SERIANU

Africa Cybersecurity Report

Botswana, 2020/2022

Local Perspective on **Data Protection and Privacy Laws**

Insights from African SMEs

2020/2022

United States International University-Africa

ISACA Gaborone Chapter

African Cyber Security

SERIANU

Africa Cybersecurity Report

Botswana, 2020/2022

Local Perspective on
Data Protection and Privacy Laws

Insights from African SMEs

About the Africa Cybersecurity Report

Africa Cybersecurity Report is a crown jewel of African based intelligence that is released annually by Africa Cyber Immersion Centre (ACIC) in collaboration with its partners. ACIC is Serianu's Research and Development arm, founded in 2017. The report provides an in-depth analysis of unique local trends, threats and attacks. Analysis is drilled down to provide you with specific industry ranking, cost of cybercrime and priority focus areas for organisations. The report pulls intelligence from numerous threat sensors, industry experts, regulators and professional associations and spans over 10 African countries.

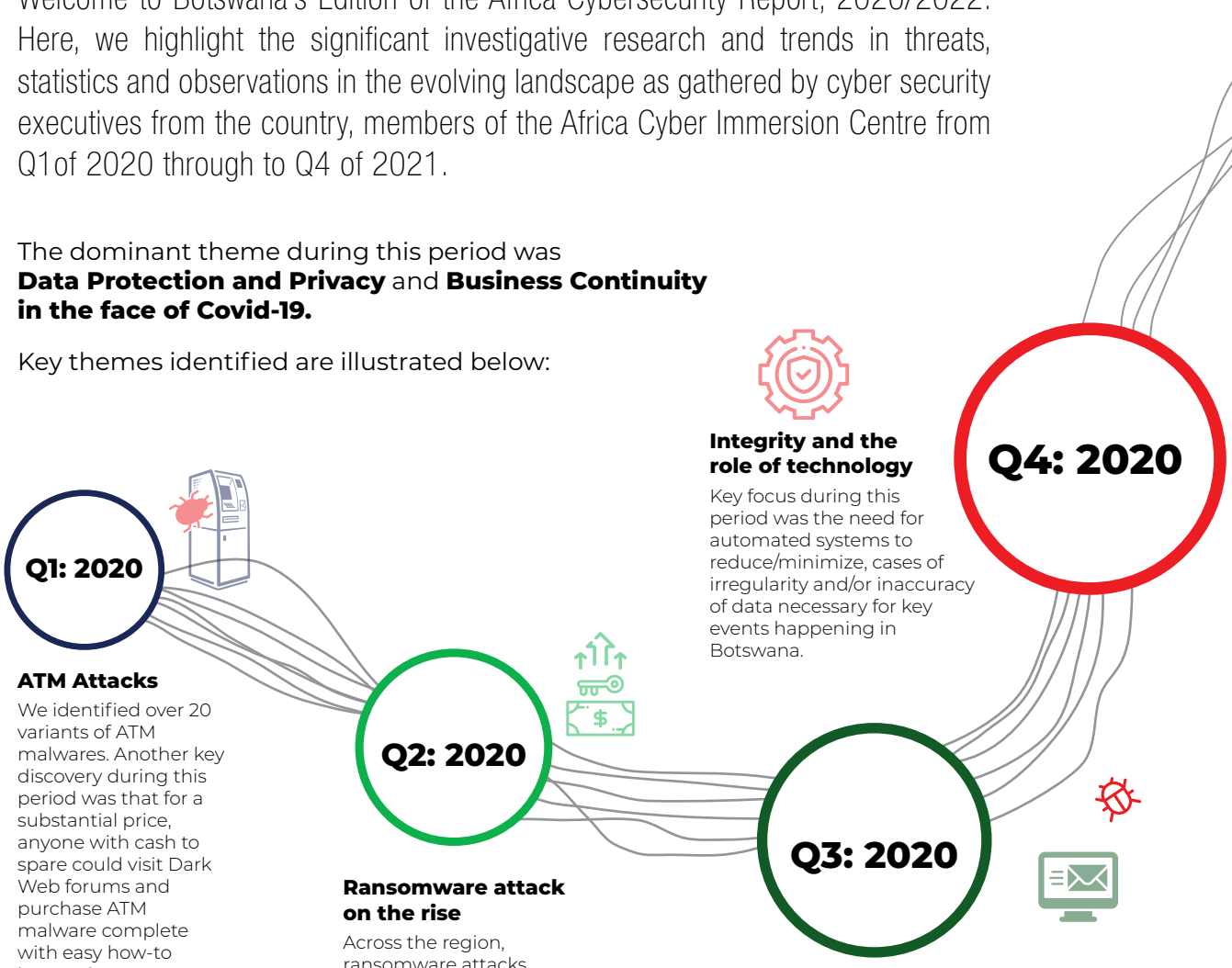
TABLE OF CONTENTS

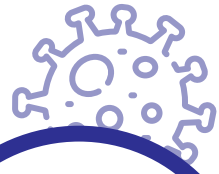
INTRODUCTION

Welcome to Botswana's Edition of the Africa Cybersecurity Report, 2020/2022. Here, we highlight the significant investigative research and trends in threats, statistics and observations in the evolving landscape as gathered by cyber security executives from the country, members of the Africa Cyber Immersion Centre from Q1of 2020 through to Q4 of 2021.

The dominant theme during this period was **Data Protection and Privacy** and **Business Continuity in the face of Covid-19.**

Key themes identified are illustrated below:





Q1: 2021

Business Continuity in the face of Covid-19.

This period was a great test on the effectiveness of existing Business Continuity plans. Organisations faced both security and operational challenges as they adjusted to the travel restrictions, social-distancing regulations and sometimes loss of critical staff.

Q2: 2021

Unsecured remote connections grew by over 23%.

The use of remote access technologies like RDP (Remote Desktop Protocol), VPN (Virtual Private Network) skyrocketed 41% and 33%, respectively globally. Botswana registered 23% increase in unsecured connections.

Q3/Q4: 2021

Gradual adoption of remote working.

As a result of the COVID-19 Pandemic, many organisations in Africa, including Botswana found themselves transitioning their business models. This involved re-architecting IT environments, processes and workforce to work from home securely.

Expectations for the coming year

- The COVID crisis showed that it is important to digitize information, processes and interactions.
- Organisations are moving to more managed services to cope with a rising strain on limited resources.
- Business continuity models have been redesigned to cater for pandemics and remote working.
- Reduced spending on cybersecurity tools due to uncertainty of the future.
- Increased social engineering attacks targeting company executives and senior managers.
- Third party vendors and vulnerable systems will continue to be weak links, forming a primary access compromise point that needs to be checked thoroughly.
- Malware attacks, especially locally developed or re-engineered ones, are expected to rise.
- Other industries will rise to the occasion and develop their own specific cybersecurity guidelines, just as the financial services sector has done.

ACKNOWLEDGEMENTS

In developing the Africa Cybersecurity Report - Botswana 2020/2022, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;

United States International University-Africa

The USIU-A'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 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 Security, an Information Security company focused on offering innovative and holistic top-down trainings and audits for organisations. They 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

- Brencil Kaimba - Researcher and Editor
- Brilliant Kaimba - Researcher, Cyber Intelligence
- Barbara Munyendo - Researcher, Cyber Intelligence
- Margaret Ndungu - Researcher and Editor
- Matthew Wanjohi - Researcher and Editor
- Nabihah Rishad - Researcher, Framework
- Benson Muchiri - Researcher
- David Kamau - Researcher
- Joy Adhiambo - Data Analyst

Contributors

United States International Univesity-Africa

- Varun Sanjay Gupta
- Coulibaly Demba Aboubacar
- Abdihamid Ali Abdi
- Dharmik Hitesh Karania

Multimedia University of Kenya

- Geoffrey Manoti
- Edwin Muema
- Mercy Chebet
- Manyara Bonface
- Kipkosgei Daniel
- Munene Mathendu
- Felix Kipkirui
- Paul Pande

Taita Taveta University

- Stella Kaniaru
- Kenneth Ngumo
- Neville Chenge

Jomo Kenyatta University of Agriculture and Technology

- Allan Wasega

Commentaries

→ **Margretmary Mushango**

Former President of IIA Botswana

→ **Onalenna Giddie**

President, ISACA Gaborone Chapter

→ **Oteng Tabona (PhD.)**

Lecturer in Cybersecurity
Department of Computer Science and Information Systems, Botswana International University of Science and Technology

→ **Tshoganetso Kepaletswe**

Adviser to the National SOC

→ **Dr. June Jeremiah**

PhD Cyber Defense
Director and Cybersecurity Engineer
MCS Security Solutions Pty Ltd

→ **Senwelo Modise - FIP, CIPP/E, CIPM, Security+, ICA CertAML**

Partner – Botlhole Law Group [In Association with Neill Armstrong]

→ **Dr. Paula Musuva**

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

→ **Tshepho Tsheko - Botswana Innovation Hub**

Acting CEO

Africa Cyber Immersion (ACIC) Coordinator

→ **Brilliant Kaimba**

ACIC Training Assistant

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 Africa.

Our **new** Serianu CyberThreat Command Centre (SC^3) Initiative serves as an excellent platform in our mission to improve the state of Cybersecurity in Africa. It opens up collaborative opportunities for Cybersecurity 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

We are immensely pleased to launch our 2nd edition of the Botswana Cyber Security Report. Our previous edition focused on the need for skills development to maintain cybersecurity and achieve cyber resilience.

The first Botswana Cyber Security Report concentrated on the skills gap within our country and reported an annual shortfall of 1,000 cyber security experts that was expected to rise to 5,000 over a 5- year period as demand for cyber security catapulted in the economy. Unfortunately, there has been little improvement in the development of those skills 3 years later. The Covid 19 pandemic made things even more complicated by introducing new dynamics for organisations and businesses which grappled with new ways of working. In Botswana, we saw workers move out of their offices and use their homes as workplaces. Even though this had its benefits, it unfortunately also introduced new cyber risks into our environments.

In order to scale up the country's cyber preparedness, we are glad to note a number of key progressive developments. Firstly, Botswana's National Cyber Strategy is now being implemented and setup of the national Security Operations Centre is progressing well. The government has also initiated a regular national conversation, starting with the inaugural Cyber Security Week that brought together local and international expertise to increase cyber awareness. I look forward to this event becoming entrenched in our calendar.

In this edition we turn to data protection and privacy. With the Data Protection Act now in force, there is now a legal obligation to keep personal data secure. More importantly, we need to be open and transparent about the way we process the personal data that we have collected from all our stakeholders including customers, clients, employees, business partners, suppliers and board members.

Personally, I am no stranger to data protection. I first encountered it in 1984 whilst working in the United Kingdom when the first data protection legislation was passed. Legislative developments in the European Union intensified after Convention 108 of 1981, then eventually morphed into the General Data Protection Regulation (GDPR) in 2018, forcing businesses and organisations, including the government to rethink the way they handle personal data.

The aim of data protection legislation is to provide individuals with safeguards on their personal data and to impose obligations on those that use all forms and types of personal information.

In Botswana's Data Protection Act, these requirements are entrenched in Section 14 where in order to process personal data, a data controller and/or data processor ought to ensure that:

a. Personal data is processed fairly and lawfully, and where appropriate, the data is obtained with the knowledge or consent of the data subject;

b. Personal data that is collected is adequate and relevant in relation to the purposes of its processing;

c. To the extent necessary for processing, personal data is accurate, complete and kept up-to-date;

d. Personal data is collected for specific, explicitly stated and legitimate purposes

e. Personal data is not processed for any purpose that is incompatible with the specified, explicitly stated and legitimate purposes;

f. Personal data is protected by reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, modification or disclosure;

g. Where data is incomplete or incorrect, all reasonable measures are taken to complete, correct, block or delete the personal data, having regard to the purposes for which it is processed;

h. Personal data is not kept for a period longer than is necessary, having regard to the purposes for which it is processed;

i. Personal data is processed in accordance with good practice.

Whilst all these principles are essential for compliance, in this report we focus on the principle of integrity and confidentiality. Failure to implement appropriate technical and organisational safeguards to ensure secure processing attracts a fine of up to P 500,000 or a prison term of 9 years or both. Such failure may also lead to contravention of the provisions of the Act relating to sensitive personal data which then attracts a fine of up to P1,000,000 or a prison term of 12 years or both.

Notably, this legislation moves cyber security beyond the sole responsibility of the IT department, to the ultimate responsibility of the Board.

It is expected that with this shift, many organizations may experience compliance challenges since their respective boards of directors may not have similar technical capacities as Chief Information Security Officers (CISO's) or dedicated IT security professionals.

Though we have a long road ahead, the important thing is we have taken our first steps. I believe by working together with government, academia and the private sector, we will safeguard our personal data and make Botswana the leader in the field of cyber security within our region.

There is no silver bullet that will reduce our cyber risks to zero. I have seen too many examples of expensive technologies that have been purchased and either not properly deployed or poorly configured and lacking expert support.

Similarly, with data protection compliance, we do not expect a one-size fits all solution. Adequate protections begin with a thorough understanding of the personal data being processed and how it flows within and outside the organisations. For us to achieve a high level of protection for our organisations we will need to dedicate the appropriate level of resources, including people, process and technologies.

When these measures have been implemented, we can then look at cyber insurance as a risk mitigation tool and not as a first level of defense. I hope you find this report insightful and I look forward to your comments, questions and contributions.

Pula!

Chris Johnson

CEO, African Cyber Security, Botswana

01

What's new on the scene?

Cybersecurity is a Constantly Evolving Puzzle

In this section we highlight the top trends, innovations and their impact to the overall security posture of organisations.

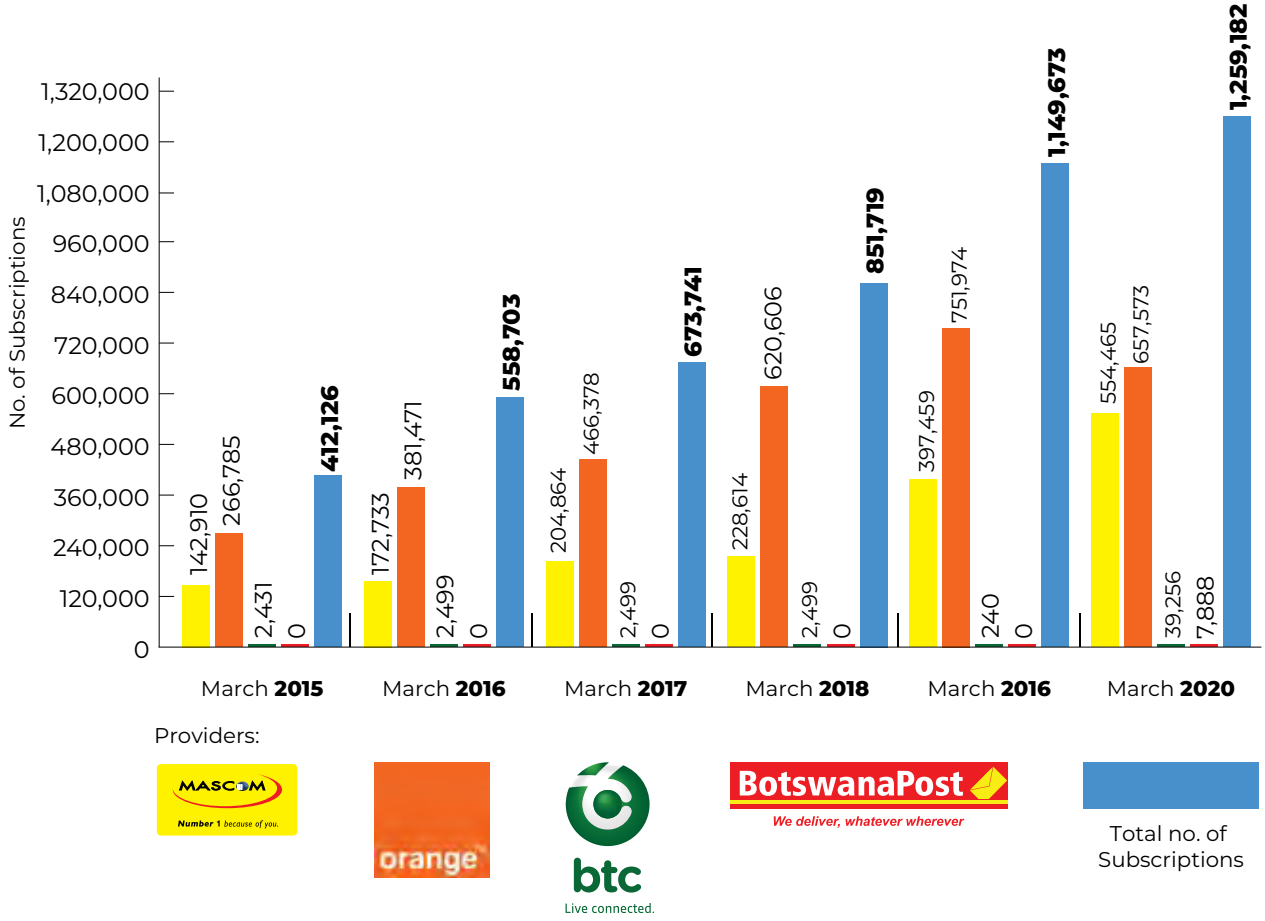
1. BOTSWANA'S CYBER LANDSCAPE

2020/2022 was marked by an increase in both innovation and attacks techniques across all key sectors from financial services, government, manufacturing and insurance.

1.1. TRENDS REALIZED IN 2020

Increase in Internet Connectivity

FIGURE 1. *Mobile money subscriptions as at March 2020.*



Increased Awareness and Collaboration (AppFactory)

The AppFactory (Launched in 2018) equips selected ICT graduates with high-level skills in software development, including secure coding, machine learning, bot framework and data analytics – giving them the critical skills that match today's digital job opportunities.

Increased Adoption of Cloud Technologies

Cloud adoption in Botswana, much like the rest of Africa, is on the rise. The use of Dropbox, ERPs, and Google Apps and Drive has emerged with cloud usage, amongst many internet users. Academic institutions have also heavily invested in cloud technologies for collaboration based programs, communication, application process. Public institutions have adopted cloud storage for their vast data storage needs and banking institutions have incorporated cloud based software as a service for their daily transaction reconciliation. Cloud security is now top of mind.

Increased Risk Exposure for Banks in Botswana

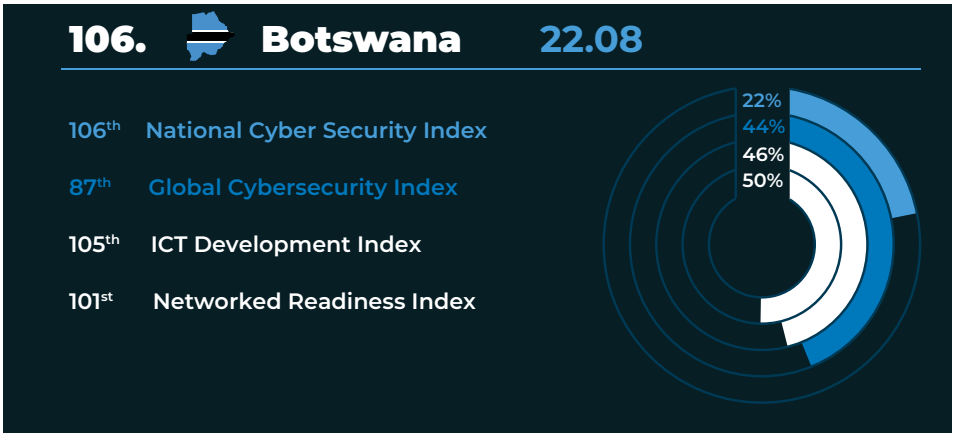
According to the Bank of Botswana Annual Supervision Report 2020, the most common operational risk management weaknesses among banks in 2020, to varying degrees, continued to be the lack of segregation of duties in some functions, lapses in internal controls and information-technology (IT) security. Furthermore, lack of documented procedures for processes, inadequate review of policies and procedure manuals, periodic breaches of internal limits and lack of integration of management information system into the core banking system contributed to an increase in the operational risk. The above deficiencies heightened operational risk thereby increasing vulnerability to cyber-crime risks.

1.2. BOTSWANA'S RANKINGS ON GLOBAL SCALE ARE ALSO POSITIVE

Botswana was ranked 106th in Africa in the 2020 Global National Cyber Security Index. Notable was the country's performance on Data Protection particularly the existence of an independent public supervisory authority that is responsible for personal data protection. The National Cyber Security Index is a global index which measures the preparedness of countries to prevent cyber threats and manage cyber incidents.

