SERIANU

Africa Cybersecurity Report

Uganda, 2019/2020

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

Insights from African SMEs

2019/2020

United States International University-Africa

ISACA Kampala Chapter

Milima Security

Africa Cyber Immersion Centre acic

SERIANU

Africa Cybersecurity Report

Uganda, 2019/2020

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

EDITOR'S NOTE

Brencil Kaimba
Editor-in-chief and Cybersecurity Consultant, Serianu Limited

Welcome to the Uganda Edition of Africa Cybersecurity Report, 2019/2020. In this edition, we highlight the significant investigative research and trends in threats statistics and observations in the evolving threat landscape gathered by the Africa Cyber Immersion Centre Researchers, Milima Security and Cyber Intelligence teams in Q1 of 2019 through to Q4 of 2020.

The dominant theme of **2019** was **Data Protection and Privacy** while that of **2020** has been **Business Continuity in the face of Covid-19.**

Key themes identified in 2019/2020 are illustrated below:

Q1: 2019

Ransomware attacks grew by 118% globally.

We identified over 20 variants of ATM malwares. Another key discovery during this period was that for a substantial price, anyone with cash to spare could visit Dark Web forums and purchase ATM malware complete with easy how-to instructions.

Q2: 2019

Data Protection.

Uganda's first data protection law came into force. The president approved the data protection law that sets out restrictions on how personally identifiable data can be handled, stored and shared.

Q3: 2019

Regionally coordinated attacks in East Africa on the rise.

Replication of attacks across the Eastern Africa region was seen to be a key trend in Q3, particularly in the attack execution, tools utilized and targeted systems.

Q4: 2019

Uganda Police released Annual report on Cybercrime.

This indicated increase in reported cybercrime cases. A total of 248 cases were reported during the period under review compared to 198 cases reported in 2018.

Q1: 2020

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: 2020

Unsecured remote connections grew by over 30%.

The use of remote access technologies like RDP (Remote Desktop Protocol), VPN (Virtual Private Network) skyrocketed 41% and 33%, respectively globally. Uganda registered 30% increase in unsecured connections.

Q3/Q4: 2020

Gradual adoption of remote working.

As a result of the COVID-19 Pandemic, many organizations in Africa, including Uganda 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 is forcing anything which can digitize, to digitize.
- Organisations are moving to more managed services to cope with strain on limited resources.
- Business continuity models 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 parties vendors and vulnerable systems, will be weak links, forming a primary access compromise point that need to be checked thoroughly.
- Malware attacks are expected to rise, especially locally developed or re-engineered malware.
- We also anticipate 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 - Uganda 2019/2020, 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 Kampala Chapter

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

Milima Security

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

Milima Security Contributors

- Emmanuel Agape Chagara - Research Lead
- Jerome Okot - Research Co-Lead
- Sandra Namiiro
- Joy Amanda
- Gordon Fredrick Kateregga

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

- 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

→ **Andrew Walusimbi**

Head

Information Security, Ecobank Uganda

→ **Noah Balesanvu**

Chairperson

National Information Security Advisory Group(NISAG)

→ **Wilbrod Owor**

Executive Director

Uganda Bankers' Association

→ **Paul Kavuma**

Chief Executive Officer

Uganda Insurers' Association

→ **Simon Peter M. Kinobe**

Partner

Ortus Africa Advocates

→ **Dr. Paula Musuva**

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

→ **Robert Kirunda**

Kirunda & Wasige Advocates.

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

Uganda experienced significant growths in it's cybersecurity sector for the years 2019 and 2020 with significant achievements being registered in the two years as opposed to the previous years.

Following Uganda's consent to the Malabo Treaty of 2014 on African Union Convention On Cybersecurity and Personal Data Protection, Uganda went on to enact into law it's own Data Protection and Privacy Act (DPPA) in February 2019. The enactment of the DPP Act meant a bold step by the government to oversee maturity of the nation in regards to data privacy and information security. Not surprising, a report by the National Cybersecurity Index (NCSI) of Estonia which assesses UN subscribing countries for cybersecurity initiatives and digital growth placed Uganda as top of African nations for cybersecurity maturity in that year

The year 2020 came with many promises of technological advancements owing to the already exponential growth in the Information and Communications Technology (IT) witnessed across many sectors of the economy. These hopes were quickly put to a shocking halt with the emergence of COVID-19 which went on to become a global pandemic. By March 2020, many nations across the globe, including Uganda had nearly shut down with only minimal activities being conducted.

