauthorized transfer of funds from one account to another in the same or different financial institution.
Online Fraud	Makes use of the Internet and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

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

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



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



INDUSTRY PLAYER PERSPECTIVE

NABIHAH RISHAD

Senior Risk Consultant, Serianu Limited

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

CYBER VISIBILITY AND EXPOSURE QUANTIFICATION (CVEQ™) FRAMEWORK

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

Serianu CVEQ™ Framework

08

DID YOU KNOW?

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

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

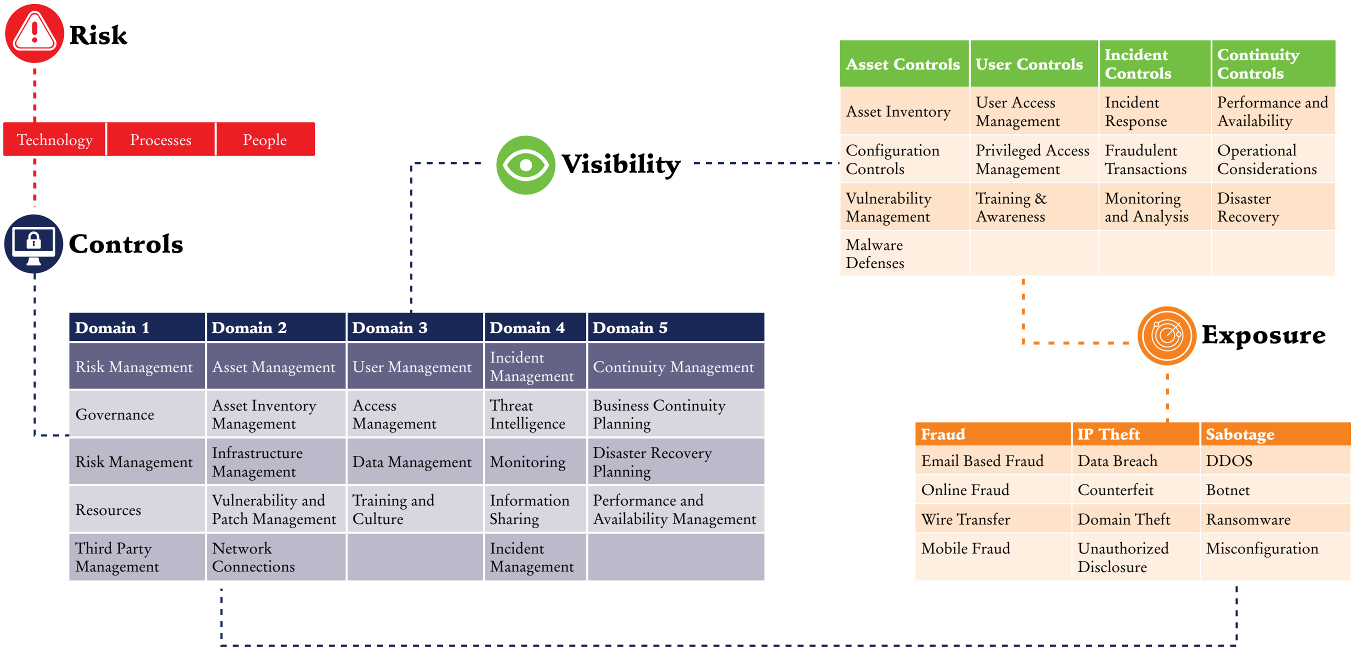
The Cyber Visibility Statements are an effective way to continuously measure your cyber security posture across a range of key security performance indicators. Measuring control effectiveness is a key element in any cyber security risk management process.