National Cyber Security Index (NCSI)

FIGURE 2. *National Cyber Security Index (NCSI).*

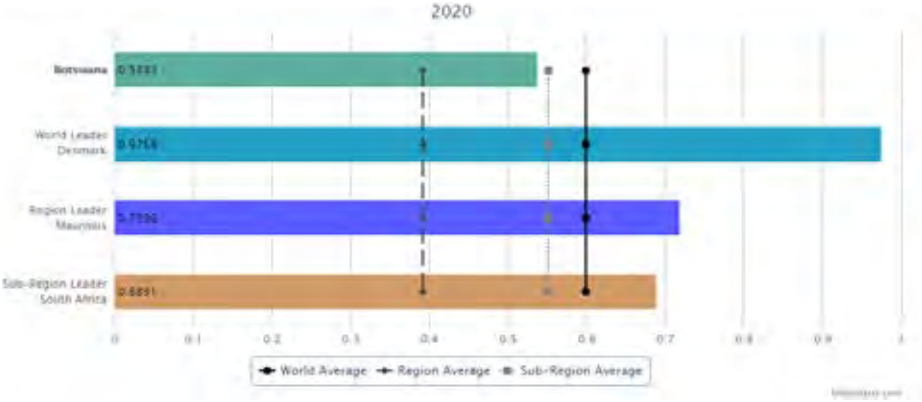


Rank	Country	National Cyber Security Index	Digital Development
69.	Zambia	41.56	35.56
99.	South Africa	27.27	54.80
106.	**Botswana**	**22.08**	**47.95**
107.	Malawi	20.78	27.99
119.	Zimbabwe	15.58	36.03
135.	Namibia	11.69	45.16
145.	Mozambique	9.09	33.03

E-Government Development Index (EGDI)

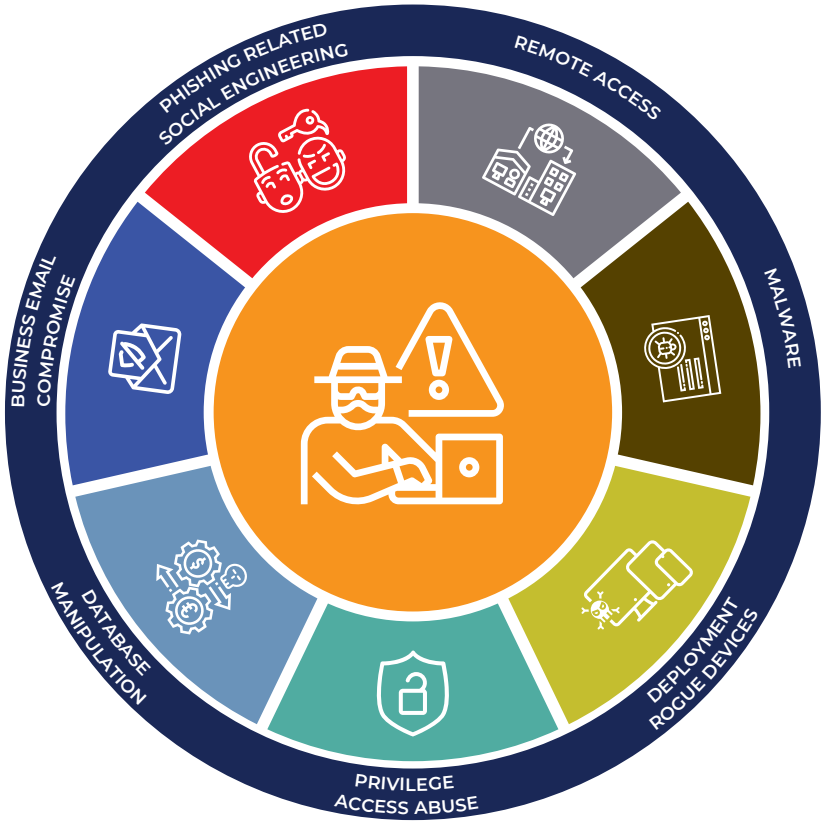
The E-Government Development Index presents the state of E-Government Development of the United Nations Member States.

FIGURE 3: *E-Government Development Index (EGDI).*



Threats and Cyber Crime Trend

FIGURE 4: *Attack vectors across key sectors.*



THE STATE OF CYBERSECURITY IN THE INTERNAL AUDIT PROFESSION

This presents the state of cyber security in the Internal Audit profession.

Internal Audit is responsible for governance, risk and compliance in an organisation. It independently reviews the effectiveness of the programs in place to address cyber security risks and also informs the Board about risk management effectiveness.

Margaretmary Mushango

Former President of IIA Botswana

Internal Audit can play a significant role in the organizational response to cyber security risks.

According to the Institute of Internal Auditors (IIA) Global, internal audit is a trusted cyber adviser. The Institute notes that cyber security must be considered holistically and systematically, as the effects of failure can range from an inability to conduct basic operational processes, to loss of intellectual property.

Increasingly, many companies are recognising the need for a third line of cyber defense – an independent review of security measures and performance by the internal audit function.

Internal Audit should therefore play an integral role in assessing and identifying opportunities to strengthen enterprise security. At the same time, internal audit has a duty to inform the Board Audit Committee that the controls for which they are responsible are in place and functioning correctly. This, understandably, is a growing concern across boardrooms as directors increasingly face potential legal and financial liabilities.

In its position paper on Three Lines of Defense in effective Risk Management and Control, the IIA Global explains that these three lines of defense in an organisation should be properly segregated and operated effectively. This will ensure that cyber security is properly managed, and that ownership is clearly allocated.

According the paper, the Board and Executive Management sit above the three lines of defense, effectively acting as the primary stakeholders for the three lines and being collectively responsible and accountable for setting the organisation's objectives, strategies, governance structures and processes to best manage the risks.

The first line of defense comprises operational management whose responsibilities are as follows:

- Ownership, responsibility and accountability for data, processes, risks and controls.

- This function often resides with system administrators and others charged with safeguarding the assets of the organisations; and
- Administering security procedures, training and testing; maintaining secure device configurations and ensuring that software and security patches are up-to-date; and conducting penetration testing. Amongst other tasks associated with the ownership and management of risks and controls..

The second line of defense comprises risk, security, control, and compliance oversight functions and is responsible for:

- Ensuring that the first line processes and controls exist and are effectively operating;
- These functions often comprise of IT risk management and IT compliance functions;
- Typically facilitate and monitor the implementation of effective risk management practices by management and help risk owners in reporting adequate risk-related information up and down the firm;
- Assessing the risks and exposures related to cyber security against their organisation's risk appetite and ensuring that they are properly aligned; monitoring current and emerging risks and changes to laws and regulations; and collaborating with the first line functions to ensure appropriate control design; and
- Include designing cyber security policies, procedures, training and testing; conducting cyber risk assessments, monitoring incidents, key risk indicators and remediation; and assessing relationships with third parties and suppliers, amongst other things.

At the third line of defense is the internal audit function which is responsible for:

- Ensuring that the second lines of defense are functioning as designed – provides independent and objective assurance to the board and executive management on how effectively the organisation assesses and manages its cyber risks;
- Providing independent ongoing evaluations to preventative and detective measures related to cyber security;
- Evaluating IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration;
- Tracking diligence of remediation; and
- Conducting risk assessments of third parties and suppliers in line with the second line of defense's own work in this area.

CONCLUSION

Internal Audit has a critical role in helping organisations in the ongoing battle of managing cyber threats, by providing an independent assessment of existing and needed controls and helping the Audit Committee and board understand and address the diverse risks of the digital world.

The threat from cyber-attacks is significant and continuously evolving.

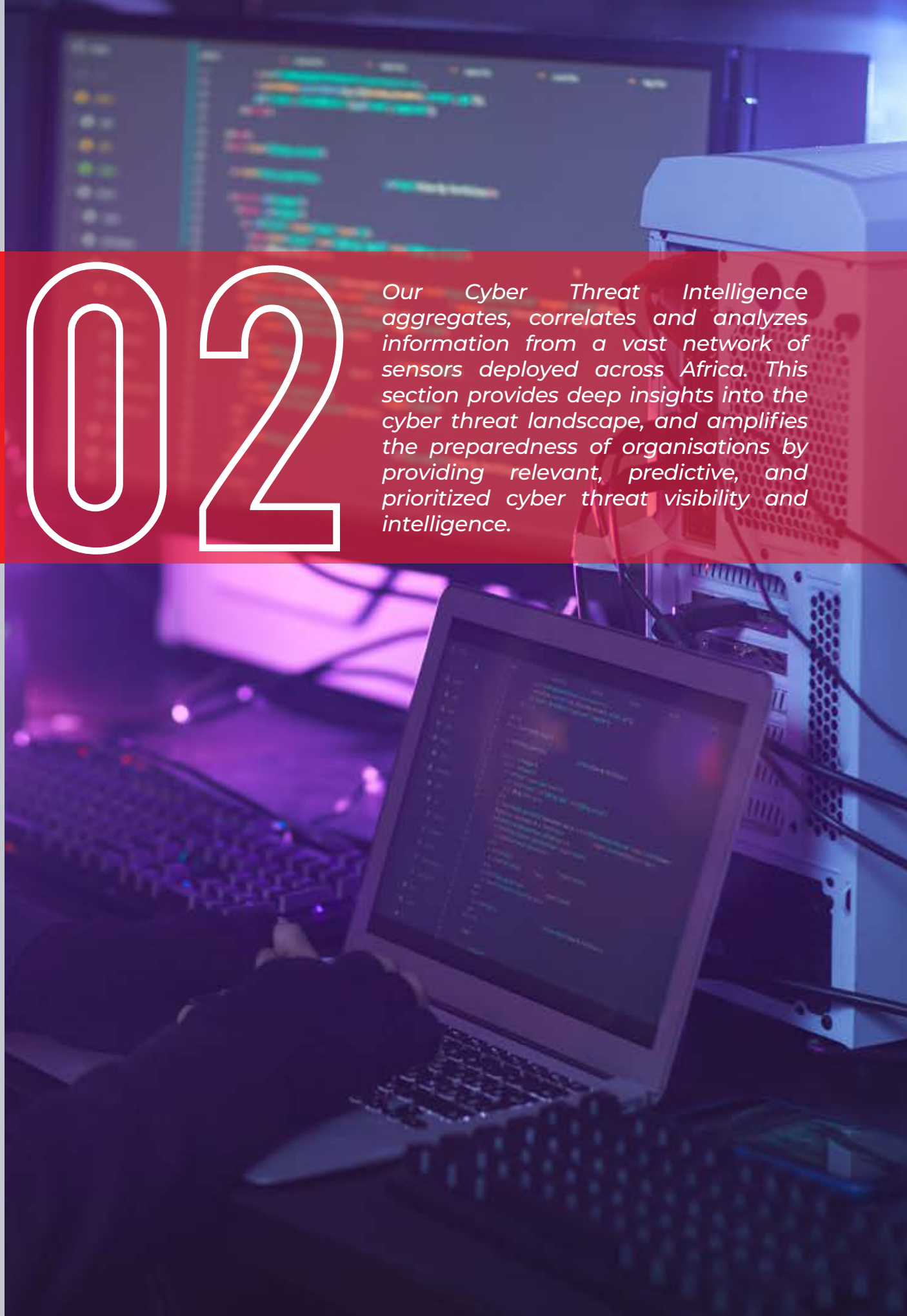
Many audit committees and boards have set an expectation for Internal Audit to understand and assess the

organisation's capabilities in managing the associated risks. An effective first step for Internal Audit would, therefore, be to conduct a cyber risk assessment and distill the findings into a concise summary for the Board audit committee which will then drive a risk-based, multi-year cyber security internal audit plan.

References: Chartered Institute of Internal Auditors, and Deloitte website

02

Our Cyber Threat Intelligence aggregates, correlates and analyzes information from a vast network of sensors deployed across Africa. This section provides deep insights into the cyber threat landscape, and amplifies the preparedness of organisations by providing relevant, predictive, and prioritized cyber threat visibility and intelligence.



2. CYBER INTELLIGENCE

2.1. TOP MALWARES

Botnets

"Botnet" is a combination of the words "robot" and "system". Botnets are usually contaminated with malware that permits programmers to remotely take over use of various devices mostly without the knowledge of the gadget owner.

Approaches to prevent botnet malware:

- Introduce trusted, powerful antivirus applications on your gadget.
- Set your software settings to regularly update automatically.
- Exercise caution on the links you click, download from, or open

Ransomware

This is a type of malicious program (or malware) that assumes control of your PC and threatens you with harm, typically by denying you access to your data. The attacker usually requests a payment, promising to re-establish access to the data upon payment.

The attackers then guide you on the best way to pay to get the decoding key. Typical ransom ranges from a couple of hundred to thousands of dollars, mostly paid in the form of Bitcoin.

Approaches to prevent a ransomware:

- Always make sure your operating system is kept up to date.
- Avoid introducing new software unless you know precisely what it is and what it does.
- Introduce antivirus software, which detects malicious programs like ransomware as they show up
- Use whitelisting software, which keeps unapproved applications from executing at all.
- Back up your documents, oftentimes and automatically. That won't stop a malware attack, but it can considerably reduce the significance of the harm brought about by one.

Crypto jacking

Crypto-jacking is the unapproved use of another person's system to mine crypto-currency. Hackers do this by either getting the victim to tap on a vindictive link in an email that heaps crypto mining code on the system or by contaminating a site or online ad with JavaScript code that auto-executes once it loads on a victim's browser.

Crypto jacking happens when you visit a site that runs a malicious script that hijacks your CPU. You can introduce browser extensions that prevent this from happening.

1. Emotet

A deadly botnet malware that once installed, the malware hijacks email credentials and could even send malicious emails to people in your contact list.

2. Trickbot

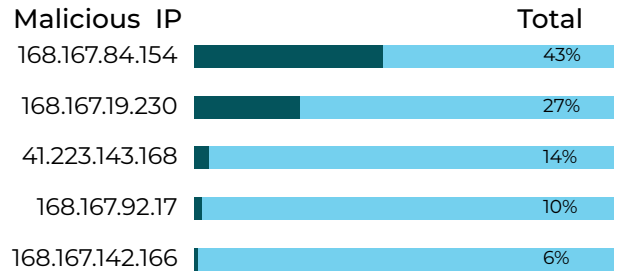
Trojan that can disable Windows Defender. The trojan deploys 17 steps to disable Windows Defender's real-time protection. Trickbot trojan affected nearly 250 million Gmail accounts last time it gained cookie stealing abilities.

3. Ryuk Ransomware

Costliest malware ever, it appeared throughout the year and affected millions of people all over the world.

Top Dictionary Attackers

FIGURE 4. *Top Botswanan Dictionary Attackers.*



Top Email Spammers

FIGURE 5. *Top Botswanan Email Spammers.*

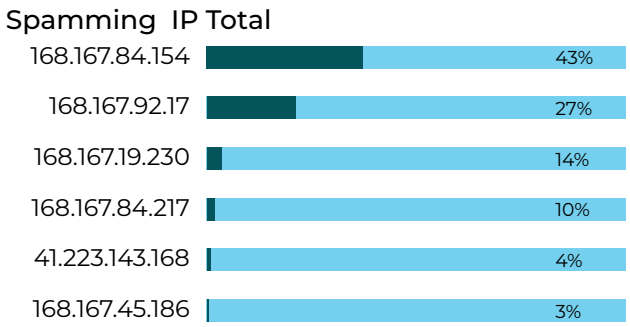


TABLE 5: *Top 10 malware families in Q1-2020.*

	Q1-2019		
	Exploit Target	**Malware Families**	**Botnets**
1	MS IIS	MSOffice/CVE_2017_11882	ZeroAccess
2	ThinkPHP	W32/Agent	Andromeda
3	Apache Struts	JS/ProxyChanger	H-Worm
4	D-Link 2750B	W32/Kryptik	Conficker
5	MS Windows	Riskware/Refresh	Sora
6	Netcore Netis	Riskware/Coinhive	Emotet
7	DASAN GPON	W32/STRAT_Gen	XorDDoS
8	WebRTC	Android/Hiddad	Necurs
9	Apache Tomcat	Riskware/Generic	AAEH
10	Linksys	Android/Generic	Torpig

Source: Fortinet Analysis

TABLE 6: *Top 10 malware detections in Q2-2020.*

	Q2-2019			
	Top 10 Malware Detections	**Africa**	**Top 10 IPS Detections**	**Africa**
1	CVE_2017_11882	188k	ThinkPHP.Controller	3.3m
2	Framer.INF!tr	116k	ThinkPHO.Reqest	2.5m
3	Agent.OAY!tr	63k	PHP.Diescan	2.4m
4	Abnormal.C!exploit	41k	Apache.Struts	1.9m
5	ProxyChanger.ES!tr	38k	Joomla!.Core	1.9m
6	Agent.MUV!tr.dldr	37k	MS.IIS	1.2m
7	Agent.NIK!tr.dldr	34k	Drupal.Core	1.2m
8	Heuri.D!tr	26k	HTTP.URI	1.2m
9	Phish.EMW!tr	20k	MS.Windows	900k
10	RBot.BMV!tr.bdr	20k	HTTP.Header	874k

Source: Fortinet Analysis

TABLE 7: *Most prevalent botnets, malware variants and exploit attempts detected in Africa in Q3-2020.*

	Q3 2019					
	Most prevalent botnets detected	**Africa**	**Most prevalent malware variants detected**	**Africa**	**Most prevalent categories of exploit attempts detected**	**Africa**
1	GhOst	57.20%	HTML/Framer.INF!tr	44.10%	Code. Execution	50.50%
2	Bladabindi	57.30%	JS/Agent.OAY!tr	12.60%	Command.Injection	42.70%
3	WINNTI	47.80%	HTML/ScrInject.OCKK!tr	14.40%	Command. Execution	39.90%
4	Mirai	22.60%	HTML/Download.7031!tr	13.40%	Buffer.Overflow	39.30%
5	Ganiw	20.90%	Riskware/InstallCore	16.30%	Code.Injection	34.50%
6	Pushdo	14.60%	W32/InnoMod.AYH	12.50%	SQL.Injection	33.90%
7	Zeroaccess	12.80%	W32/Injector.EHDJ!tr	11.70%	Information. Disclosure	34.00%
8	Xtreme	8.50%	MSOffice/ CVE_2017_11882.B!exploit	7.90%	Multiple.Vulnerabilities	29.60%
9	Andromeda	27.40%	HTML/Phish.EMW!tr	8.20%	Script.Injection	25.10%
10	Sality	12.30%	JS/Agent.OCQ!tr	5.90%	Argument.Injection	24.80%

Source: Fortinet Analysis

TABLE 8: *Top 20 IPS detections and malware variants in Q4 2020.*

	Q4 2019			
	Top 20 IPS Detections	**Africa**	**Top 20 Malware Variants**	**Africa**
1	ThinkPHP.Controller	34.60%	W32/FlyAgent.K!tr.bdr	11.8
2	vBulletin. Routestring	33.20%	VBA/Agent.QAP!tr.dldr	32.7
3	Joomla!.Core	32.70%	W32/Injector.EHDJ!tr	22.1
4	Drupal.Core	33.10%	W32/Wintri!tr	32.4

5	Apache.Struts	29.40%	HTML/ScrInject.OCKKItr	9.7
6	MS.Windows	28.90%	VBA/Agent. NVEItr.dldr	31.7
7	Dasan.GPON	24.70%	W32/Frauder.ALT!tr.bdr	31.6
8	Bash.Function	15.90%	JS/ProxyChanger.ES!tr	44
9	Apache.Tomcat	19.90%	VBA/Agent. 136E!tr.dldr	3.4
10	MS.IIS	18.10%	VBA/Agent. IP Itr.dldr	5.9
11	PhpMoAdmin.moadmin	16.60%	Adware/AdblockPlus	11.9
12	Java.Debug	18.30%	VBA/Agent. D5 CD Itr	5
13	Red.Hat	15.60%	VBA/Agent. F36A!tr.dldr	11.3
14	WIFICAM.P2P	13.20%	MSOffice/CVE_2017_11882.C I exploit	6.8
15	OpenSSL.Heartbleed	18.40%	W32/Glupteba,B!tr	13.6
16	Plone.Zope	14.20%	W32/CrypterX.IA93!tr	9.9
17	Alcatel-Lucent.OmniPCX	12.90%	W32/Banker!tr.pws	4.1
18	AWStats.Configdir	13.70%	MSOffice/CVE_2017_11882.B! exploit	7
19	MS.Office	20.30%	W32/SillyFDC.A! worm	8.2
20	PHP.CGI	16.10%	HTML/Framer.INFItr	9.1

Source: Fortinet Analysis

2.2. INCREASE IN ATTACKS DURING COVID

Phishing: Volumes of phishing attacks have seen a substantial increase.

Remote access: Errors in configurations for remote working can open vulnerabilities.

Malware distribution: Creative campaigns and new malware variants are on the rise.

Risks from reduced monitoring: With a focus on BCP, monitoring and response capabilities should not get diluted.

Exploitation of new teleworking infrastructure.