COVID-19 pandemic brought about a paradigm shift to our way of life which could not have been imagined in the near future. A notable transition that organisations had to embrace was remote working and subsequent integration of technologies into day-to-day operations. Whereas a handful or organisations had mastered the art of remote-work and vast adaption of day-to-day digital tools, many local businesses had to adapt the hard way.

As organisations struggled to adapt to the new way of life commonly referred to as the "new normal", bad actors took to the field and quickly cybercrime became the second biggest crisis. Cybercrime is reported to have had a 300% fold growth in the year 2020. Hackers took advantage of the fear and anxiety across the masses to spread various forms of malware embedded in malicious links, smishing and phishing emails. The World Health Organisation went on to categorize this crisis as "Infodemic".

As many nations continue to wage war against a still extensively dangerous disease, organisations have had to embark on reviewing and strengthening their business continuity plans to ensure businesses are operational amidst the crisis. Ugandan businesses of all sizes have had to evolve in the way they do business with significant emphasis now being placed on: improving and strengthening of ICT resources; cybersecurity strategies; recruitment of experienced cybersecurity and data privacy personnel; and for some, establishment of ICT and Cybersecurity departments.

As you read this report, we hope you find valuable insights drawn from the past 2 years that can help you build workable strategies to not only survive another year but thrive to become more cyber secure. At Milima Security and Africa Cybersecurity Report Team, we are committed to supporting you through provision of such valuable insights as we build a cyber secure Uganda.

Emmanuel A. CHAGARA

CEO, Milima Security and Milima Cyber Academy

EXECUTIVE SUMMARY

As the year 2020 heads to a close, many people remain confounded by how the whole world turned out as a result of the Covid-19 pandemic. Ever since news of the Coronavirus started seeping out of Asia and grabbing global headlines, literally every plan, projection and expectation has been upended, making it the strangest year in recent memory.

By December 2019, for instance, cybersecurity experts prepared a list of top trends expected in 2020 including a steady growth of artificial intelligence and machine learning and the spread of 5G and the Internet of Things (IoT), but by the beginning of March this year, many of these had changed, or slowed down tremendously.

In the last few months, we have seen a quick reconfiguration of entire IT systems to accommodate work from home and remote meeting as well as implementation of business continuity plans. Within six months, webinars, zoom meetings and remote access became the norm rather than the exception. Affordable, fast internet access to cloud services and general understanding of how to use remote technologies has become a necessity for every working executive.

The upshot of a disruption of what was previously the normal course of business and an attendant rise in reliance on technology, was the increase in cybersecurity attacks as criminals stepped up their foray into weak and exposed networks. Consequently, we witnessed a sharp increase in malware distribution, business email compromises, the spread of fake news and mobile money network fraud.

Over the last eight years, we have consistently championed cybersecurity awareness, spreading the word across the African continent at every opportunity and urging every organisation to invest in secure systems and processes. This year, with all the developments I have outlined above, it has become even more urgent. It means that every institution must integrate cyber-security risk into its overall management and requires a shift away from the traditional risk-controls approach to a threat intelligence driven cyber risk programs.

It means they must fast track a number of short term interventions including enabling remote access with Two Factor Authentication (TFA), setting up strong anti-virus applications, consistent environmental scanning for misconfigurations and look out for phishing emails and sites. They should also avoid installing any news software, employ transaction monitoring tools and update and exercise business continuity plans.

For the long term, it is important for organisations to build capacity to withstand cyber threats by remaining focused on the broader intelligence based cyber risk assessment and management and investing in cloud based data management. Cyber insurance will also take a more central role in their overall threat management as a number of local underwriters already offer these solutions. Finally, the need for robust policies covering teleworking and all independent devices (also known as BYOD) will be paramount.

William Makatiani

CEO, Serianu Limited

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. UGANDA'S CYBER LANDSCAPE

2019/2020 was marked by an increase in both innovation and attacks techniques across all key sectors from financial services, government, manufacturing and insurance.

1.1. INNOVATION IS ON THE RISE

The pace of digital adoption over the past two years has surpassed expectations and this trend is likely to accelerate further. The increasing role of technology has heightened customer expectations and transformed the way customers interact with financial institutions

Innovations in the Banking Sector

PDQs machines and cards

ATM bulk note acceptors

Agency banking

Innovations in the Manufacturing Sector

Electronic Cargo Tracking Systems

URA
Uganda Revenue Authority

Innovations in the Public Sector

EduTrac

(a mobile phone-based data collection system being piloted by the Ministry of Education and Sports and UNICEF)

EDU TRAC

Ministry of Education and Sports

unicef for every child

1.2. POSITIVE UGANDA'S RANKINGS ON GLOBAL SCALE

Uganda was ranked as the most secure cyberspace in Africa in the 2018 Global National Cyber Security Index. Previously 2nd in the 2017 ranking, the elevation to the number 1 spot is exciting news for the nation. 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 1. *National Cyber Security Index (NCSI).*