The statements include:

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

A Summary of the CVEQ™ Framework

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



Risk

Technology | Processes | People

Controls

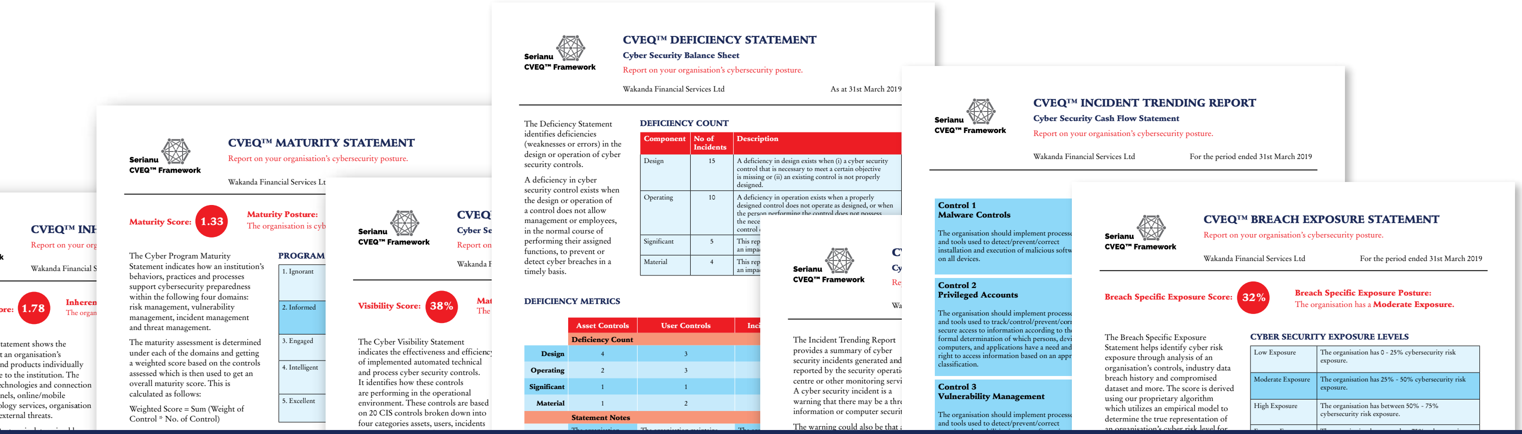
Domain 1	Domain 2	Domain 3	Domain 4	Domain 5
Risk Management	Asset Management	User Management	Incident Management	Continuity Management
Governance	Asset Inventory Management	Access Management	Threat Intelligence	Business Continuity Planning
Risk Management	Infrastructure Management	Data Management	Monitoring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

Visibility

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

Exposure

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


CVEQ™ MATURITY STATEMENT
Report on your organisation's cybersecurity posture.
Maturity Score: 1.33
CVEQ™ DEFICIENCY STATEMENT
Cyber Security Balance Sheet
Report on your organisation's cybersecurity posture.
Visibility Score: 38%
CVEQ™ INCIDENT TRENDING REPORT
Cyber Security Cash Flow Statement
Report on your organisation's cybersecurity posture.
CVEQ™ BREACH EXPOSURE STATEMENT
Report on your organisation's cybersecurity posture.
Breach Specific Exposure Score: 32%
Seriánu CVEQ™ Framework

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 Botswana. Retrieved from http://www.cue.or.ke/index.php/approved-academic-programmes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

https://censys.io/

https://www.shodan.io/

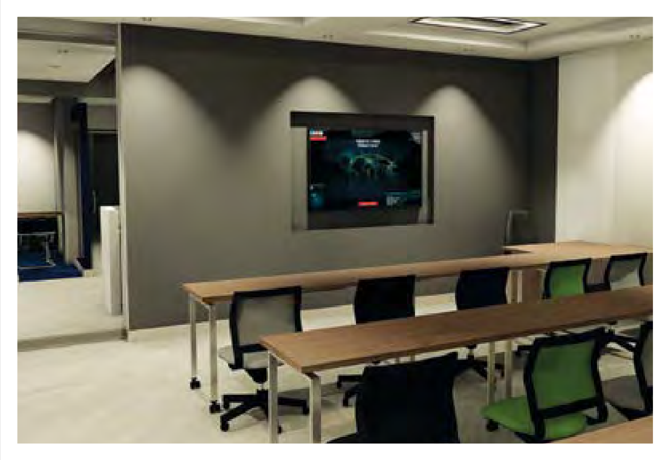
Cybercrime law review: https://www.nation.co.ke/news/Court-suspends-portions-of-cybercrime-law/1056-4585936-thh4s5/index.html

Africa Cyber Immersion Centre

acic

Engage | Educate | Empower

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



For more information contact:

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