2.3. REMOTE CONNECTION VULNERABILITIES IN 2020

Globally, the use of remote access technologies like RDP (Remote Desktop Protocol), VPN (Virtual Private Network) have skyrocketed 41% and 33%, respectively, since the onset of the coronavirus (COVID-19) outbreak. In Botswana, the statistics are as equally staggering. Our research team's analysis revealed the following:

FIGURE 3. *Remote Connection Vulnerabilities in 2020.*

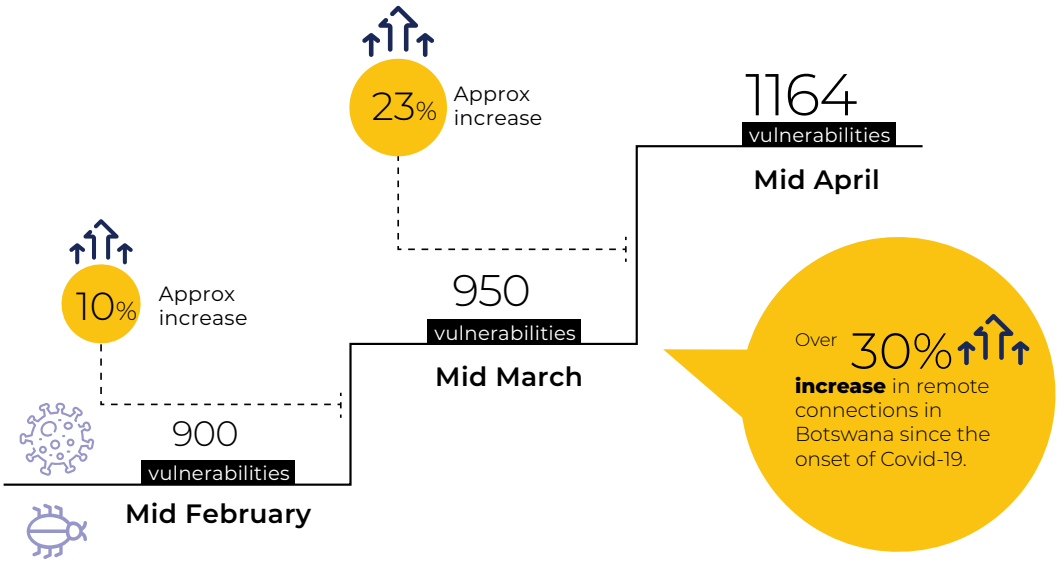


FIGURE 4. *Publicly Accessible Remote Connection Ports in Gaborone (as at November).*

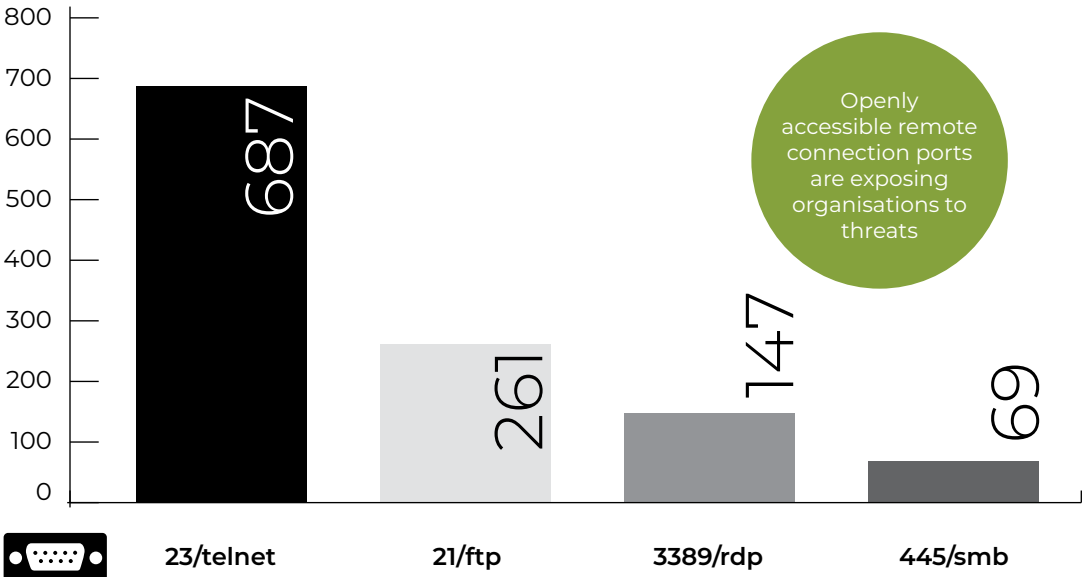


FIGURE 5. *Vulnerable Remote Connections.*

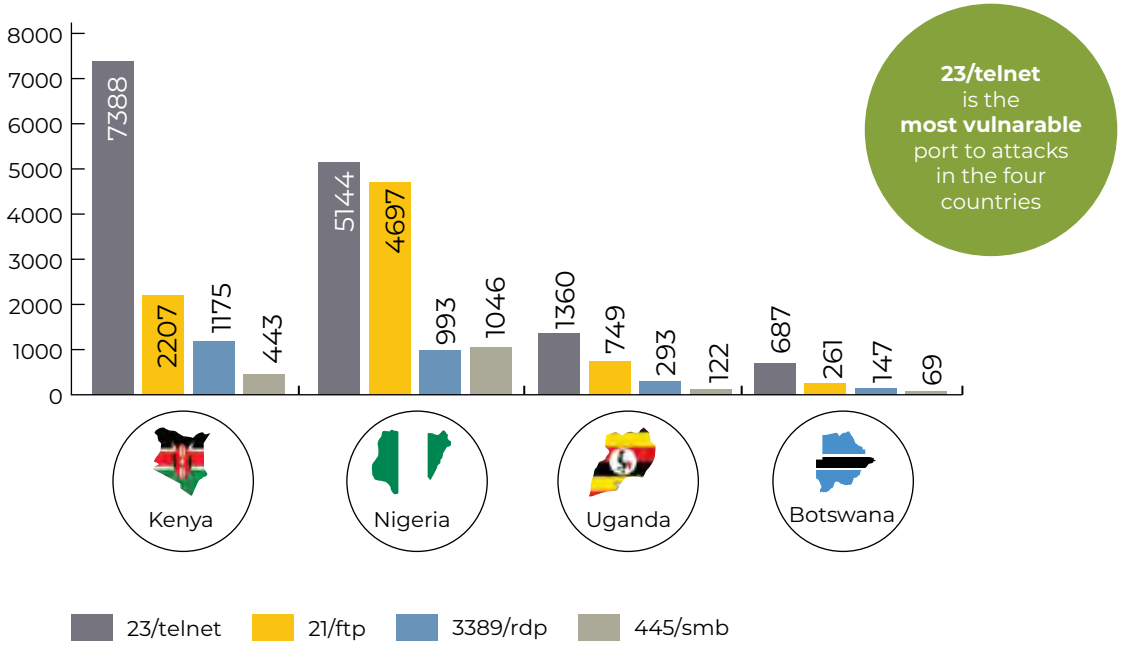
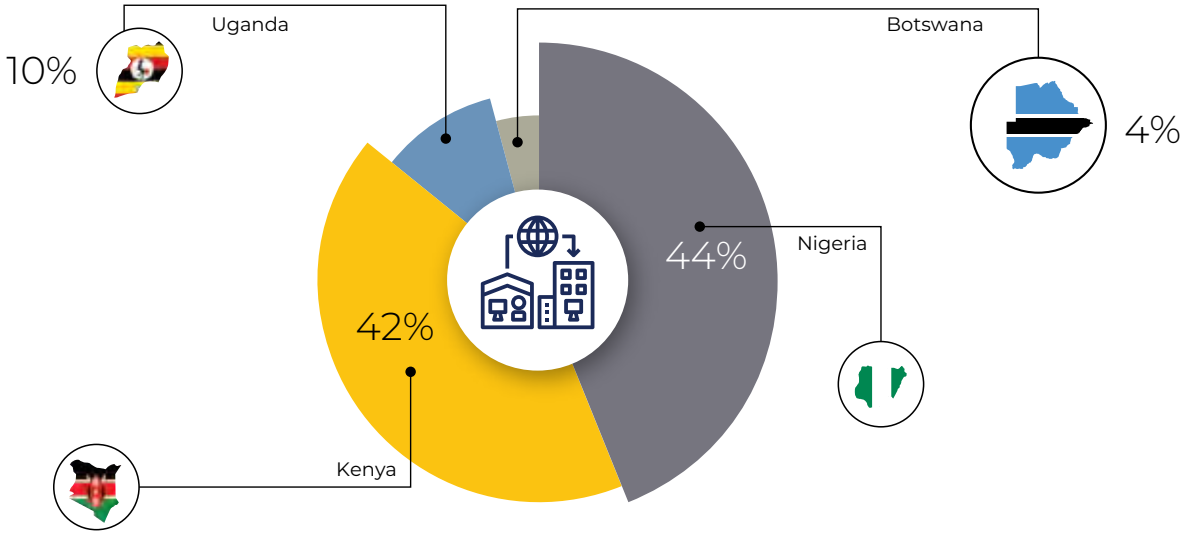


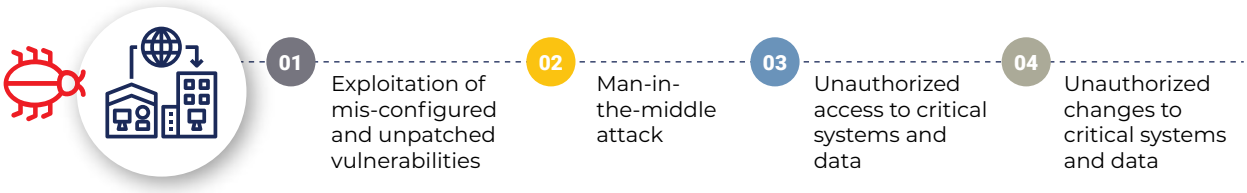
FIGURE 6. *Country Analysis – Insecure Remote Connections.*



2.4. THE RISK

Unsecured remote connections expose organisations to a series of threats increasing the risk of compromise.

FIGURE 7. *Risk of unsecured remote connections.*



2.5. HOW CAN ORGANISATIONS PROTECT THEMSELVES?

It is important to remember any time you open up your organisation to remote access, there is an inherent risk of compromise. Organisations should therefore:

01 Regulate and limit internal and external remote connections.

02 Enable strong passwords and account lockouts.

03 Use two-factor authentication.

04 Inventory and monitor all remote access applications.

05 Audit your network for systems using for remote connection services.

06 Restrict and monitor vendor remote connections.

2.6. EVERYTHING YOU NEED TO KNOW ABOUT ATM SECURITY

ATMs have long been a physical target for criminals due to the limited physical security controls. However, with the growing sophistication of organized crime, self-service cash machines are increasingly becoming the targets of high-tech fraud. Malwares such as Trojan. Skimmer, which steals card and PIN data, and Ploutus, which can be used to trigger cash withdrawals via text messages is becoming a significant threat to financial institutions.

Summary of ATM malware families

There are over 20 strains of known ATM malware. We have profiled four of those strains to give readers an overview of the diversity of malware families developed for ATM attacks.

TABLE 9: *Summary of ATM malware families.*

Malware	Description
WinPot ATM malware	Forces ATM machines to empty their cassettes of all funds.
GreenDispenser Malware	When installed, it displays an 'out of service' message on the ATM, but attackers who enter the correct PIN codes can then drain the ATM's cash vault and erase malware using a deep-delete process, leaving no trace of how the ATM was robbed.
Ploutus	Designed to force the ATM to dispense cash, not steal card holder information. It's introduced to the ATM computer via inserting an infected boot disk into its CD-ROM drive. And an external keyboard (or mobile phone) for executing commands.
Anunak/Carbanak	It arrives as email attachment to a spear phishing email. Once in the network, it looks for and records activities of administrators or bank clerks. The attacker uses this knowledge to move money out of the bank.
Cutlet Maker	It displays information about the target ATM's cash cassettes, such as the type of currency, the value of the notes, and the number of notes for each cassette.
SUCEFUL	Designed to capture bank cards in the infected ATM's card slot, read the card's magnetic strip and/or chip data, and disable ATM sensors to prevent immediate detection.

PRACTITIONER'S VIEW ON DATA PROTECTION IMPLEMENTATION

The main challenge facing the implementation of data protection and cybercrime laws is the level of awareness among the leadership.

Tshoganetso Kepaletswe

Adviser to the National SOC

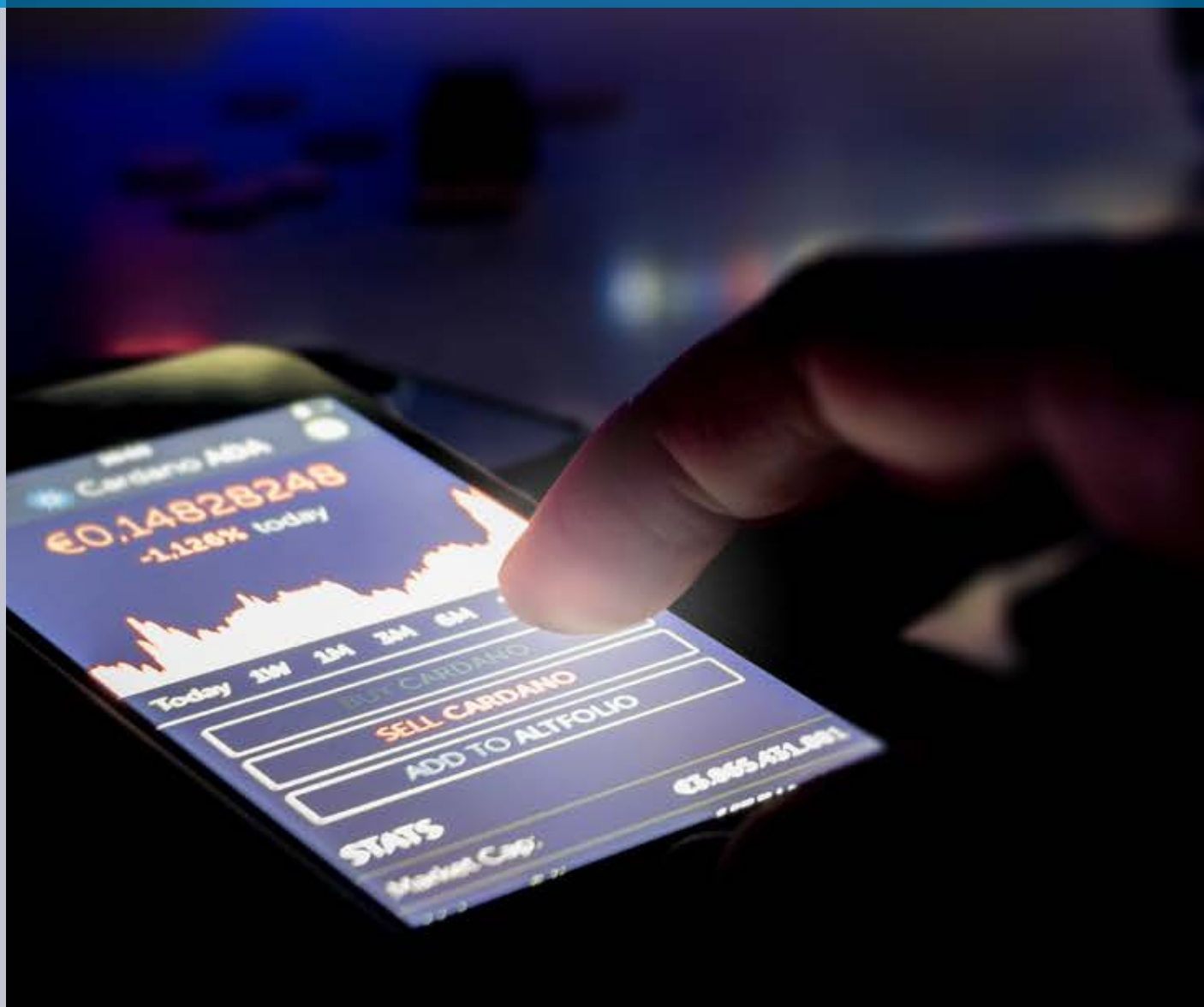
It is very important to implement a detailed consumer education and awareness program among the various stakeholders. The data protection law deals with protection of the personal data of individuals, therefore it is very important to find the right balance in the protection of individual rights and implementing various cybersecurity initiatives. Strong advocacy groups and Non-Governmental Organisations (NGO) for data protection are required to guard against the erosion of individual rights by the cybercrime laws.

Data protection law deals with protection of the personal data of individuals.

03

The 2020/2022 Cybersecurity Survey provides insight into what Botswanan organisations are doing to protect their information and assets, in light of increasing cyber-attacks and compromises impacting them.

Based on the feedback from over 300 IT and security professionals, an analysis of the findings yielded a few notable themes, which are explored in greater detail herein and highlights are summarized as shown.

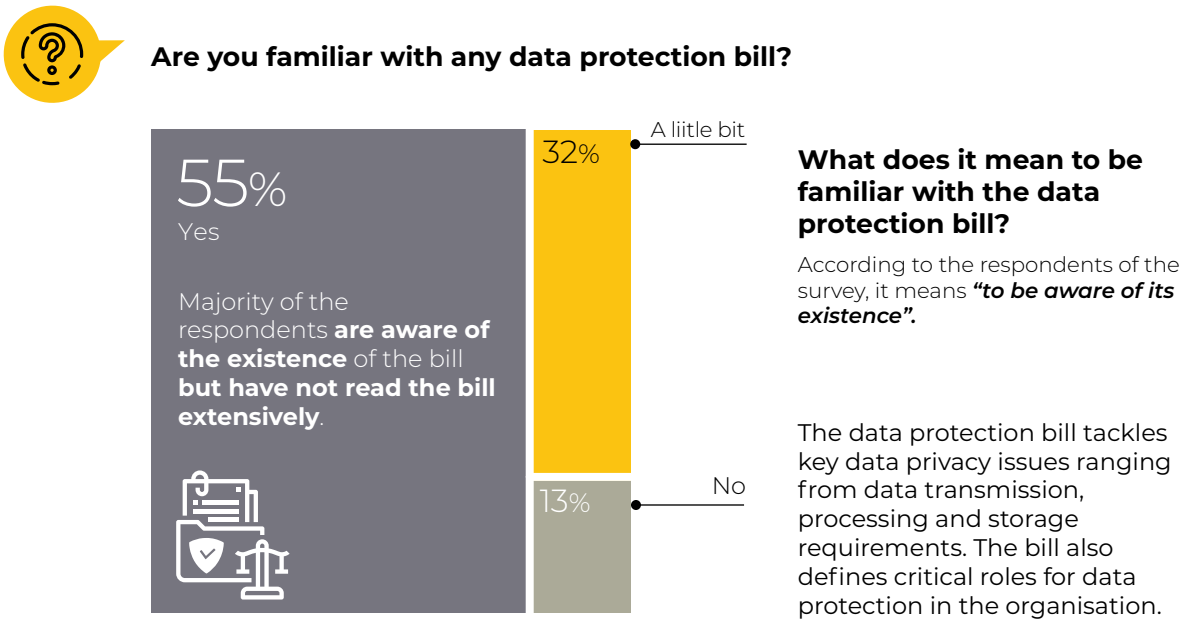


3. SURVEY ANALYSIS

3.1. DATA PROTECTION AWARENESS

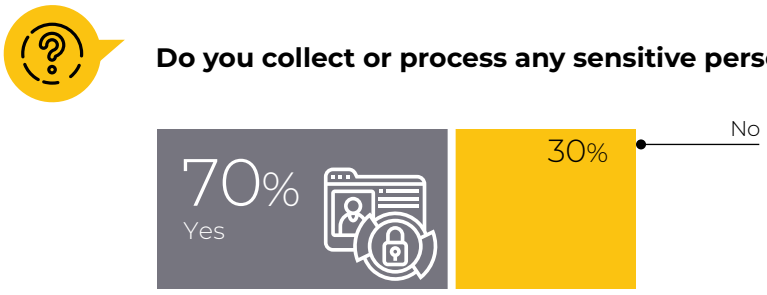
3.1.1. Familiarity with Data Protection Bill

FIGURE 8. *Familiarity with the data protection bill.*



3.1.2. Processing of Personal Data

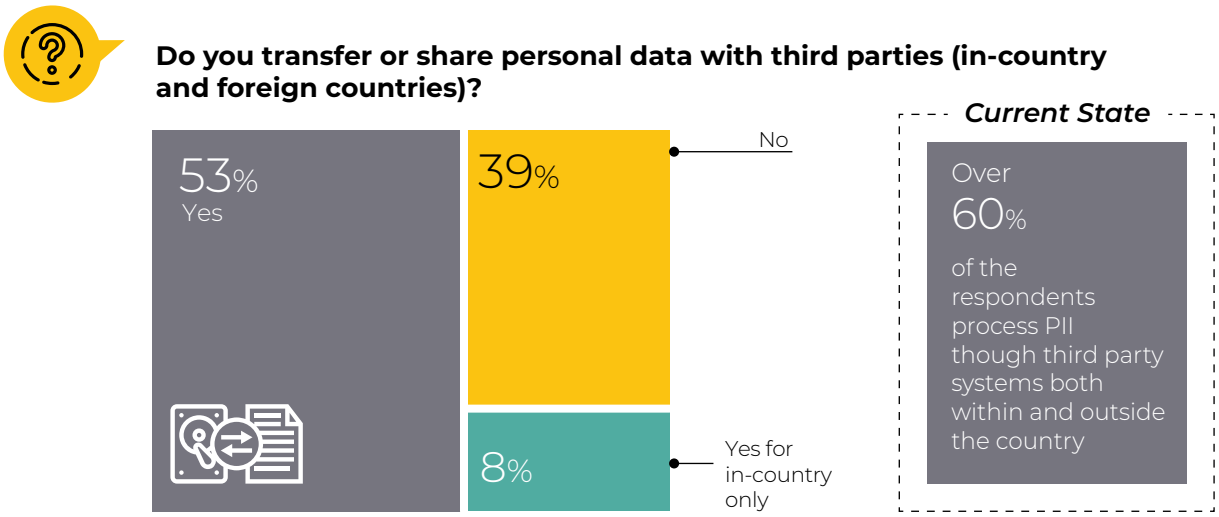
FIGURE 9. *Processing of any sensitive personal data.*



Personal data means information relating to natural persons who are identifiable, directly or indirectly from the information in question; or in combination with other information.

3.1.3. Transfer of Personal Data

FIGURE 10. *Transfer of personal data with third parties.*



Processing means an operation or activity or set of operations by automatic or other means that concern data or personal data and includes:

- Collection, organisation, adaptation or alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data by transmission, dissemination or any other means
- Alignment, combination, blocking, deletion or destruction of information.