Country	Rank	National Cyber Security Index	Digital Development
Nigeria	45	54.55	35.86
Uganda	51	50.65	33.09
Kenya	77	35.06	41.69
Ethiopia	85	32.47	30.39
Ghana	89	31.17	45.25
Rwanda	97	27.27	38.76
United Republic of Tanzania	129	12.99	29.76

E-Government Development Index (EGDI)

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

TABLE 1: *E-Government Development Index (EGDI).*

	Country	Rank 2020	EGDI 2020
	Kenya	116	0.5326
	Rwanda	130	0.4789
	Uganda	**137**	**0.4499**
	United Republic of Tanzania	152	0.4206

Threats and Cyber Crime Trend

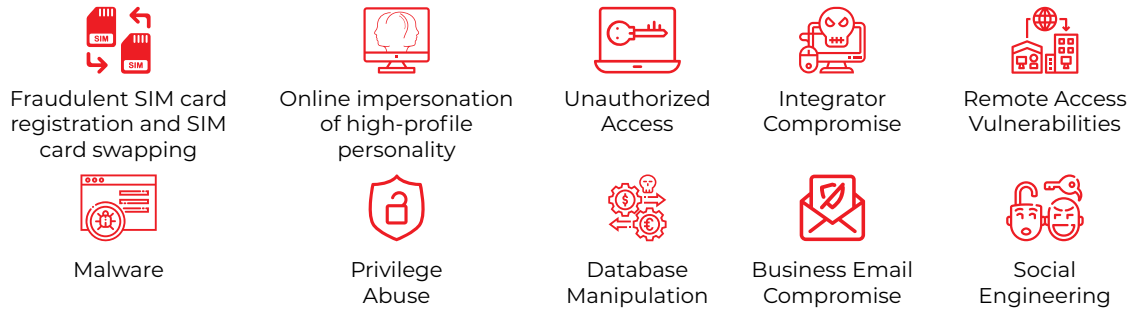
A total of 248 cases were reported during the period under review compared to 198 cases reported in 2018.

TABLE 2: *Threats and cyber crime trend.*

No.	Category	No. of Cases Reported	
		2019	2018
1.	Cyber (Computer) Crimes	248	198

The major Fraud categories of cybercrimes identified were:

FIGURE 2. *Major Fraud categories of cybercrimes.*



Some of the cases handled by the Uganda Police in 2019 included;

Cybercrimes led to a loss of **Ugx. 11,446,603,500** in **2019** in which **Ugx. 51,890,000** was recovered.

TABLE 3: *Some of the cases handled by the Uganda Police in 2019.*

	Crime	Amount	From
CPS Kampala CRB 1473/2018	Unauthorized Access and Theft of Money	Ugx. 2,600,000,000	Beyonic Ltd Systems
CID Headquarters E/369/2018	Unauthorized Access and Theft of Money	Ugx. 802,000,000	MTN Uganda
CID Headquarters GEF 604/2019	Unauthorized Access and Theft	Ugx. 383,000,000	DFCU Bank
CPS Kampala 1457/2019	Unauthorized Access and Theft	Ugx. 800,000,000	Centenary Bank
CID Headquarters GEF 705/2019	Unauthorized Access and Theft	Ugx. 116,000,000	True African Systems

Breakdown of some of the Cyber offences reported 2018/ 2019 by Uganda Police.

TABLE 4: *Some of the cyber offences reported handled by the Uganda Police in 2018/2019.*

	Cyber Offence	Number of cases reported	
		2019	2018
1	Electronic Fraud	68	76
2	Unauthorized Access	27	10
3	Cyber Harassment	4	7
4	Cyber Stalking	2	1
5	Unauthorised Disclosure of Information	2	2
6	Unauthorized Modification of Computer Material	0	2

1.3. MOBILE FRAUD

Fraudulent SIM card swapping and registration

During the year 2019, a number of cybercrimes were committed using pre-registered SIM cards to steal money from unsuspecting victims. In total 519 fraudulently swapped (duplicated to make two lines with same number to work at the same time) pre-registered SIM cards were used to transfer and steal monies from various banks and mobile money accounts