Requirement for data processing: The use of personal data for commercial purposes is prohibited unless the person undertaking this processing:-

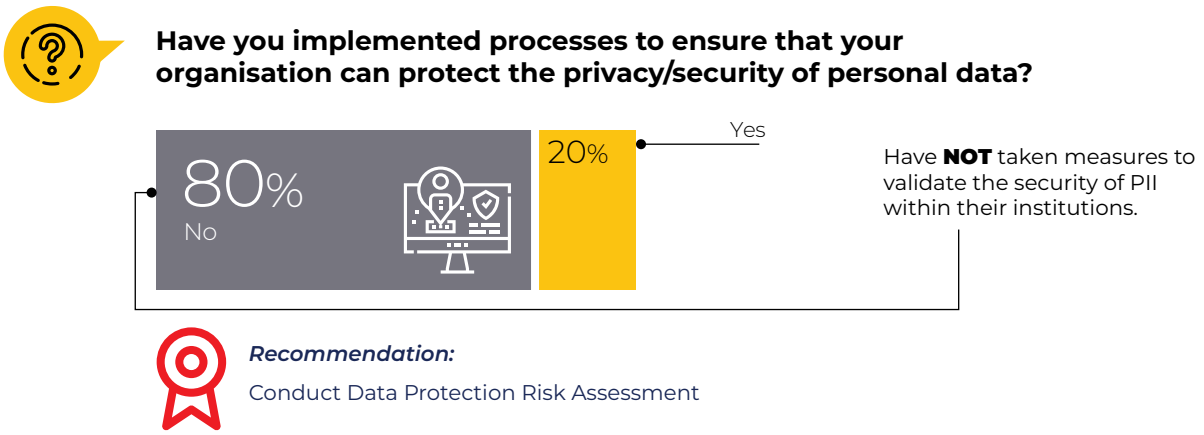
- Has sought and obtained express consent from a data subject; or
- Is authorized to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject

Requirement for data transfer: The transfer of personal data outside Botswana is highly regulated under the Act. Prior to any transfer the data controller or data processor must provide proof to the DPC on the appropriate safeguards with respect to the security and protection of the personal data including jurisdictions with similar data protection laws. The consent of the data subject is required for the transfer of sensitive personal data out of Botswana.

3.2. IMPLEMENTATION OF DATA PROTECTION BEST PRACTICES

FIGURE 11. *Implementation of processes in an organisation.*

Protection of personal data



Requirement: An agency shall take the necessary steps to ensure the integrity of personal data in its possession or control through the adoption of appropriate, reasonable, technical and organisational measures to prevent:

- Loss, damage or unauthorized destruction
- Unlawful access or processing

FIGURE 12. *Effect of of data protection law Implementation.*

Impact of Data Protection Law

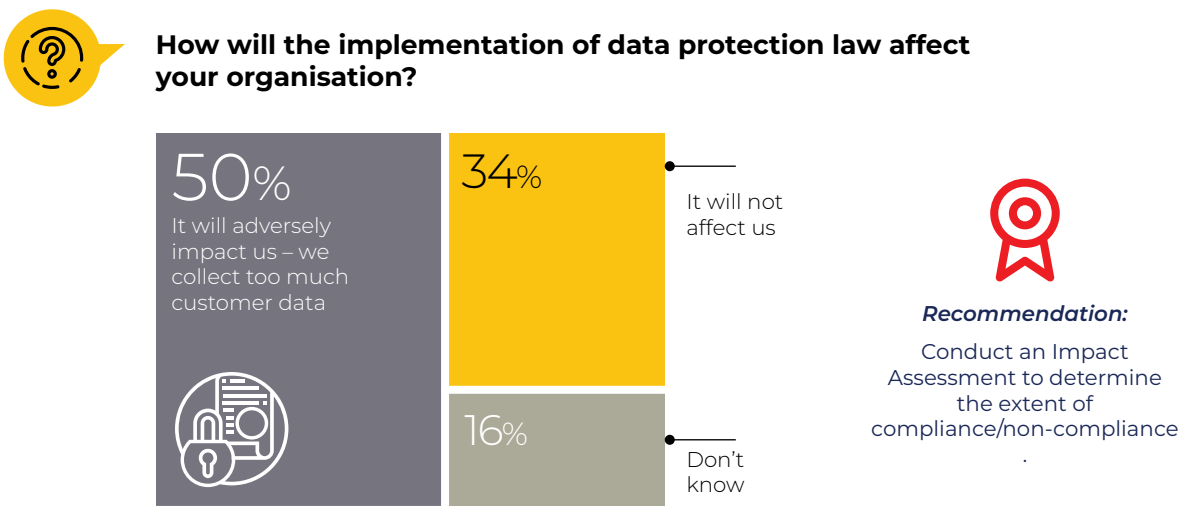
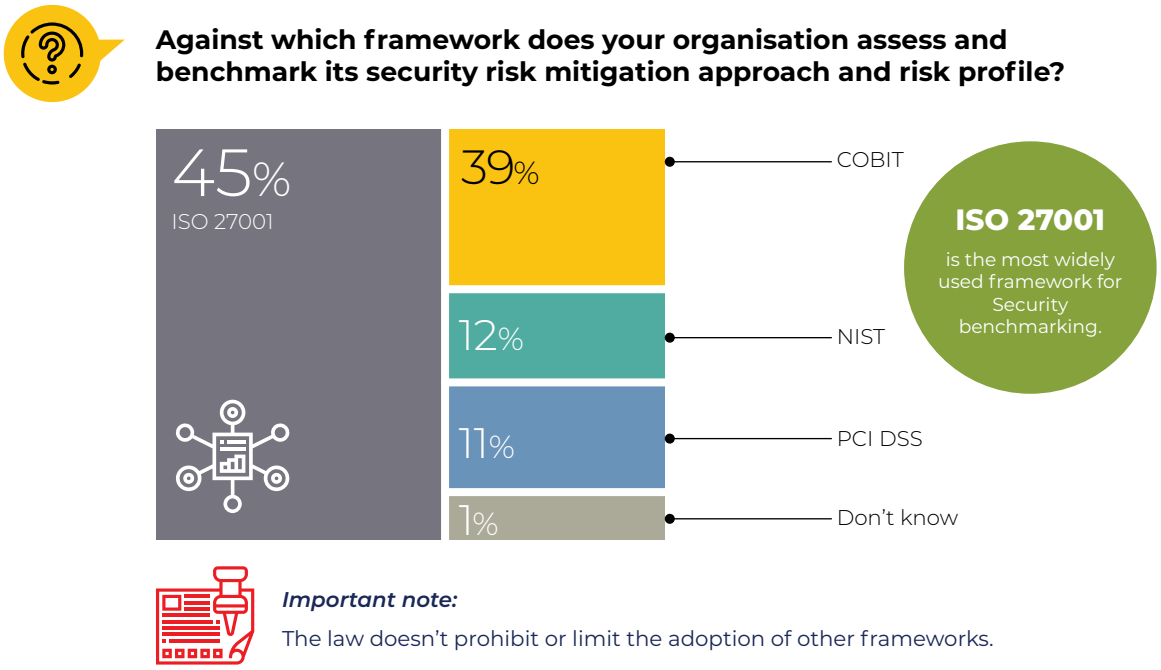


FIGURE 13. *Cyber Risk management frameworks use in organisations.*

Framework for data protection



Why use a Cybersecurity Framework?

The Framework provides a common language and systematic methodology for managing cybersecurity risk. The Core includes activities to be incorporated in a cybersecurity program that can be tailored to meet any organisation's needs. The Framework is designed to complement, not replace, an organisation's cybersecurity program and risk management processes.

The process of creating Framework Profiles provides organisations with an opportunity to identify areas where existing processes may be strengthened, or where new processes can be implemented.

Industry	Framework Adoption			
	ISO 27001	CoBIT	PCI DSS	HIPPA
Banking Sector	✔	✔	✔	
Public Sector	✔	✔		
Healthcare	✔	✔		✔

Complying with multiple cybersecurity regulations

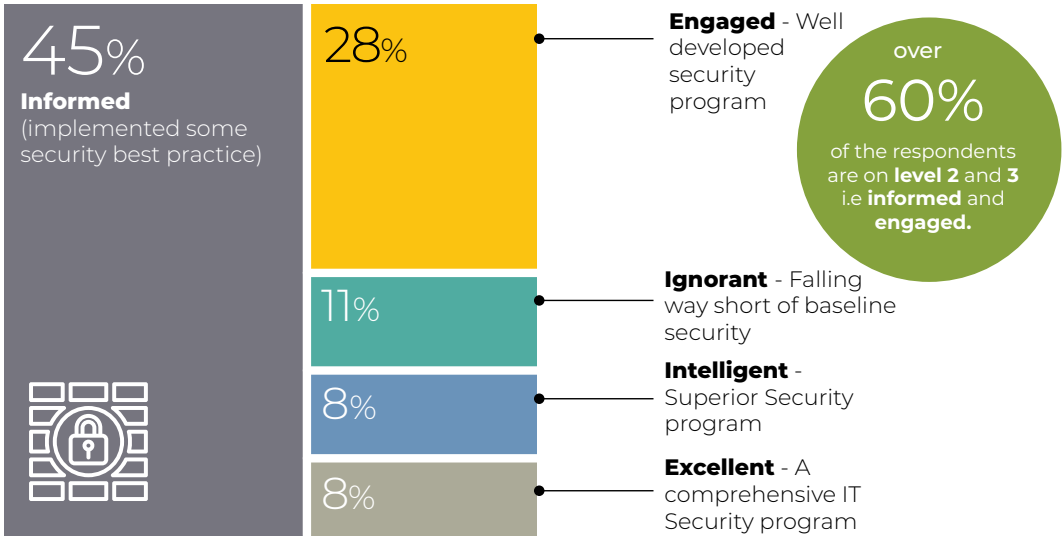
As the number of cyber-attacks continues to rise, businesses are under increasing pressure to protect their systems from cyber-attacks and data misuse. But the challenge of complying with multiple cybersecurity regulations is considerable.

3.3. CYBERSECURITY PROFILE

FIGURE 14. *Organisation's maturity rank.*

Benchmarking Cybersecurity Maturity

On a scale of 1 to 5, 1 being ignorant and 5 being extremely mature. Where does your organizations maturity rank compared to other organizations in your industry?



PRACTITIONER'S VIEW ON DATA PROTECTION AND PRIVACY

What is your opinion on the recently accepted Data Protection Bill 2018 approved in 2021?

"The Data Protection Act defines what constitutes personal data, as well as outlines the rights and obligations of parties involved in the processing of personal data, including the data subject, data controller, and data processor. Further, the Data Protection Act establishes the Information and Data Protection Commission ('the Commission'), which will be responsible for ensuring effective application of the Data Protection Act after its commencement."

Extract from the DPA Bill of 2018.

Onalenna Giddie

President, ISACA Gaborone Chapter

The objective of the Data Protection Act is to regularize and provide protection of personal data by ensuring that those who process personal data do so in a lawful and reasonable manner.

By empowering individuals to take control of their personal data and have a say in how their personal data is used, the Data Protection Act creates transparency and provides the data subject with legal recourse where their personal data is collected or used in an unlawful manner.

Although it has taken over several years to come into operation, I believe it is a welcome development from government to address this topical issue given the current cyber landscape through the significant step of appointing a commissioner to ensure personal data is protected.

Do you think the Commissioner has involved all stakeholders in this process in the implementation of the Data Protection Act?

- Yes. The law was enacted by Parliament having followed all the relevant legislative processes required, including consultation with relevant stakeholders and publishing in the Government Gazette.

What are some of the gaps that you think should be addressed?

- Given the nature of data in Botswana, I believe organisations will require a longer time period than the one year provided for ascension of the Act. Like all legislative pieces of work, the Data Protetcion law has areas of improvement and there are learnings that may be adopted from other Acts in the region, such as POPIA in South Africa, or GDPR. Once the act has become operational in a large number of organisations what is necessary to implement in the Botswana context will become more apparent.

What ways can organisation show compliance to this bill?

- The Act is a 22-page document. For large organisations the Act can be interpreted with the assistance of experienced legal advisors and/or other relevant SMEs in the data privacy/protection space, such as external audit firms.
- For start-ups and other smaller entities, there is a wealth of information available in the Internet. This research can be the starting point to understand the compliance requirements of the act.
- They can also tap into Botswana's ISACA members who constitute professional IT-related professionals in the disciplines of IS/IT audit, risk, security and governance. Our members also include practitioners in the data privacy/protection space, who work in nearly all industry categories, including finance and banking, public accounting and the public sector. As such they play a key role in Botswana's data compliance journey.

What are some of the must have controls every organisation must have to ensure that they are compliant in regard to data protection?

- In looking at the Act, the key focus is in the receipt of consent for storage of personal data and the protection of said data thereof. As such the key steps to compliance will include at a minimum:
  1. The classification of the data in the organisation in accordance with the act;
  2. The appointment of a key person to ensure compliance with the Act – this can be the person who ensures that the responsibilities of the data controller are adequately carried out;
  3. Implementation of controls to safeguard data that has been classified as personal data to ensure that the data is secure
- Most importantly, with this being one of the significant areas pertaining to information security, employees are the 1st line of defense. As such a data privacy and protection culture should be promoted and adopted throughout the organization. Running a data privacy/ protection campaign may assist with compliance.

Is Cyber Insurance a must have for your organisation. Give more insights

- Being part of a global network, our organisation regularly evaluates the risks that arise out of these connections. These risk assessments are then used as an input into determining the risk mitigation products required and include insurance products as and where this has been deemed necessary. In this age where cyber security risk remains a business risk for most businesses, it is advisable for organizations to assess this risk and implement the necessary risk mitigation strategies to obtain in order to obtain the right level of assurance.

FIGURE 15. *Organisation's cybersecurity profiles.*

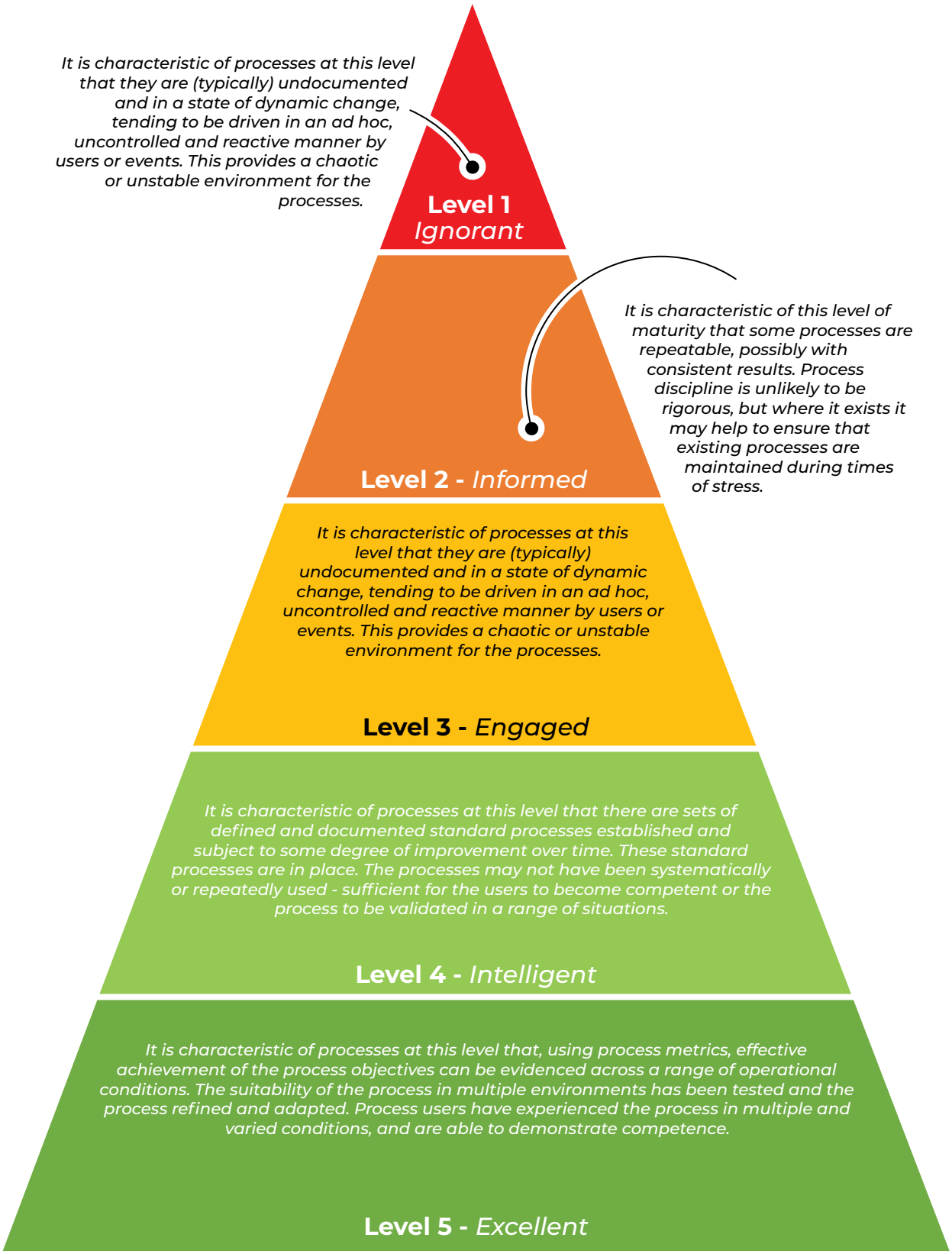
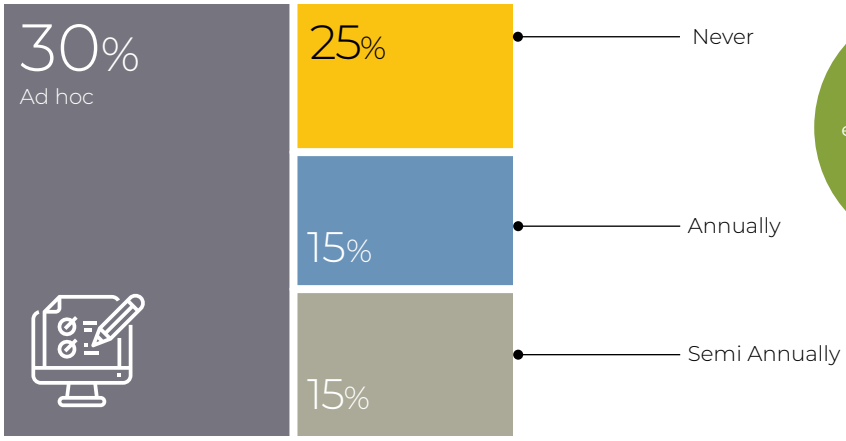


FIGURE 16. *Organisation's frequency of performing cyber breach scenario testing.*

Breach Scenario testing

How frequently does your organisation perform cyber breach scenario testing?



So, your Incident Response Plan looks good on paper – it's been mapped, planned, documented. But has it been tested? Will it work?

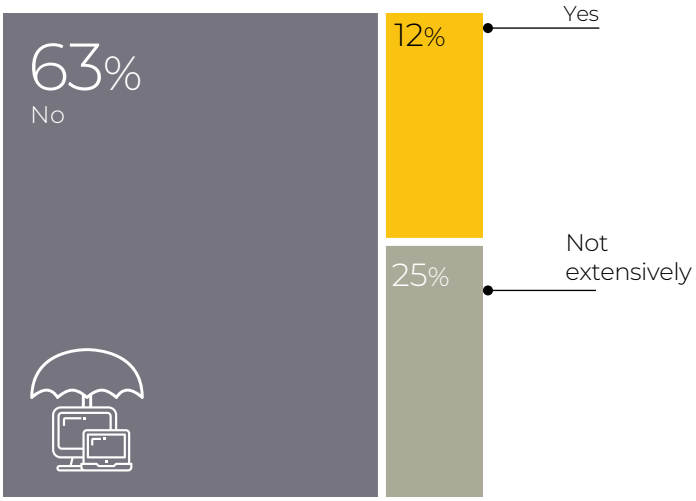
Important note:

Testing your Incident Response plan through breach scenario testing provides employees the opportunity to understand how to respond in the event of an incident. Participating in table top exercises to simulate a real-world scenario is the best way to prepare.

FIGURE 17. *Organisation's frequency of performing cyber breach scenario testing.*

Cyber Insurance

Does your organisation have cyber insurance?



Majority of organisations in Botswana have not taken up Cyber Insurance. Whether its ignorance or low awareness regarding the importance of Cyber insurance, the benefits of having a cover cannot be overstated.

Real Scenario:

Target (USA based Retailer reported a breach in 2013).
Their insurance policy covered 36% of its $252 million data breach costs.

2013 **$61m** cost of data breach

[insurance covered $44m]

2014 **$191m** cost of data breach

[insurance covered $46m]

cost of data breach for 2 years
$252m

cost of insurance policy for 2 years
$90m

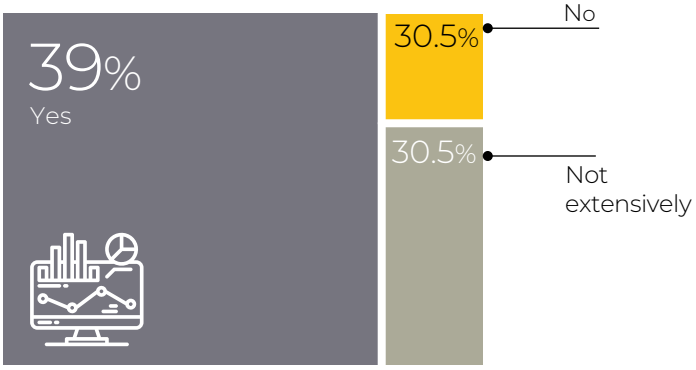
Total Target paid out of pocket

$162m

FIGURE 18. *Reports and metrics to measure cybersecurity posture.*

Reports and Metrics

Do you prepare reports and metrics that go beyond events and incidents to address the institution's security posture?



The biggest gap identified was that, majority of these organisations **don't know what metrics to use to define and measure KPIs.**

You've invested in cybersecurity, but are you tracking your efforts? Are you tracking metrics and KPIs?

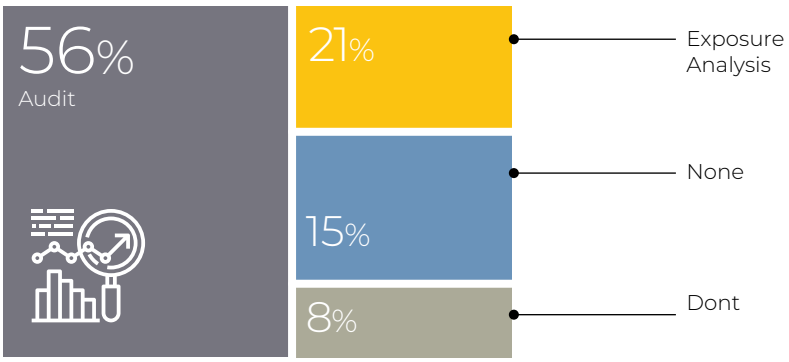
Important note:

You can't manage what you can't measure. And you can't measure your security if you're not tracking specific cybersecurity KPIs. Cybersecurity benchmarking is an important way of keeping tabs on your security efforts.

FIGURE 19. *Establishment of benchmarks metrics for security posture.*

Performance Metrics

How does your organisation evaluate the effectiveness of its cyber risk program?



Majority of organisations perform Audits as a **measure of performance and improvement.**

FIGURE 20. *Use of security testing techniques.*

Security Testing Techniques

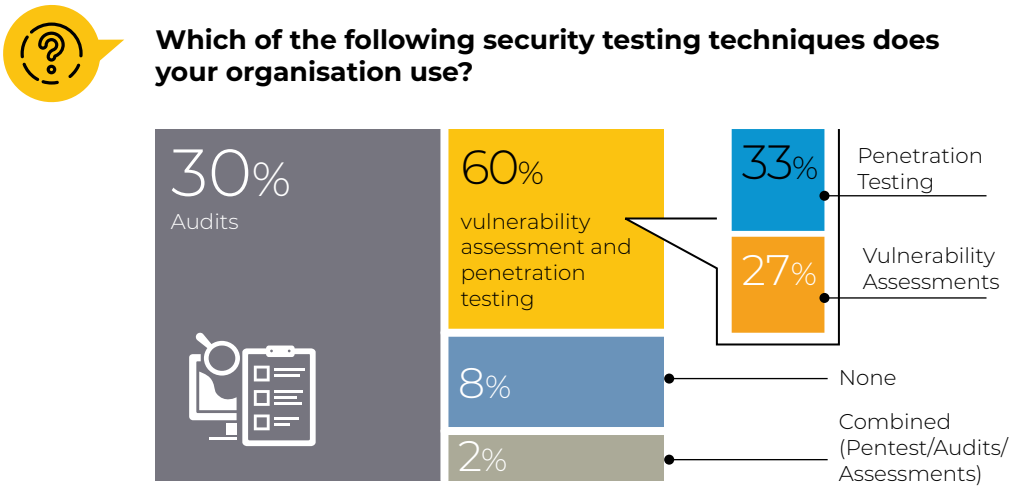
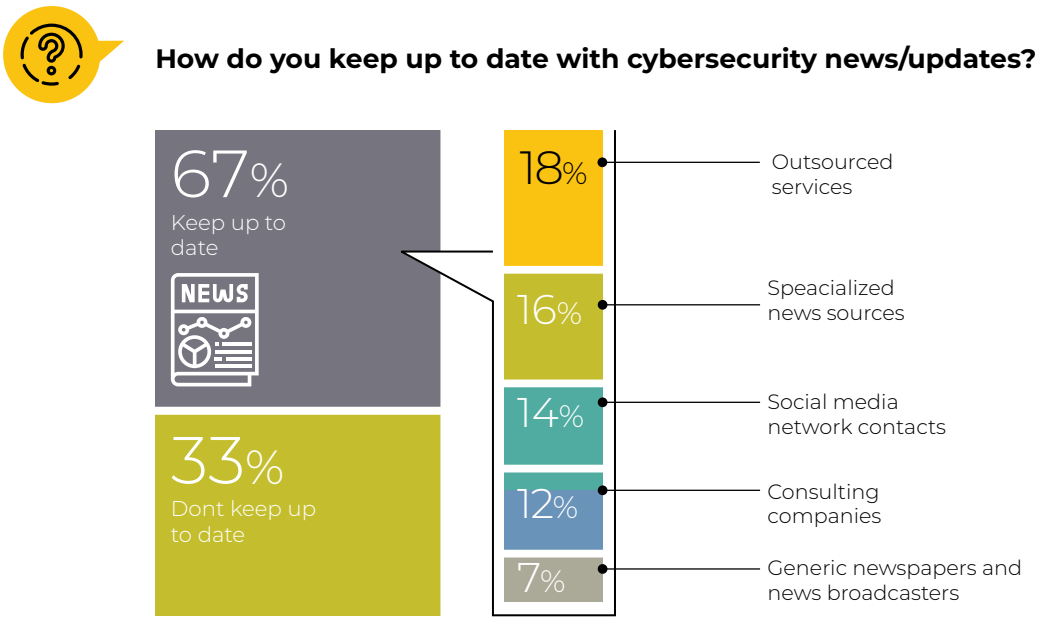


FIGURE 21. *Keeping up with cybersecurity news/update.*

Cybersecurity News



The low rate of Cyber awareness in Africa can be attributed to a myriad of reasons but the most evident is that we do not READ. The internet allows for faster information sharing and in this age, there is no excuse. There are a number of free online news sources such as google alerts, hacker news etc. that allows individuals to keep up with latest trends and news regarding cyber-attacks.

FIGURE 22. *Staff training on cybersecurity risks.*

Cybersecurity Training

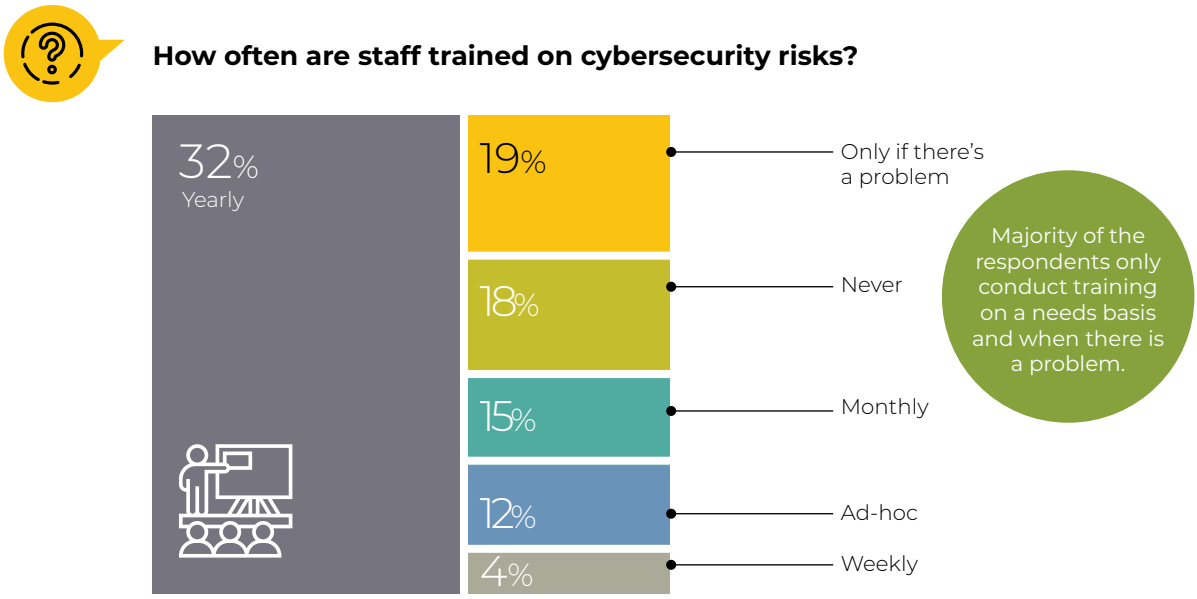


FIGURE 23. *Staff training on cybersecurity risks.*

Cybersecurity Expenditure

PRACTITIONER'S VIEW ON DATA PROTECTION AND PRIVACY

Understanding of Cyber Law:
In your view, what is the intention of Cybercrime/data protection law in Botswana? Does it achieve its goal?

The main aim of the DPA is to control how personal data is used by the organisations, businesses and government. Currently the DPA (2018) of Botswana is not yet enforced so it does not achieve its goal.

Oteng Tabona (PhD.)

Lecturer in Cybersecurity, Department of Computer Science and Information Systems, Botswana International University of Science and Technology

What are the legal implications of data protection laws in Botswana and globally?

- The effects of the Botswana Data Protection Act are not yet applicable since it is yet to be enforced.

How can organisations ensure that they have the right level of consent when capturing data?

- Organisations need to inform customers and other stakeholders about the data they are collecting, how they are going to use it, where it will be stored, what will be stored, in what state will it be stored, and the data retention policies in place.

How have the new regulations (GDPR, Cybercrime Law, Data Protection Law) impacted security practices in general?

- In talking about Cybercrime Laws, we are referring to the Cybercrime and the Computers Related Act and Botswana's Data Protection Act of 2018.
- GDPR has not had an effect locally as generally people are unaware of the regulation and how it impacts how the European Union deals with personal data.
- Since Botswana's DPA of 2018 has not been enforced yet, it has no impact on the general public or local organisations.
- On the other hand, the Cybercrime and Computer Related Act of 2018 has been implemented in a number of cases locally. Some people are aware of its existence, but most are not yet cognizant of what is deemed an offence or not, particularly when interacting on social media.

Cyber awareness and general Internet penetration in Africa is low. How best do we create awareness on Data Protection Laws?

- It is true there is low cyber awareness, but Internet penetration is growing exponentially. According to the ITU, Africa achieved 21% growth in 4G rollout in the past one year. In creating cyber awareness, the focus should be to educate the population about effects of cybercrime and regulation. Educating the nation about existing cybersecurity laws should take precedence over enforcement.

African Culture and Privacy: Africans are known to be culturally social both with finance and data. How do we Africanize the aspect of Data privacy to allow people know what to share and what not to share?

- People are usually unaware of the effects of oversharing especially on social media. Therefore, one way of addressing this issue is to educate them about the consequence of sharing private data online.

Implementation: What do you think is the greatest challenge facing the implementation of data protection and Cybercrime laws in Botswana?

- The greatest challenge is the lack of involvement of all concerned stakeholders in the whole implementation process starting with conceptualizing, drafting, approving and enforcement.

What initiatives would you recommend to reduce the impact of these challenges?

- Identify roles that stakeholders can play in the implementation
- Assign roles to each stakeholder, for example; education training and providers can be given the role to educate the nation about the laws

Flying into the cloud without falling: Cloud computing is a growing trend in public and private sector, what advice would you give to organisations that are transitioning into the cloud?

Based on the SLA the client should verify the following;

- Establish who is responsible for ensuring security of the cloud services
- Establish whether the Cloud Service Provider (CSP) compliance with industrial regulations such as GDPR, Payment Card Industry Data Standard Security
- Research and ensure that the CSP has adequate cybersecurity measure to protect against breaches
- Establish whether the CSP have a policy to notify their client when there is a data breach.

Auditing: The new data protection and policy states that every organisation should conduct a detailed audit of their privacy and data protection practices; in your opinion, do you think organisations have the budget and technical know-how to conduct these audits?

- The value of cybersecurity is not appreciated in Botswana. As a result, majority of companies do not have a budget for cybersecurity. Also, there are few cybersecurity experts in organisations, because companies are not aware of (or have not experienced) the consequences of cybersecurity attacks. In most cases audits are outsourced to companies who specialize in cybersecurity locally.
- Also, it a common trend that majority of cybersecurity companies in Botswana are collaborating with established companies from other countries. This is a concern especially when there are involved in projects of critical national security.

I therefore, recommend that the nation contribute towards building cybersecurity capacity in Botswana to avoid over dependence on other nations.

What is your view on BYOD? What are some of the negative impacts of BYOD to an organisation and should organisations have a no BYOD policy?

- BYOD is a good initiative only if it is regulated. Issues concerning BYOD include malicious apps within the device with backdoors, unauthorized data transfer, outdated operating system and apps just to mention a few. A regulated organisation towards BOYD through policies will enforce compliance and minimize cyber threats.

04

The Data Protection Act, 2018 ('the Act') was assented to by the Parliament of Botswana on 3 August 2018. However, its commencement date is currently on notice.

4. DATA PROTECTION LAW

Country: Botswana **Name of Bill/Law/Act:** Data Protection and Privacy Act (DPPA)
Year Assented: 2018

Prior to the DPA the following legislations were primarily in use:

- **Cybercrime and Computer Related Crimes Act No. 22 of 2007** which is intended to: combat cybercrime and computer related crimes, repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence. The Act is currently being reviewed to address the latest technology changes and related cybercrimes.
- **Communications Regulatory Authority Act No. 19 of 2012,** which provides for the regulation of the communication sector, comprising telecommunications, Internet, Radio communications, Broadcasting, Postal services and related matters.
- **Electronic Communications and Transactions Act No. 14 of 2014** is intended to provide for the facilitation and regulation of electronic communications and transactions. It is to provide specifically for electronic commerce and electronic signatures as well as for matters incidental and connected thereto. The associated secondary legislation (regulations) have also been developed.
- **"Electronic Records (Evidence) Act No. 13 of 2014.** The Act provides for the admissibility of electronic evidence in legal proceedings and authentication of electronic evidence. The associated secondary legislation (regulations) have also been developed. The National Information and Communications Technology Policy commonly called (Maitlamo)" has also been adopted.

4.1. WHAT QUALIFIES AS PERSONAL IDENTIFIABLE INFORMATION ACCORDING TO THE LAW

4.2. TRANSFERRING OF DATA

STAY IN THE KNOW

GET TO KNOW

Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual.

PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

According to the NIST PII Guide,

Items that qualify as PII, because they can unequivocally identify a human being:

Full name (if not common), face, home address, email, ID number, passport number, vehicle plate number, driver's license, fingerprints or handwriting, credit card number, digital identity, date of birth, birthplace, genetic information, phone number, login name or screen.

The transfer of personal data from Botswana to another country is prohibited save for trans-border transfers to countries that have been designated by the Minister through an Order published in the Government Gazette.

Tran's border transfers of personal data require prior authorization to be granted by the Commissioner so as to assess and ensure that adequate levels of protection are provided by the country receiving the personal data. The assessment will be in light of all the circumstances surrounding the data transfer operation and particular consideration will be given to:

- The nature of the data;
- The purpose and duration of the proposed processing operation;
- The country of origin and the country of final destination;
- The rule of law, both general and sectoral, in force in the third country in question; and
- The professional rules and security safeguards which are complied with in that country.

Notwithstanding the above, Trans border transfers to countries which do not offer an adequate level of protection will be allowed where the data subject consents to the proposed transfer or, where the transfer is:

- Necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre contractual measures taken in response to the data subject's request;
- Necessary for the performance or conclusion of a contract in the interests of the data subject between the data controller and a third party;
- Necessary for the public interest, or for the establishment, exercise or defense of a legal claim;
- Necessary to protect the vital interests of the data subject; or
- Made from a register that is intended to provide the public with information and is open to public inspection.

Regardless of the above mentioned restrictions, Tran's border flow of personal data to a country without adequate levels of protection may be authorized where the data controller provides adequate safeguards which may be by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

4.3. SUPPORT SYSTEM FOR DATA PROTECTION

4.3.1. Presence of National Cybersecurity Strategy/CERT/CIRT/CSIRT

Botswana has documented a National Cybersecurity Sccctrategy under the Ministry of Transport and Communications (MTC) collaboration with all the relevant stakeholders from the private sector, relevant ministries, regulator, and academia. The National Cyber Security Strategy clarifies the roles of the various stakeholder and outlines various action plans to be carried out to ensure that the country is cybersecurity secure. The strategy recommends the establishment of Computer Incidence Response Team (CIRT) as a matter of urgency due to rising and complexity of cybersecurity threats and attacks. To ensure a secure cyberspace for Botswana, MTC requested BOCRA to establish a communications sector CIRT to ensure the communication sector both private and public, are secure. The CIRT also acts as the cybersecurity focal point. COMM-CIRT will assume National Cybersecurity responsibilities in the interim, while awaiting the Establishment of the National CIRT (BWCIRT).

BENEFITS OF HAVING A CSIRT

Having a dedicated IT security team helps an organisation to mitigate and prevent major incidents and helps to protect its valuable assets.

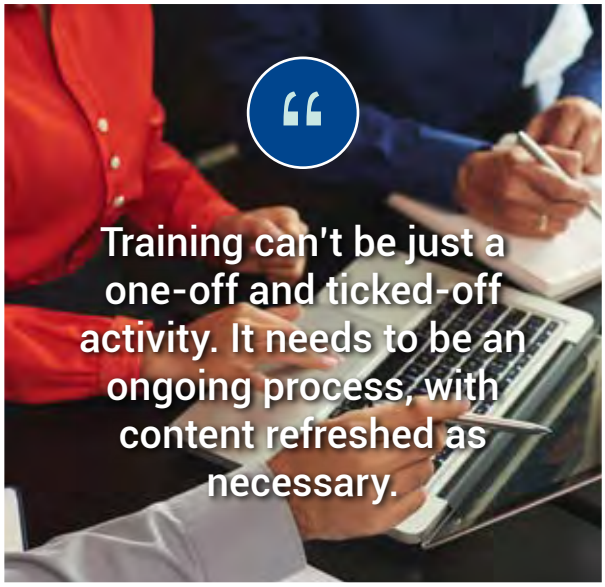
- Having centralized coordination for IT security issues within the organisation (Point of Contact, PoC).
- Centralized and specialized handling of and response to IT incidents.
- Having the expertise at hand to support and assist the users to quickly recover from security incidents.
- Dealing with legal issues and preserving evidence in the event of a lawsuit. Keeping track of developments in the security field.
- Stimulating cooperation within the constituency on IT security (awareness building).

4.3.2. Training and awareness

An awareness program for data protection can be used to support and reinforce training. The need to create an awareness campaign is to deliver the message on the following issues; keeping passwords safe, confidentiality, personal data breaches and individual rights.

Training requires a feasibility study to identify the need to carry out training which include;

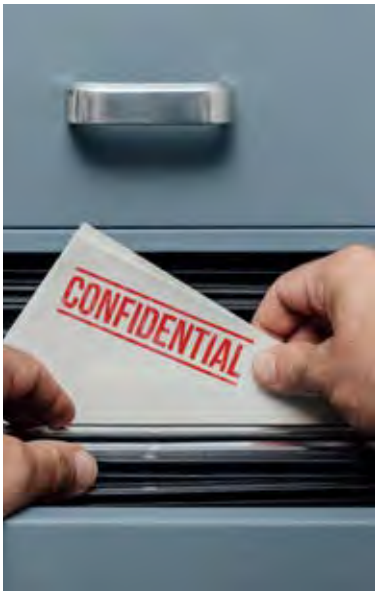
- Instructor-led workshops/classes (delivered by an internal or external instructor)
- Instructor-led webinars/video links
- Online or offline learning



PRACTITIONER'S VIEW ON DATA PROTECTION AND PRIVACY

What is your opinion on the recently accepted Data Protection Bill 2018 approved in 2021?

Understanding what the public want from data protection is key. However, the public views can appear to be contradictory to what they say and what is reflected in their behavior. Likewise, the attitude of the public toward the protection of data and personal data is difficult to characterize as one common view between the public and Data Protection Authorities (DPAs).



Dr. June Jeremiah

PhD Cyber Defense, Director & Cybersecurity Engineer, MCS Security Solutions Pty Ltd

For the Botswana Data Protection Act to be effective the Commission needs to understand what the public is concerned about, how they understand their data protection rights, what they expect Commission to do to uphold their rights, and how they would like to be empowered by the Commission to use them.

There is, of course, no 'one size fits all view on what the public is concerned about, at a more granular level there are much more nuanced views on sharing their data and how this should be used by organisations, and what they would like to see from Information. There are however several themes that appear from the views of the public across Botswana.

The commonly recurring themes of what the public wants from data protection are;

- control over their data;
- transparency, they want to know what organisations will do with their data;
- to understand the different purposes and benefits of data sharing;
- security of their data; and
- specific rights of access, deletion, and portable personal data.

The themes of what the public wants from the Commission are;

- **Independence:** Commission's free from outside influence.
- **Consistency:** where possible a consistent approach to data protection across Botswana aligned with industry standards.
- **Visibility:** Commission Officers making themselves known, providing clear help and guidance to the public and to organisations.
- **Compliance Certification:** Industry compliance certifications, seals, and trust marks that give the public confidence in how organisations in Botswana process their data compliant with the laws and regulations
- **Responsive to new technologies:** The Commission should understand data privacy implications that come with new technology as we become more dependent on technology in our daily lives
- **Enforcement:** there should be effective and appropriate remedies that the commission follows to ensure that organisations in Botswana comply with data protection rules.

The Commission needs to be proactive and creative in response to what the public wants to benefit the most often limited budgets, alongside increasing numbers of complaints and data privacy implications that come with new-driven technologies. Both the public and organisations in Botswana have different expectations about the Data Protection Act and what it should be able to deliver it is usually impossible and unrealistic to meet all these. A balance must be set between ensuring the public have access to tools and means that support them to voice out their rights and ensuring the organisation does comply with the laws and regulations.

Do you think the Commissioner has involved all stakeholders in this process in the implementation of the Data Protection Act?

- Major stakeholders responsible for protecting user privacy. Protecting user privacy is a responsibility not only limited to device manufactures, services, and app developers but also of users themselves. Government also has a key role to play to governing the standardization processes.

What are some of the gaps that you think should be addressed?

With more and more governing bodies implementing data protection and privacy laws, it is becoming more significant for organisations to mitigate cyber risk within their IT Infrastructure before they encounter a data breach and a hefty fine. In the age of zero trust where personal data is becoming valuable to malicious attackers, the governing bodies need to come up will laws and regulations which enable organisations to deploy and implement innovative security measures to protect data to avoid privacy gaps that many organisations in Botswana will get trapped in. To minimize security risks and increase data protection and privacy these common privacy gaps need to be addressed:

- **Security Testing:** For organisations in Botswana to comply with the Data Protection Act and respect public privacy rights they need to keep their data secure. Diligent security testing in form of vulnerability assessments and penetration testing should be performed regularly at least twice annually.

- **Privacy Policies:** Organisations in Botswana when gathering personal data from the public, need to have proper access to privacy policies that are clear and easily understandable and explain individual privacy rights. This can be in a form of online privacy statements or written, organisations need to implement policies that meet regulatory requirements and review them annually to keep up with new emerging cyber threats.

- **Continuous Monitoring:** You can further protect private information by implementing continuous monitoring of your organisation's processes to be notified of risks and gaps that need to be addressed. This can be achieved through the deployment of Security Operation Centers (SOC) within the organisation to have clear visibility of their threat landscape to prioritize and remediate cyber risk before being exploited by attackers.
- **Employee Training:** Humans will remain the weakest link in cybersecurity, however educating employees on rising cyber threats transform them into becoming the first line of defence to protect and secure data. Training should be done regularly to ensure employees upload privacy laws when managing personal data within organisations.
- **Data Mapping:** For an organisation in Botswana to secure and protect privacy they must understand where they store data and who has access to it. Data mapping is significant in the creation of proper data transfer records for your systems.

What ways can organisation show compliance to this bill?

- Cybersecurity Compliance involves meeting various controls (usually enacted by a regulatory authority, law, or industry group) to protect the confidentiality, integrity, and availability of data. Compliance requirements vary by industry and sector, but typically involve using an array of specific organisational processes and technologies to safeguard data. Controls come from a variety of sources including HIPPA, PCI DSS, the NIST Cybersecurity Framework, and ISO 27001 can assist origination in Botswana to meet compliance requirements of this bill.

What are some of the must have controls every organisation must have to ensure that they are compliant regarding data protection?

- Despite the business size and industry, you operate on, in this connected world of internet of thing and big data odds are organisations in Botswana already have or will have some form of sensitive personal data in their possession. The three main basic security controls that organisation must have to ensure they are compliant with Data Protection Act these includes confidentiality, integrity, and availability, which are often collective called CIA or the CIA triad. The Confidentiality control is based on the principle of the least privilege restricting each user's access to the minimum required to perform their jobs. Data security controls that promote least privilege include ACLs, encryption, two-factor authentication, strict password protocols, configuration management, and security monitoring and alerting software. Establishing guidelines for appropriate authorization and prevention of unauthorized access is a key confidentiality component. Integrity is aimed at protecting data from modification by unauthorized users and improper modification by authorized users. To verify integrity, you can use hashing algorithms and digital signatures. Availability involves ensuring that authorized users can access information and information systems in a timely and uninterrupted manner.

Is Cyber Insurance a must have for your organisation? Give more insights

- It is not surprising you have heard that it no longer matters when a data breach will occur to your organisation but it's a matter of when and how much it will cost. Despite investment in high-tech security mechanisms which enable security in-depth humans remain to be the weak link in cybersecurity openly falling prey to various cyber-attacks. With cyber insurance, the organisation will be in a better position to mitigate cyber incidents. It is no doubt organisations in Botswana still think "that if a data breach is inevitable, to what extent it is sufficient to attempt to secure personal data aligned to Data Protection Act? The truth is cyber insurance coverage is significant to most organisations in Botswana and the type of data they possess, and this is crucial to how the organisation manages and protects personal data. Organisations in Botswana should implement an information security management system that is aligned with industry-standard which will ensure proper management of personal data and mitigation of complicate cyber threats such as ransomware attacks risks through cyber insurance. Just because you have auto insurance, doesn't mean you drive recklessly so does apply to cybersecurity insurance.

Training can't be just a one-off and ticked-off activity. It needs to be an ongoing process, with content refreshed as necessary.

Those responsible for data protection should work closely with HR and/or training teams to ensure data protection training is implemented and effective.

Creating and embedding training that includes information security, data protection and privacy, e.g. collecting data, lawful use, data retention, following company policies etc. is not easy, but can perhaps be encouraged by using motivators and incentives.

4.3.3. Fines

The DPA carries severe penalties for non-compliance. The penalties are a combination of fines and a possibility of imprisonment. The minimum fine for non-compliance is BWP 20 000.00 with a maximum fine of BWP 1 million. Prison sentences range from a minimum of three years to a maximum of 12 years.

TABLE 10: *Breakdown of DPA fines in Botswana.*

Crime	Fine	Other consequences
A person who has access to personal data and is acting under the authorization of the data controller or the data processor but refuses to process personal data only as instructed and has prejudice to any duty or restriction imposed by law	Not exceeding BWP20 000	Imprisonment for a term not exceeding three years, or both
Processing of sensitive personal data without the required authorization	Not exceeding BWP500 000	Imprisonment for a term not exceeding nine years, or both
Failure to provide the addressee with an optional opt-out facility	Not exceeding BWP10 000	Imprisonment for a term not exceeding five years, or both
Originator who persists in sending unsolicited commercial communications to an addressee who has opted-out from receiving such through the originator's opt out facility	Not exceeding BWP50 000	Imprisonment for a term not exceeding eight years, or both
When data controller fails to implement safeguards	Not exceeding BWP500 000	Imprisonment for a term not exceeding nine years or both
A data controller who processes personal data despite the objection made by the data subject	Not exceeding BWP500 000	Imprisonment for a term not exceeding nine years or both
Failure of data controllers and data processors to immediately notify the Commissioner of any breach to the security safeguards of personal data	Not exceeding BWP100 000	Imprisonment for a term not exceeding three years, or both
Data controller who doesn't inform a data subject of the rights conferred on the data subject under this Act commits an offence	Not exceeding BWP100,000	Imprisonment for a term not exceeding three years or both
Data controller who processes sensitive personal data in contravention under this Act commits an offence	Not exceeding BWP100,000	Imprisonment for a term not exceeding twelve years or both

4.4. HOW TO PROTECT PERSONAL IDENTIFIABLE INFORMATION?

Multiple data protection laws have been adopted by various countries to create guidelines for companies that gather, store, and share personal information of clients. Some of the basic principles outlined by these laws state that some sensitive information should not be collected unless for extreme situations.

Also, regulatory guidelines stipulate that data should be deleted if no longer needed for its stated purpose, and personal information should not be shared with sources that cannot guarantee its protection.

- Identify the PII your company stores
- Classify PII in terms of sensitivity
- Delete old PII you no longer need
- Establish an acceptable usage policy
- Encrypt PII
- Eliminate any permission errors
- Develop an employee education policy around the importance of protecting PII
- Create a standardized procedure for departing employees
- Establish an accessible line of communication for employees to report suspicious behaviour.

4.5. CHALLENGES

Implementation of these laws

The Commission is the competent authority that will be tasked with protection of personal data through effective application and compliance with the DPA. However, since the DPA has not yet commenced, there is currently no enforcement

Reporting and prosecution of these breaches

The development of the National Cybersecurity Strategy (NCS) enables the government and other stakeholders to establish appropriate measures that would ensure Confidentiality, Integrity and Availability (CIA) of networks, systems and data as ICT services are offered to the public.

Botswana developed the National Cybersecurity strategy that enables government and other stakeholders to establish appropriate measures to ensure enhanced security in the public. Despite this statistics indicate that there is still an increase in registered cases for the past four years - 56 registered cases by September 2018, 39 registered in 2017, 25 in 2016 and 23 in 2015.

In the four years, a total of 143 cases were recorded, according to the Botswana Police Service.

Skills shortage

According to our previous analysis (2018), Botswana recorded less than 100 Cybersecurity professionals. Botswana is faced with the challenge of shortage of digital forensic examiners, which inhibits the prosecution of cybercrime offences with offenders going unpunished and companies and individuals losing millions of Pula through such offences.

4.6. PRINCIPLES OF DATA PROTECTION

01 **Disclosure:** Data subject shall be informed of the purpose to which the information shall be put and the intended recipients of that information at the time of collection.

02 **3rd party:** Information shall be collected directly from and with consent of the data subject, where information relation to the data subject is held by a third party, the information may only be released to another person or put to a different use with consent of the data subject.

03 **Retention:** Information shall not be kept for a longer period than is necessary for achieving the purpose for which it was collected, unless

- The data subject consents to the retention;
- The retention of the data is required by virtue of a contract between the parties to the contract.

04 **Publicly available information:** An agency shall not be required to collect personal data directly from a data subject where the data is a matter of public record.

05 **Misuse of information:** An agency that holds data that was obtained in connection with one purpose shall not use the data for any other purpose.

06 **Commercial use of data:** A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this act unless it has sought and obtained express consent from the data subject.

07 **Protection of Children:** An agency shall not process personal data of a child unless the processing is

- Carried out with the prior consent of the parent or guardian or any other person having the authority to make the decisions on behalf of the child.
- Necessary to comply with the law.
- For research or statistical purposes.
- Publicly available

08

Securing the data: Appropriate technical and organisational measures shall be taken to safeguard the data subject against the risk of loss, damage, destruction of or unauthorized access to personal information.

09

Notification of security compromises:

- Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or processed by unauthorized person, the agency shall
  - As soon as reasonably practicable after the discovery of the unauthorized access or processing of the data, notify the commission and the data subject;
  - Take steps to ensure the restoration of the integrity of the information system.
- A data subject may request an agency that holds personal data relating to the data subject to correct, delete or destroy false or misleading data
- The agency shall consider the request and inform the data subject of the decision within 7 days of the receipt of the request.

10

Oversight and enforcement:

The commission shall oversee the implementation of and be responsible for the enforcement of the act. (Monitor, investigate and report on the observance of the right to privacy).


MASTER
35
0
30
25
20
15

EXTRACTING VALUE WHILE PROTECTING DATA

Data is the new oil of the digital economy. We have heard this metaphor used a number of times. It seeks to illustrate the increasing value of data as the fuel for today's digital economy, which just like oil, needs to be processed from its raw form, refined and converted to different forms in order to draw real value.

Dr. Paula Musuva

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

The phrase is credited[1] to a British mathematician Clive Humby who coined it in 2006 and was later popularized in 2017 by The Economist when it published an article titled *"The world's most valuable resource is no longer oil, but data"*[2].

However, many do not agree with this analogy because oil is a finite, non-renewable and polluting resource that leading economies are moving away from as they seek to go carbon-neutral by 2030[3] and others by 2050[4].

According to United Nations Conference on Trade and Development (UNCTAD)[5] 27 African countries have enacted Data Protection and Privacy Legislation with 9 countries in the process of finalizing their draft legislation for enactment. This is commendable progress since Africa is noted to be ahead of the Americas and close to Asia-Pacific region. The European region is a clear leader with 96% of the countries having legislation in place with the European Union's 2016 General Data Protection Regulation (GDPR) being a model law for many countries around the world.

It is expected that innovative technologies build on Artificial Intelligence, Machine Learning, robotics and data science will be crucial in driving economies in the fourth

[1] *https://www.quora.com/Who-should-get-credit-for-the-quote-data-is-the-new-oil*

[2] *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*

[3] *https://www.euronews.com/2020/09/07/how-the-eu-is-trying-to-make-one-hundred-cities-carbon-neutral-by-2030*

[4] *https://ec.europa.eu/clima/policies/strategies/2050_en*

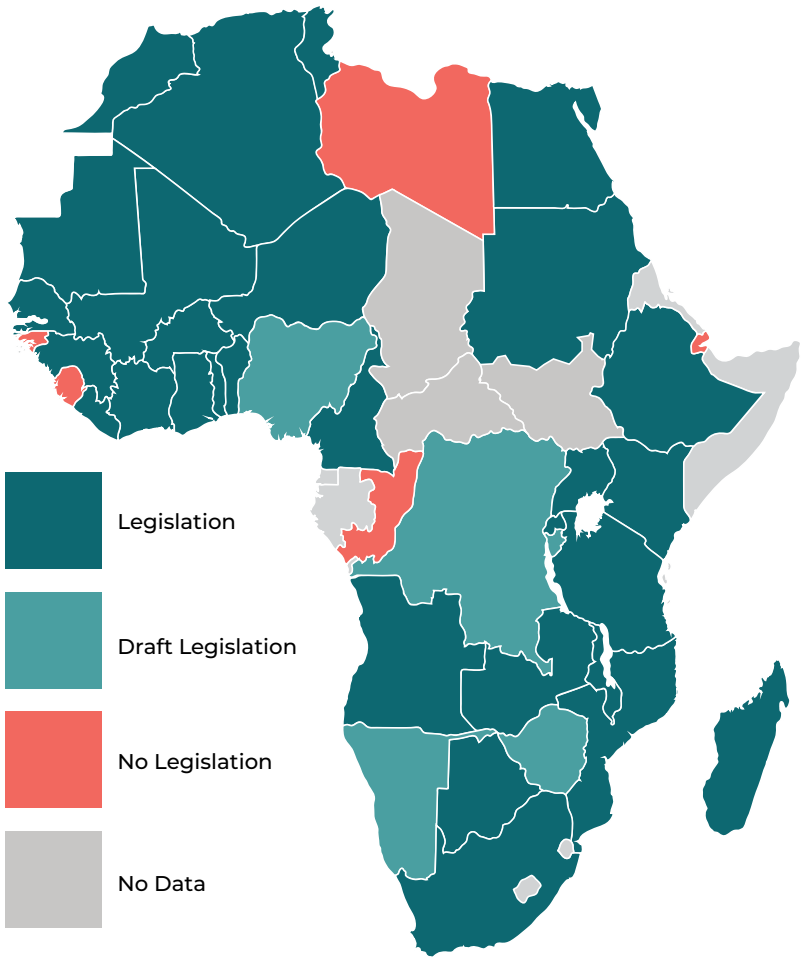
[5] *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*

industrial revolution[6]. Therefore, it is important that African countries take up these legislative provisions around data protection because it is possible that Africa can end up as a testing ground due to an increased uptake of smart phones and increasing digitaization of public services.

There needs to be increased collaboration between academia and the industry so that learning institutions produce career-ready graduates with approriate skills relating to data protection and privacy. Curriculum design and delivery needs to focus on developing graduates with skills in data protection starting from systems analysis, systems design, application development, data engineering, data science and cyber security to drive the next wave of global competitiveness in the fourth industrial revolution.

[6] *https://www.weforum.org/centre-for-the-fourth-industrial-revolution*

FIGURE 28: *Data Protection and Privacy Legislation in Africa (UNCTAD, 2020)*



There needs to be increased collaboration between academia and the industry so that learning institutions produce career-ready graduates with approriate skills relating to data protection and privacy.

05

The Data Protection Law outlines the conditions for the transfer of personal data outside of Botswana and stipulates that a person's data shall not be used for commercial purposes, unless with obtainment of consent from the person whose data is to be used.

5. IMPACT OF DATA PROTECTION LAWS TO VARIOUS DEPARTMENTS

Determining how data protection laws impacts your organisation:

Current state analysis

This is fundamental in order to define and understand the data that an organisation handles and that which is relevant to this context. SMEs should answer the following questions considering all the various phases of the data processing (collection, storage, use, transfer, disposal, etc.) and their subsequent parameters:

01 WHAT IS THE PERSONAL DATA PROCESSING OPERATION?

02 WHAT ARE THE TYPES OF PERSONAL DATA PROCESSED?

03 WHAT IS THE PURPOSE OF THE PROCESSING?

04 WHAT ARE THE MEANS USED FOR THE PROCESSING OF PERSONAL DATA?

05 WHERE DOES THE PROCESSING OF PERSONAL DATA TAKE PLACE?

06 WHAT ARE THE CATEGORIES OF DATA SUBJECTS?

07 WHO ARE THE RECIPIENTS OF THE DATA?

5.1. FINANCE DEPARTMENT

Finance department processes financial records of vendors, employees and other stakeholders. This data includes: bank account, bank balance, payslips, etc.

Payroll Management

PROCESSING OPERATION DESCRIPTION	EMPLOYEES PAYROLL MANAGEMENT	
Personal Data Processed	Contact information (last and first name, address, telephone number,) social security number, taxation Identifier, date of employment, salary information	
Processing Purpose	Payroll management (payment of salaries, benefits and social security contributions)	
Data Subject	Employees	
Processing Means	Human Resources IT System	
Recipients of the Data	External	Financial Institutions
	External	Social Insurance Schemes

PROCESSING OPERATION DESCRIPTION	EMPLOYEES PAYROLL MANAGEMENT
Potential Gaps	There is a specific use policy in place. However, there are no specific policies regarding data retention and destruction. Although the HR officer has signed a confidentiality disclaimer, no security or data protection training has recently been performed for the SME's employees.

IMPACT

Overall impact as a result of unintended disclosure of income (and other relevant data) to third parties is High. This could expose the data subject to consequences ranging from the discomfort arising from the public knowledge of one's own private data to even, in specific cases, the potential risk of targeted attacks from thefts or money seekers.

5.2. HUMAN RESOURCE DEPARTMENT

Recruitment

Staff recruitment is a process run by HR and consists of numerous organisational activities aimed at the selection of people who have specific skills or are capable of performing certain tasks.

PROCESSING OPERATION DESCRIPTION	RECRUITMENT
Personal Data Processed	Academic education and qualifications, working experience, further professional or academic training, family status, first and last name, address, telephone numbers, date of birth, interview notes/report
Processing Purpose	Managing candidate selection for recruitment Assessment of the performance and professional characteristics that arise in the execution of the work
Data Subject	Recruitment Candidates Employees
Processing Means	Recruitment IT platform Human Resources IT System
Recipients of the Data	Internal-Senior Management, Line managers
Potential Gaps	There is a specific use policy in place. However, there are no specific policies regarding data retention and destruction. Although the HR officer has signed a confidentiality disclaimer, no security or data protection training has recently been performed for the SME's employees

IMPACT

Overall impact is Medium: The loss of confidentiality could allow disclosure of data of the candidates, potentially leading to embarrassment, defamation or even limitation of the employee, e.g. when seeking for a new job. However, for HR professionals who process psychological tests or specific behavioral characteristics of the candidates such as personal data related to disabilities, ethnic background the impact can be higher.

5.3. USE CASES: CUSTOMERS MANAGEMENT, MARKETING AND SUPPLIERS

Sales and Marketing teams process personal data of customers and perform marketing activities so as to attract new customers. They may also process personal data in relation to its suppliers. Below are key areas:

5.3.1. Order and delivery of goods

Process involved: Let's consider an online store.

- Step 1: Customers browse through the available goods
- Step 2: Add items to the cart and check out.
- Step 3: In order to complete the order, the customer has to register at the e-shop platform (if not already registered) and provide their contact details (first and last name, delivery address, telephone number and email address). During the checkout process, registered users are also asked to provide payment details in a separate form, which is provided by the payment services provider.

PROCESSING OPERATION DESCRIPTION	**ORDER AND DELIVERY OF GOODS**	
Personal Data Processed	Contact information (last and first name, address, telephone number) payment data (credit card, bank account information)	
Processing Purpose	Order and delivery of goods	
Data Subject	Customers	
Processing Means	Order Management system	
Recipients of the Data	External	Payment service provider
	External	Delivery service provider
	Internal	Customer Relation Management (CRM) system
	Internal	Enterprise Resource Planning (ERP) system
Processing	Following the successful placement of the order and the confirmation from the payment service provider, the details of the order are transmitted to the Enterprise Resource Planning (ERP) system, to the Customer Relation Management (CRM) system and to the delivery services provider.	
Potential gaps	Regarding the use of the system there is a specific use policy in place and best practises are implemented and maintained. However, there are no specific policies regarding data retention and destruction and not all employees involved have received relevant information security training.	

IMPACT

The impact due to loss of confidentiality and integrity is medium as unauthorized disclosure and or alteration of personal data processed, including financial data, could result in significant inconveniences for the data subject (which can be recovered with some effort).

5.3.2. Marketing/advertising

Marketing teams process personal data of potential customers in order to promote the different kinds of goods available within its portfolio. For this processing operation, the Marketing teams makes use of web tools such as CRMs, Mailchimp, Survey Monkey etc. Every now and then, these teams initiate new marketing campaign, which then sends respective personalized emails, to the lastly updated recipients list. For each campaign, marketing teams' get a report with statistics on the percentage of emails read, unread, deleted without however providing information on specific individuals.

PROCESSING OPERATION DESCRIPTION	MARKETING/ADVERTISING	
Personal Data Processed	Contact name, postal address, telephone number, email	
Processing Purpose	Promotion of goods and special offers to possible customers	
Data Subject	Customers and potential customers	
Processing Means	Third party marketing campaign web service	
Recipients of the Data	External	Third party marketing campaign web service provider
	Internal	Marketing Department
	Internal	CRM IT system
Data Processor Used	Third party marketing campaign web service provider	

IMPACT

Loss of confidentiality, integrity and availability as individuals may encounter some minor inconvenience, e.g. by unauthorized disclosure of their contact information (which could lead to spam) or unauthorized modification of their data, excluding them from a potential marketing campaign. In all cases the issue can be easily resolved with some small effort.

5.3.3. Procurement (Suppliers of services and goods)

Procurement departments process personal data, for instance, contact data of specific employees working for the suppliers or contact and financial data of persons that are in direct contract with the SME (i.e. directly acting as suppliers of goods or services).

They make use of Enterprise Resource Planning (ERP) system and the Accounting System. The processed personal data include company name and contact details, financial data (tax number, banking account), employee pictures and access credentials (for staff working on premises).

PROCESSING OPERATION DESCRIPTION	PROCUREMENT (SUPPLY OF RAW MATERIALS, GOODS AND SERVICES)
Personal Data Processed	First and last name, contact Information, tax and banking information (for supplier), picture and access credentials (for staff working on premises).
Processing Purpose	Supply Management

IMPACT

Overall impact is low as individuals may encounter in certain cases minor problems by having their processed personal data being accessed by third parties in an unknown way.

PROCESSING OPERATION DESCRIPTION	PROCUREMENT (SUPPLY OF RAW MATERIALS, GOODS AND SERVICES)	
Data Subject	Employees working for suppliers of goods and services	
Processing Means	IT system	
Recipients of the Data	Internal	Enterprise Resource Planning (ERP) system
	Internal	Accounting system
	External	Suppliers CRM
	External	Payment service provider

IMPACT

Overall impact is low as individuals may encounter in certain cases minor problems by having their processed personal data being accessed by third parties in an unknown way.

5.4. ACCESS CONTROL

Organisations process personal data of employees and visitors for physical access control within its premises, in order to ensure that only the authorized individuals have access into and out of specific areas.

What happens upon departure or expiry of the duration of visit? Are the cards invalidated and returned to the security officer.

PROCESSING OPERATION DESCRIPTION	ACCESS CONTROL	
Personal Data Processed	For Employees: Name, date of employment, position within the organisation, end of employment, a profile picture. For visitors: first and last name, date and time of visit, expected time of departure.	
Processing Purpose	Physical-logical Access Control Security	
Data Subject	Employees, visitors	
Processing Means	Access control management platform	
Recipients of the Data	Internal	Security Officer

IMPACT

Loss of confidentiality, integrity and availability is considered to be LOW as individuals are expected to encounter minor inconveniences which they will be able to overcome with limited effort. For example, employees might not be able to access specific premises of the SME and perform their task (integrity or availability loss) or a visitor's presence in the SME premises might be disclosed (confidentiality loss).

RIGHTS OF THE DATA SUBJECT UNDER THE DATA PROTECTION ACT OF BOTSWANA

The commencement of the Data Protection Act, 2018 ("the Act") confers rights that individuals may exercise in relation to the personal data processed in respect of them. The Act classifies the individuals it seeks to afford data protections as "data subjects".

Senwelo Modise, *FIP, CIPP/E, CIPM, Security+, ICA CertAML*

Partner – Botlhole Law Group [In Association with Neill Armstrong]

A data subject is any individual who can be directly or indirectly identified from the personal data processed by an organisation.

Anyone can be a data subject, depending on the circumstances under which personal data is processed, it may be a prospective or current customer, a client, a web browser, an employee, a representative of a business partner or supplier and/or a member of the Board of Directors. In complying with the Act, organisations have to give effect to the rights of the data subject and for the data subject, to enjoy the protections entrenched in the Act awareness of the rights established by the Act is imperative.

The Act affords individuals the right to be informed; the right to access; the right to object; the right to revocation of consent; and the right to rectification and erasure. The Act also gives the data subject an opportunity to seek recourse from the courts of law. Unlike the General Data Protection Regulation ("GDPR") the Act does not afford the right to restriction of processing and the right to data portability.

Furthermore, it does not set the time constraints within which a response to a data subject access request should be done and permits the imposition of a reasonable fee for a data subject access request at first instance. Lastly, the right to objection appears to be only exercisable in relation to direct marketing.

THE RIGHT TO BE INFORMED

The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. A data controller has information obligations whether the personal data being processed is collected directly or indirectly from the data subject.

In terms of Section 28 of the Act where personal data is obtained directly from the data subject, the data controller or processor should at the time of collection provide with information about the identity and habitual residence or principal place of business of the data controller or data processor; the purpose of the processing for which the personal data is intended; the existence of the right to object to the intended processing,

if the processing of the personal data is obtained for the purposes of direct marketing. Depending on the circumstances the data controller or data processor may also have to prove information about the recipient or category of recipients of the data; the existence of the right to access, rectify, and where applicable, the right to delete the data concerning him or her; or any other information necessary for the specific nature of the processing, to guarantee fair processing in respect of the recording of personal data or if a disclosure to a third party is foreseen, not later than the time when the personal data is first disclosed. A data controller or data processor is only exempt from the obligation to inform when data is collected from third parties if any other law provides for the registration or disclosure of any such personal data, and appropriate security safeguards are adopted; if the personal data is required for processing for statistical purposes, purposes of historical or scientific research, or purposes of medical examination of the population, with a view to protect and promote public health. A data controller or data processor will also be exempt from its information obligations regarding personal data collected from third parties if the provision of such information will be impossible or would involve a disproportionate effort. It may involve disproportionate effort for example to inform data subjects about personal data collected from third parties and processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Organisations should take heed of their information obligations. In terms of the Act, failure to inform a data subject of the rights conferred on the data subject is an offence and attract liability to a fine not exceeding BWP100 000 or to imprisonment for a term not exceeding three years, or to both.

THE RIGHT TO ACCESS

It is fundamental in data protection to grant data subjects the right of access to personal data which have been collected concerning him or her and to enable them to exercise that right easily and at reasonable intervals, in order for them to be aware of, and verify, the lawfulness of the processing. Within the right to access the Act at Section 30(1)(a) empowers the data subject with the right to obtain from a data controller or data processor, confirmation of whether or not the data controller or data processor has personal data relating to him or her. If the data controller or processor does process personal data relation to the data subject, Section 30(1)(b) empowers the data subject to request access to the details of personal data relating to him or her within a reasonable time from the time of request. Should the request for access be refused, the data subject has to be given reasons for the refusal and may also submit a complaint with the Information and Data Protection Commission challenging the refusal.

The right to obtain confirmation of processing and request for access shall not apply when the personal data is processed solely for the purpose of scientific research or is kept in a personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics. However, this above described exemption will not be applicable where the personal data is used for taking a measure or decision regarding any particular individual or where there is a risk of breaching the privacy of the data subject.

Modalities should be provided for facilitating the exercise of the data

subject's right to access including mechanisms to request and if applicable, obtain access to their personal data. Where possible organisations should provide means for requests to be made electronically, especially where personal data are processed by electronic means. Failure to respect the data subject's right to access is an offence that falls within processing personal data in contravention with the Act. The offence attracts a liability of up to BWP500 000.00 or to imprisonment for a term not exceeding nine years, or to both.

THE RIGHT TO OBJECT

The right to object is the ability of a data subject to stop or prevent an organisation from processing his or her personal data. Under the GDPR a data subject may object to processing for any activity including direct marketing. Under the Act the right to objection is only afforded to data subjects in relation to personal data processed for direct marketing. Under the information obligations of data controllers and data processors, the data subject has to be informed about the existence of the right to object to the intended processing, if the processing of the personal data is obtained for the purposes of direct marketing. In terms of Section 18 provides that where personal data is processed for purposes of direct marketing, the data controller shall, at no cost, inform the data subject of his or her right to oppose the processing. Where the data subject gives a notice of objection to the processing of his or her personal data for direct marketing, the personal data of the data subject shall not be processed for such purpose. A data controller who processes data despite the objection of the data subject commits an offence and is liable to a fine not exceeding BWP500 000 or to imprisonment for a term not exceeding nine years, or to both.

THE RIGHT TO RECTIFICATION AND ERASURE

In terms of Section 30(1)(e) a data subject has a right to challenge personal data relating to him or her by submitting a complaint to the Information and Data Protection Commission. If the challenge is successful the data subject may have the personal data deleted, rectified, completed or amended, whichever is required in the outcome of the investigation of the complaint lodged. Even though these rights may be exercised through engagement of the Information and Data Protection Commission organisations are not barred from granting easy access to the right to rectification and erasure. Unlike the GDPR the Act does not specify the circumstances under which the data subject will be entitled to right to erasure (also known as the right to be forgotten under the GDPR).

REVOCATION OF CONSENT

Although not specified as a right under the Act, the Act makes provision for the withdrawal of consent. At Section 19 it provides that where the processing of personal data takes place with the consent of the data subject, the data subject may at any time revoke his or her consent for legitimate grounds compelling him or her at that particular time. The grounds for revocation have to be legitimate, reasonable and compelling. In the same way the Act requires that consent be in writing, the revocation of consent by the data subject has to be in writing.

RECOURSE TO THE COURTS OF LAW

The data subject does not always have to reach out to the Information and Data Protection Commission to assert their rights. The Act also gives the data subject an opportunity to get compensation for damages for violation of their data protection rights. A data subject may institute an action for damages against a data controller who processes data in contravention of the Act. The n action instituted in terms of the Act shall be commenced within a period of 12 months from the date when the data subject became aware or could have become aware of such contravention, whichever is earlier.

5.5. HEALTH SECTOR

5.5.1. Health Services Provision

A hospital processes personal data in order to provide healthcare services as follows:

- An electronic record is created (or updated) and includes patients' contact details, social insurance number, medical exams' results, pathologies, allergies, diagnosis and cure schemas (medical information).
- Insurance details area also validated against the hospital/insurance records.

Definition of the processing operation and its context.

PROCESSING OPERATION DESCRIPTION	HEALTH SERVICES PROVISION
Personal Data Processed	Contact Information (last and first name, address, telephone number), social insurance number, medical examination results, pathologies, allergies, diagnosis and cure schemas (medical information), administrative and financial information (invoices, hospitalization papers).
Processing Purpose	Provision of healthcare services (diagnosis, treatment an hospitalization)
Data Subject	Patients
Processing Means	Medical IT system
Recipients of the Data	Internal Treating doctors and nurses
Internal	Administration and accounting IT system
External	Public Health System
Potential gap	Access rights to the patients' medical records are not explicitly defined at a granular level, as nurses and doctors need to be able to access the files at any time and the system does not support relevant granularity.

IMPACT

Overall Impact is considered to be HIGH as individuals are expected to encounter major adverse effects through unauthorized access to their health related data. Equally important (HIGH) may be the loss of integrity, as wrong medical information might even put an individual's life at risk. The same (HIGH) could be argued also for the loss of availability, as even a temporal unavailability of the clinic's IT system might hinder its operations, thus putting patients at serious risk.

5.6. EDUCATION SECTOR

5.6.1. Early childhood/High schools/Universities

Modern schools, particularly early childhood schools use web platforms to support communication of day to day physical, intellectual, language, emotional and social activities of minors between the school and the parents. A university on the other hand utilizes e-learning and course management platforms where professors and administration can send announcements to students and students can retrieve their course materials, lecture notes and slides, submit assignments, undertake assessments and tests and get evaluation results and grades.

PROCESSING OPERATION DESCRIPTION	EARLY CHILDHOOD SCHOOL COMMUNICATION PLATFORM	
Personal Data Processed	First and last name, date of birth, home address, daily information on the child's performance (including eating, activities, etc.), health data, allergies, nutrition intolerances, parent(s) first and last name, parent(s) telephone number, emergency contact number Students: first and last name, date of birth, date of admission, selected course(s), evaluation results, grades Academic Staff: first and last name, date of birth, course(s) assigned	
Processing Purpose	Provision of educational services (communication of day to day activities and child's development) e-Learning and course management platform, including undertaking of assignments and test	
Data Subject	Children, parents, students, professors	
Processing Means	Web based, e-Learning and course management platform	
Recipients of the Data	External	Parents, Administration
	Internal	Secretariat, Educators, HoD

IMPACT

Overall impact is considered as MEDIUM, as in certain cases individuals may encounter significant inconvenience from the disclosure of certain data (e.g. regarding the child's behavior, communication, eating patterns, grades).

5.7. REVIEW OF GDPR

Major GDPR fine total in Euros (approximate due to currency conversion):

TABLE 10: *Breakdown of GDPR fines across the world.*

Year	Country	Organisation	Fine	Details - Reason for Fine
November, 2019	Netherlands	Uber	€600,000	A 2016 data breach concerning 57 million Uber users, of which 174,000 were Dutch citizens, was not reported within 72 hours.
November, 2019	Romania	Raiffeisen Bank	€150,000	Bank employees sent personal information, without requesting permission from the affected individuals, to Vreau Credit (which was also fined €20,000), and did not evaluate the risks of taking these actions.
July, 2019	United Kingdom	Marriott	£99,000,000	After acquiring its competitor Starwood, Marriott discovered Starwood's central reservation database had been hacked. This included 5 million unencrypted passwords and 8 million credit card records. The hack was ongoing from 2014 to 2018. The breach impacted 30 million EU residents
June, 2019	Netherlands	Haga Hospital	€460,000	A Dutch hospital was fined over lax controls over logging and access to patient records. In one instance, 197 employees accessed one Dutch celebrity's medical records.
June, 2019	United Kingdom	British Airways	£183,000,000	As a result of an attack on British Airways' website, about 500,000 customer records were extracted by a malicious third party. The UK's data protection agency claims BA's website was compromised due to poor cybersecurity arrangements. This would represent the largest GDPR fine to date.
June 2019	Spain	La Liga, the soccer league	€250,000	La Liga is accused of listening for piracy through its smartphone application. La Liga turned on user microphones in order to listen for sounds of the soccer game and match to any pirated stream using geolocaton. La Liga used the information to sue 600 bars for pirating soccer games

TRANSITIONING TO MODERN MANAGEMENT

Flying into the cloud without falling:
Cloud computing is a growing trend in public and private sector, what advice would you give to organisations that are transitioning into the cloud?

Tshepho Tsheko
Acting CEO - Botswana Innovation Hub

There are pros and cons associated with the use of cloud computing services but before an organisation could transition to cloud computing it is ideal to consider the following practical needs:

- Strategic Business-IT Alignment
- Cloud architectures (Public, Private and Hybrid)
- Types of cloud computing models (Iaas, Paas, Saas)
- Pricing (Cost Benefits Analysis)
- Client Support
- Cloud computing services scalability
- Organisational security and privacy needs
- Cloud computing services availability and reliability to support critical business processes and systems

A business decision to migrate to cloud computing services is a strategic one that has to be well thought of and calculated. It has to create value for the shareholders and stakeholders. First the move has to be aligned to both the business and IT strategy. Alignment can be attained by asking the following questions

- How is IT aligned with the business?
- How is the business aligned with IT?

The strategic business-IT alignment will inform the type of cloud computing service suitable for the organisation.

The organisational objectives of benefit realization, risk optimization, and resource optimization which are strategic by nature include and can inform such IT decisions as to whether there is a need to transition to cloud computing or not.

Financially the decision to transition to cloud computing must make business sense.

DETAILED UNDERSTANDING OF THE BENEFITS AND CONSIDERATION OF USING CLOUD SERVICES

PRICING

The monetary savings that comes with using the cloud services is very significant, some expenses can be reduced or eliminated. Cloud services depends on what the subscriber's needs to be charged at a particular time.

Budget - The organisation should be willing to set aside a budget for investment in cloud and continued support. However, as cloud services are provided on a pay-as-you-go pricing this brings along an element of cost savings. The ability of cloud services to scale up and down depending on the demand is an important cost saving measure which helps the business attain its IT resource optimisation. Costs are also reduced by economies of scale.

The business also saves on ownership and maintenance of IT infrastructure as this becomes the responsibility of a cloud computing service provider. IT capital investment is reduced.

CLIENT SUPPORT

Cloud computing comes with several support options available to customers 24/7 through various customer support channels. The support provided by the service provider allow for the organisation to focus on its core business and not worry about IT services availability and reliability.

CLOUD COMPUTING AVAILABILITY AND RELIABILITY

Cloud services are characterised by high degree of availability reducing the risk of failure by the business to service its customers. Access the business-critical mission systems as well as the need for backing up the same systems. Data backup, disaster recovery servers and fault tolerance are expensive services in an on-premises infrastructure environment as they require additional hardware, deployment time and administration and if an organisation has transitioned to the cloud, they are guaranteed that data is secured and made redundant in decoupled data centres, there is automatic fail over to back up server to minimize downtime in any event of outage or hardware failure.

CLOUD MANAGEABILITY

Cloud computing provides enhanced and simplified IT management and maintenance capabilities through central administration of resources, vendor managed infrastructure and SLA backed agreements. IT infrastructure updates and maintenance are eliminated, as all resources are maintained by the service provider. Cloud vendors have made it easier for subscribers by provisioning free tools (web based remote interfaces) that allows them to have access on how their resources are consumed and utilized and offering suggestions on improving efficiencies. These tools make it possible to manage configuration settings.

DEPLOYMENT

Cloud computing allows organisations to access industry shaping technology quickly. It allows organisations to easily deploy applications in multiple regions around the world with just a few clicks, providing a lower latency and a better experience at minimal cost. A cloud service is always simple to deploy than on an on-premises server-based product because the service is provided to the subscriber in an installed and operational state. An admin can begin to work with the service immediately after subscribing to it. There is no need to obtain hardware, design infrastructure and install server software.

UPDATES

Cloud applications are regularly and automatically updated with the latest version of software. With a cloud-based solution, an organisation is subscribing to a service not a software product, so the provider is responsible for maintaining and updating the service functionality. In most cases the cloud-based version receives new features soon and as for on- premises service installation, a responsible update strategy requires testing and evaluation of new software releases and might require downtime.

SECURITY AND COMPLIANCE

Cloud vendors follow security standards, align to infrastructure regulations and industry best practices however its upon an organisation to evaluate and assess their readiness to offering their data for housing by a third-party provider as well as selecting the appropriate or suitable provider to meet their operational needs. Audit is a best practice that is constantly completed by cloud solution providers to ensure that compliance is attained.

When leveraging cloud services, subscribers are guaranteed that antivirus protection, message encryption, information rights management and data loss prevention are just some of the security mechanisms that are provisioned which will require additional maintenance and expense to implement for an on-premises server.

DISADVANTAGES OF MIGRATING TO THE CLOUD

DATA SENSITIVITY

All organisations, irrespective of their size run their cloud operations at the cost of data that they store in the cloud and the clients they share this data with. This data can only be shared if it has been migrated to the cloud in its entirety, and it is quite possible that some data might eventually leak out or get lost. Therefore, the process of cloud migration is a time-intensive task which requires careful planning and data evaluation, failing which you might find your precious data lost, and in some cases, irrecoverable.

CLOUD SECURITY

In today's interconnected world, cloud security is not only essential, but downright necessary for your company to remain functional. Special care needs to be taken when data is migrated from your existing systems to the cloud, and all variables related to data security needs to be checked off. Data is still vulnerable to confidentiality risk in the cloud as there is always a possibility that it can be accessed by third parties not authorized to do so. When organisations choose to house their data in their regions of preference considering bandwidths and network latency, its uncertain on how the data is handled by the cloud service provider as mostly they adopt a fault tolerance mechanism of allowing automatic failover to other data center regions in which data becomes redundant across regions which may be vulnerable in any event of attack.

APPLICATION INTEROPERABILITY

One of the biggest challenges facing cloud computing and its overall acceptance are interoperability issues. This is because each individual vendor approaches cloud computing in their own way, therefore making it tough for individual applications to communicate with each other. In an ideal world of cloud computing, a single line of code should work across applications developed by different vendors, which, sadly is not the case right now. Therefore, if your business is thinking of cloud migration in the future, do investigate interoperability and how your applications function together.

06

Proper economic quantification of an organisation's cyber exposure is essential to help board members and other decision makers understand their cyber value at risk, determine optimal investment strategies, and achieve measurable outcomes within their cyber-risk management program.

6. RISK QUANTIFICATION, CYBER INSURANCE AND COST OF CYBERCRIME

Cyber insurance - is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products.

Companies offering cyber insurance in Africa.

Britam
With you every step of the way

DAWIT INSURANCE AGENCY LIMITED
Your Insurance Department

AIG

Minet

Most organisations understand that a cyber-attack would have serious and lasting consequences for the bottom line. But why is Cyber Insurance uptake still so low?

- Companies often underestimate the likelihood of an attack, the damage that results, and the complexity of an effective cybersecurity solution.
- Limited knowledge on Cyber insurance offering: What is covered, how much it costs and how this translates into business value.

FACT

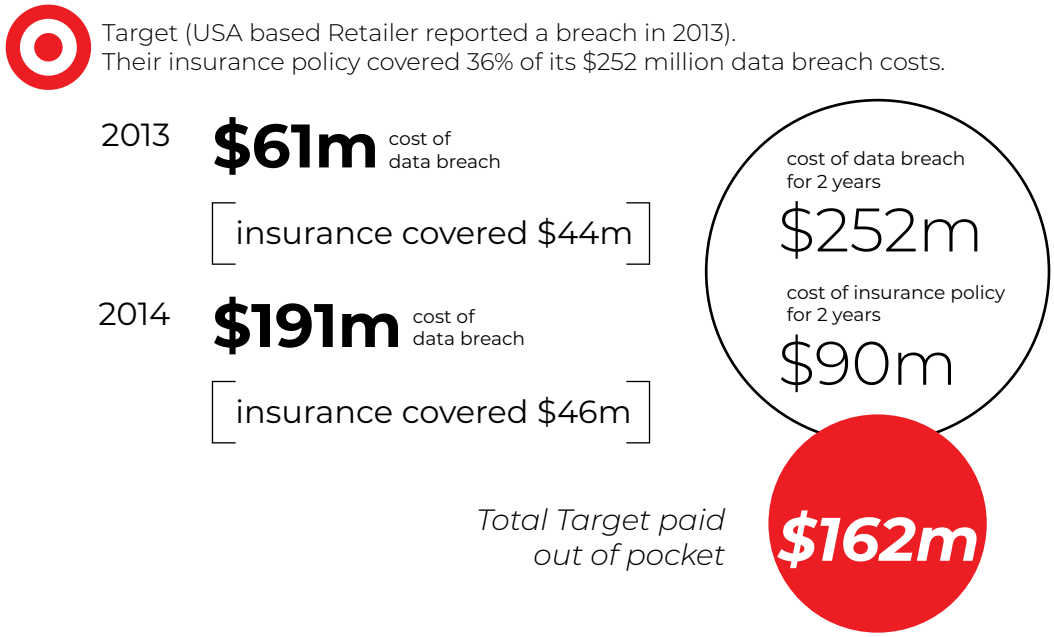
Cybercrime damages will cost the world **$6 Trillion** annually by 2021

6.1. WHAT WILL IT COST YOUR ORGANISATION NOT TO HAVE CYBER INSURANCE?

Case study:

Target's case (USA based Retailer that reported a breach in 2013) provides an example of just how devastating a cyber breach can be to a business:

FIGURE 25. *Target's case study.*

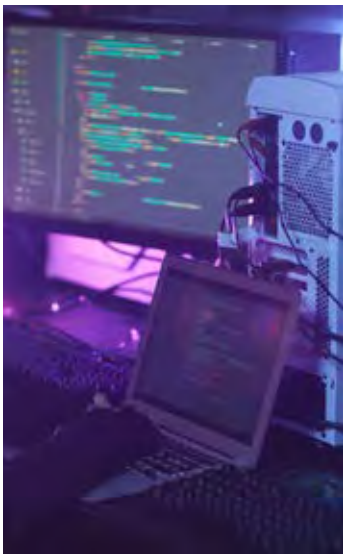


Detailed breakdown of Risk Quantification, Cyber Insurance and Cost of Cybercrime will be provided in the Cost of Cybercrime - Africa Report.


Applications
01 - Info Gathering
02 - Vulnerability
03 - Web App Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering
14 - System Services
Usual Applications
Activities Overview
cewl
crunch
hashcat
john
johnny
medusa
ncrack
ophcrack
pyrit
wordlists
HACK TOOL V2.264
Enter the code

AFRICA CYBER IMMERSION CENTRE (ACIC)

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.



Brilliant Kaimba

Training Assistant, Africa Cyber Immersion Centre

Structuring a single university program around cybersecurity 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.

HIGHLIGHTS OF THE CYBER IMMERSION PROGRAM

My main highlight was the launching of the high school cyber immersion boot camp at Nova Pioneer Girls. Over 100 students from different high schools took part in the competition. During the session, one of the challenges consisted of kahoot, a game-based learning platform that brings engagement and fun, group presentations where the students had to present their research to all other students at the boot camp and finally Cyber ranges, a learning virtual environment for cybersecurity trainings where students can learn and practice basic and advanced hacking skills.

The Nova Pioneer Girls launch was a great learning experience characterized by sharing knowledge, teamwork, building skills and meeting students who had interest in cybersecurity.

Additionally, we got to train over 500 university and high school students and over 100 teachers across the country. Our first and second training sessions for teachers were held at Alliance High School and Shanzu Teachers Training College respectively. Our aim was to empower teachers with skills that will help them manage and run cyber immersion clubs and innovation hubs within their schools. Teachers play an important role in high school and as such, they need to be empowered in order to fully manage the young talents within their various institutions.

INTERESTING PROJECTS FROM THE STUDENTS

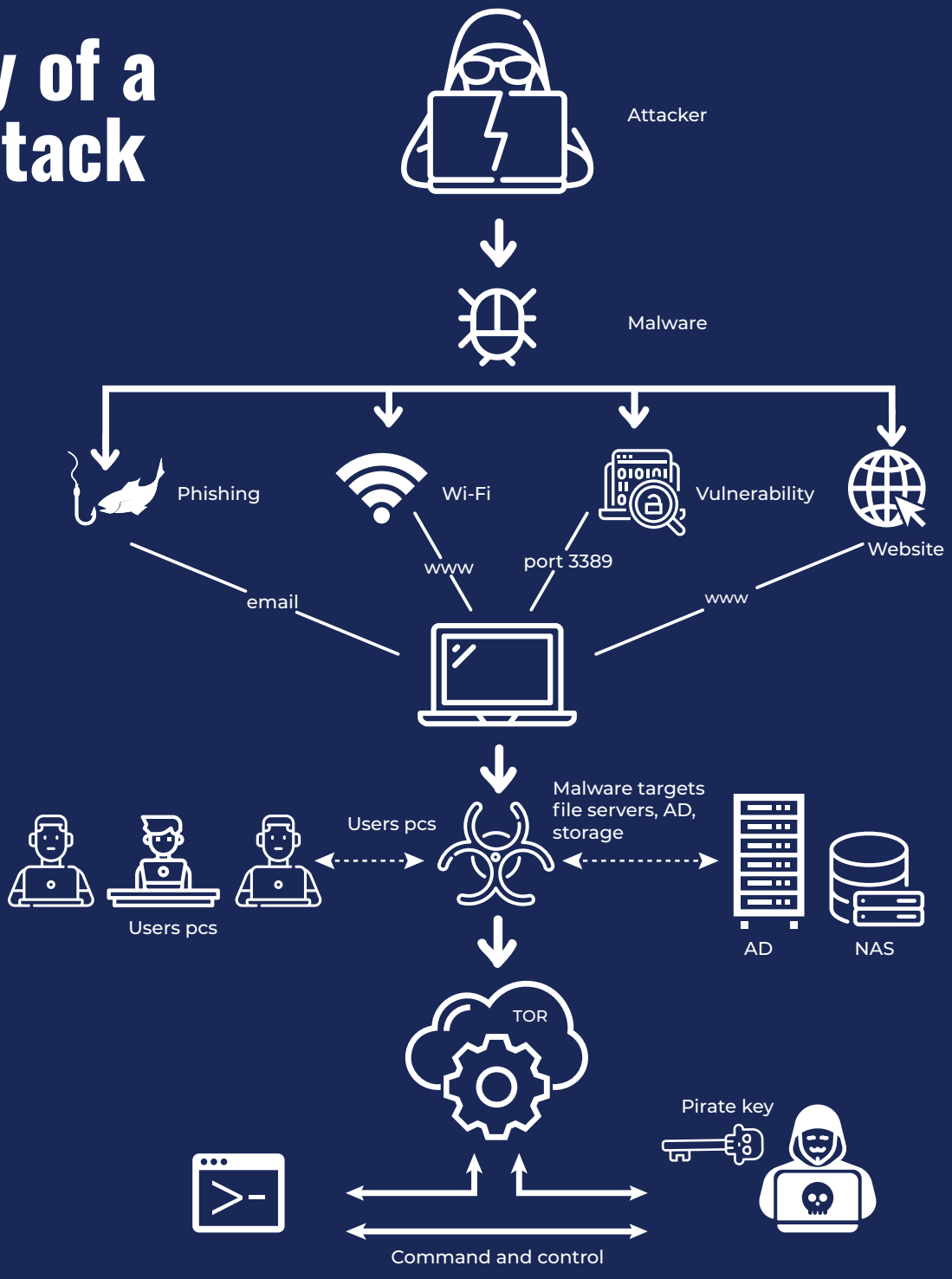
Students from Alliance High School, Kenya worked on a threat map project. A Threat Map is a visual representation of the source and destination locations around the world for malicious traffic and the exploit used during the interaction. The project lasted 5 weeks.

Students from United States International University (USIU), Multimedia University and Taita Taveta University got to participate in the Annual cybersecurity report through research. These research included local trends, insights and developments in cybersecurity industries, including fake news, spam, viruses, insider threats, phishing, botnets, malware, project honeypot and other potential harmful business risks.

ACIC is looking forward to increasing the number of training sessions per term and also our geographical reach.

Reach out to more students and teachers across the country and equip them with the general overview of Cybersecurity Landscape. Outreach is a fundamental component of cybersecurity education program within Serianu.

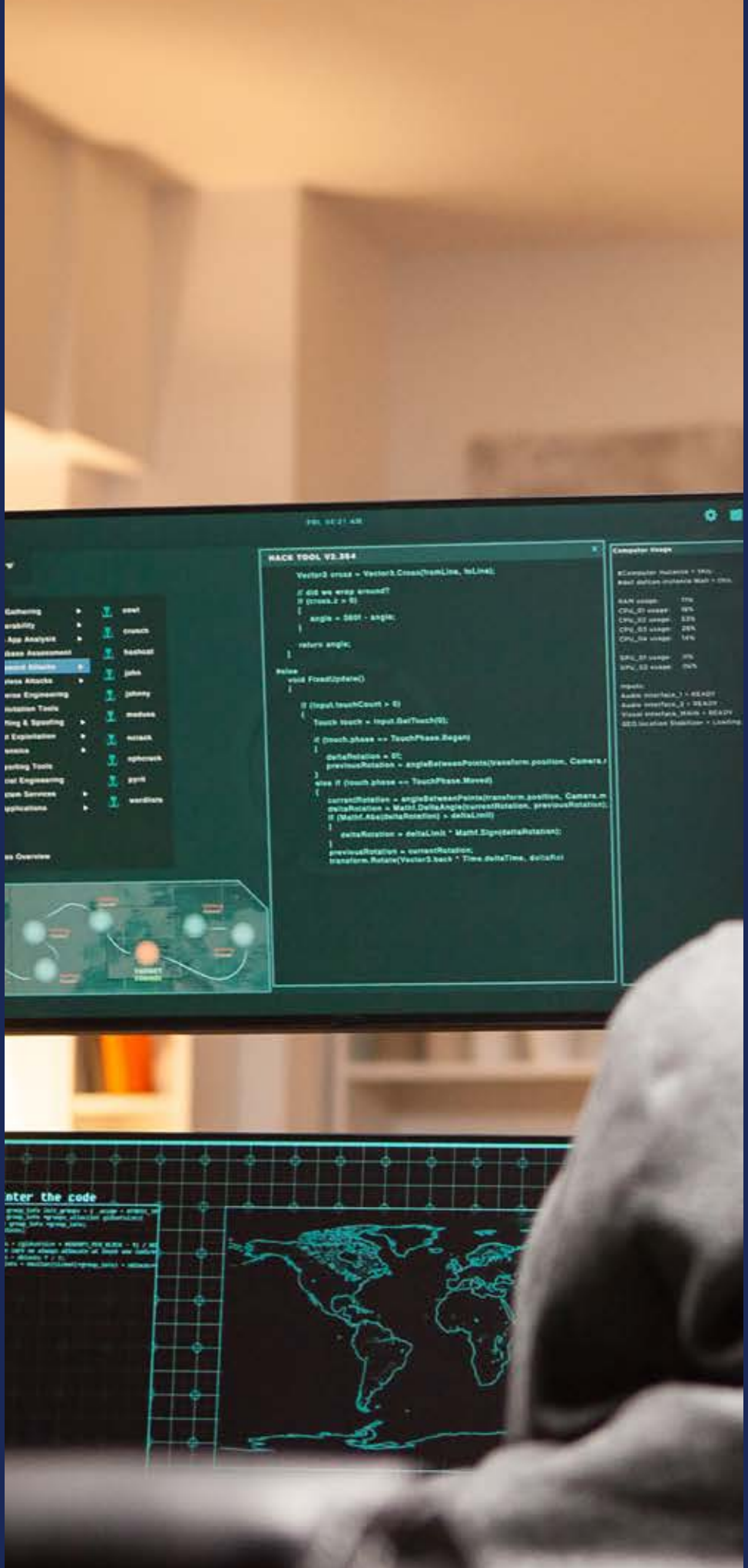
Anatomy of a cyber attack



Initial

Gaining access

Maintaining & encryption



07

Key issues that drove the industry last year and point at the ones that we believe should be top of mind.

7. 2022 PRIORITIES

In order to set the mood for this year, we take a moment to reflect on the key issues that drove the industry last year and point at the ones that we believe should be top of mind and action for all information security executives this side of the calendar.

2020/2022 was an eventful year in the cybersecurity world. A lot happened to keep cybersecurity professionals busy, including the emergence of locally developed malware, greater public awareness and rising organisational interest.

We noted an increase in attacks across all key sectors from financial services, government, manufacturing and insurance.

These attacks were perpetrated through the following vectors:


Remote access


Privilege access abuse


Phishing


Fraudulent transactions


Malware


Deployment of rogue devices


Social engineering

As we prepare for 2022 it is important to reflect and adequately prepare for the next 12 months. We anticipate an increase in targeted attacks.

Here are the priority areas for the different industries;

1 

Financial Sector:
Banking, MFI'S and Saccos

- ATM Infrastructure (Fraud)
- Mobile banking infrastructure (Fraud)
- Debit and credit card systems (Fraud)
- Third parties and vendors (Fraud)
- Identity management systems e.g. Active Directory (Sabotage - ransomware)

2 

Others:
Manufacturing/Insurance/ Healthcare/Government

- Payment systems (Fraud)
- Storage/Document management systems (Sabotage - ransomware)
- Identity management systems e.g. Active Directory (Sabotage - ransomware)
- SCADA systems (Sabotage)
- Email System (Phishing)

Top 5 Questions That Should Guide Your **Cyber Risk Program** in 2022

Risk and Compliance Teams

1. What are our top sources of cyber risk? (Connections, Applications, Employees, Third parties, Channels, and compliance)
2. What are our top cyber risk exposures? (Fraud, IP theft, Sabotage)
3. How mature are our cyber risk management practices? (Mature, immature or non-existent)
4. What is our current cyber risk profile? (Risk appetite, Risk tolerance level and Annualized Loss Expectancy)
5. What remedial actions should we take to manage our risk exposure? (Mitigate, transfer, avoid or accept)

ICT and Technology Teams

1. Has the organisation implemented asset management controls? (Malware, configuration changes, vulnerability controls, inventory and data protection controls)
2. Has the organisation implemented user management controls? (Privileged access, user/identity access management, user awareness and training)
3. Has the organisation implemented continuity management controls? (Disaster recovery, performance and availability monitoring)
4. Has the organisation implemented incident management controls? (Transaction monitoring, incident response, Monitoring and analysis)
5. Has the organisation established metrics to continuously measure the organisation's cybersecurity posture?

Audit and Assurance Teams

1. What are our top cyber risk control deficiencies? (Materiality, significance, operational and design?
2. How effective/efficient are our existing asset management controls? (Malware, configuration changes, vulnerability controls, inventory and data protection controls)
3. How effective/efficient are our existing user management controls? (Privileged access, user/identity access management, user awareness and training)
4. How effective/efficient are our existing continuity management controls? (Disaster recovery, performance and availability monitoring)
5. How effective/efficient are our incident management controls? (Transaction monitoring, incident response, Monitoring and analysis)

Top Cyber Risk Audit Focus Areas for 2022

Financial Sector:

Banking, MFI'S and Saccos

1. ATM Penetration tests and assessments
2. Middleware (ESB, API and Web services) Penetration Tests and assessments
3. Mobile and internet banking assessment
4. Card Management and SWIFT infrastructure review
5. Third party and remote access infrastructure
6. Data protection and privacy

Others:

Manufacturing/Insurance/ Healthcare/Government)

1. ERP, transactional and payment systems
2. Identity and access management systems
3. Storage and document management systems
4. Third party and remote access infrastructure
5. Data protection and privacy practices

OTHER CONSIDERATIONS

Regulatory Awareness and Compliance

In 2019, governments across Africa introduced Data Privacy laws and industry guidelines targeting financial services sector. Affected organisations need to conduct impact assessments to;

- Ensure conformance with applicable legal, regulatory, and policy requirements for new regulations;
- Identify and evaluate the risks of breaches or other incidents and effects; and
- Identify appropriate controls to mitigate unacceptable risks.

Training

Adequately skilled personnel remains a major issue for all organisations and is a major determinant of the level of preparedness for prevention and restitution.

These may not cover each and every enterprise or organisational situation and environment but they are foundational to the very heart of information security and preliminary cyber risk management across the full spectrum of your operations.

Technologies
to budget for in 2022

Application and Data Security

1. Web Application Firewall (WAF)
2. Transaction and Database Activity monitoring (DAM)
3. File Integrity/Activity Monitoring (FIM, FAM)
4. API gateway protection (Middleware, ESB, Web services)
5. Backup and replication capabilities

Security Management and Operations

1. Patch Management
2. Security configuration management
3. Vulnerability management (Application testing, Penetration testing and attack simulation)
4. Network Monitoring, User and Entity Behavior Analytics
5. Threat Intelligence (Local and global)

Identity and Access Management

1. User/account provisioning and de-provisioning
2. Privileged Access Management (PAM)
3. Multi-factor authentication and Tokens (hardware and software)
4. Network Access Control (Hardware authentication)
5. Biometrics

Network Security

1. Next Generation Firewall (NGFW)
2. Intrusion Detection/Prevention System (IDS/IPS)
3. Advanced malware analysis/sandboxing
4. Network Access Control (NAC)
5. Secure email gateway

Endpoint Security

1. Basic anti-virus/anti-malware (threat signatures)
2. Disk encryption
3. Advanced anti-virus /antimalware (machine learning, behavior monitoring, sandboxing)
4. Application control (whitelist/blacklist)
5. Data loss/leak prevention (DLP)

8. REFERENCES

Bocra.org.bw. (2020). Data protection act. [Online] Available at: https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf [Accessed 8 Feb. 2020].

BiztechAfrica. (2019). Innovation Fund winners unveiled. [online] Available at: https://www.biztechafrica.com/article/innovation-fund-winners-unveiled/15125/ [Accessed 8 Feb. 2020].

Ashurst.com. (2019). The GDPR: A year in review. [online] Available at: https://www.ashurst.com/en/news-and-insights/legal-updates/the-gdpr---a-year-in-review/ [Accessed 8 Feb. 2020].

IPv4 Hosts. (2020). Retrieved 16 February 2020, from https://censys.io/ipv4?q=.bw

Klammer, S. (2020). The GDPR: A year in review | Technology Law Source. [online] Technology Law Source. Available at: http://technologylawsource.com/2019/07/articles/privacy-1/the-gdpr-a-year-in-review/ [Accessed 8 Feb. 2020].

Top 10 Malware January 2019. (2019). Retrieved 8 February 2020, from https://www.cisecurity.org/blog/top-10-malware-january-2019/

"November 2019's Most Wanted Malware: Researchers Warn ...." https://blog.checkpoint.com/2019/12/11/november-2019s-most-wanted-malware-researchers-warn-of-fast-growing-mobile-threat-while-emotets-impact-declines/. Accessed 18 Feb. 2020.

"Data Protection Act - bocra." 3 Aug. 2018, https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf. Accessed 18 Feb. 2020

"National Cybersecurity Strategy - ITU." https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00042_02_botswana-national-cybersecurity-strategy.pdf. Accessed 18 Feb. 2020.

"Law in Botswana - DLA Piper Data Protection." https://www.dlapiperdataprotection.com/index.html?t=law&c=BW. Accessed 18 Feb. 2020.

"Cyber security stakeholders introspect - Botswana Guardian." 29 Jan. 2019, http://www.botswanaguardian.co.bw/news/item/3945-cyber-security-stakeholders-introspect.html. Accessed 18 Feb. 2020.

"Innovation Botswana 2018 - The Patriot on Sunday." 7 Nov. 2018, http://www.thepatriot.co.bw/business/item/6341-innovation-botswana-2018.html. Accessed 18 Feb. 2020.

"Botswana: Poised for cloud growth - IT News Africa - Up to ...." 10 May. 2018, https://www.itnewsafrica.com/2018/05/botswana-poised-for-cloud-growth/. Accessed 18 Feb. 2020.

"DIS hacked - Botswana Guardian." 18 Sep. 2018, http://www.botswanaguardian.co.bw/news/item/3432-dis-hacked.html. Accessed 18 Feb. 2020.

"November 2019's Most Wanted Malware: Researchers Warn ...." https://blog.checkpoint.com/2019/12/11/november-2019s-most-wanted-malware-researchers-warn-of-fast-growing-mobile-threat-while-emotets-impact-declines/. Accessed 18 Feb. 2020.

"Botswana: Poised for cloud growth - IT News Africa - Up to ...." 10 May. 2018, https://www.itnewsafrica.com/2018/05/botswana-poised-for-cloud-growth/. Accessed 18 Feb. 2020.

"Health Hub - Ministry Of Health & Wellness, Botswana." https://www.moh.gov.bw/health_hub.html. Accessed 18 Feb. 2020.

"New interactive technology for real time surveillance quality ...." https://www.afro.who.int/news/new-interactive-technology-real-time-surveillance-quality-improvement-adopted-botswana. Accessed 18 Feb. 2020.

"Botswana: Software to Help Farmers - allAfrica.com." 2 Jul. 2018, https://allafrica.com/stories/201807030085.html. Accessed 18 Feb. 2020.

"Artificial Intelligence | DHL | Botswana - logistics.dhl." https://www.logistics.dhl/bw-en/home/insights-and-innovation/insights/artificial-intelligence.html. Accessed 18 Feb. 2020.

"Mining companies embrace Sandvik's high-tech solutions." 5 Feb. 2020, http://www.miningweekly.com/article/mining-companies-embrace-sandviks-high-tech-solutions-2020-02-05. Accessed 18 Feb. 2020.

"BOTSWANA: DOWNSTREAM LINKAGES - IISD." https://www.iisd.org/sites/default/files/publications/case-study-botswana-downstream-linkages.pdf. Accessed 18 Feb. 2020.

Privacy is not something that we are merely entitled to, it's an absolute prerequisite.

ADDRESS

Serianu Limited
14 Chalbi Drive, Lavington
P. O. Box 56966 - 00200
Nairobi, Kenya

Local Office:
The Hub, iTowers
Gaborone, Botswana

TELEPHONE

General Information:
+254 (0) 20 200 6600

Cyber Crime Hotline:
+254 (0) 800 22 1377

+267 398 1900

EMAIL

info@serianu.com

WEBSITE

https://www.serianu.com