Method of operation by the criminals

Some scrupulous telephone company agents fraudulently;

i. Obtain the biometrics of unsuspecting persons more than once, and

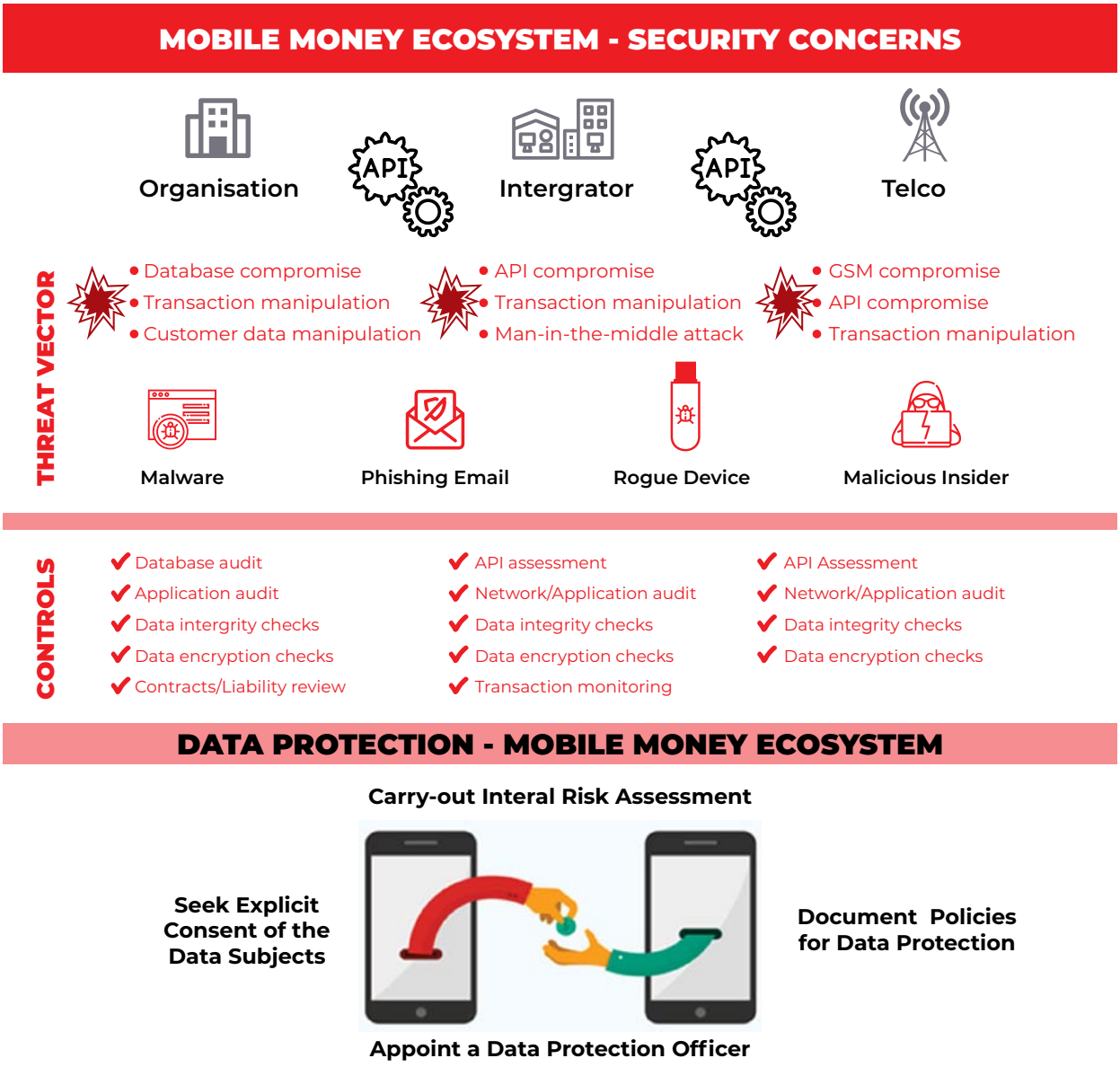
ii. Make more copies of the National Identity card of unsuspecting persons and later register more than one SIM card in the names of the unsuspecting persons whose biometrics have been taken more than once and more copies of National;

- Identity cards have been made behind their backs.
- The agents then start selling pre-registered SIM cards to people with criminal intentions.

- The criminals would use the numbers to negotiate ransom, defraud and coordinate their criminal activities among themselves.
- Criminals also use Mobile Banking numbers to steal money from Banks by swapping registered numbers without the knowledge of the registered owners, transfer funds from
- Banks to the swapped numbers, and withdraw the stolen monies from Mobile money outlets.

Uganda Communications Commission as a regulator issued directives that all telephone SIM cards must be registered using National Identity cards.

Telephone companies use agents to register SIM cards and all these agents have been given Biometric machines to obtain fingerprints.



Moving Ahead

As Cyber-attacks increase and institutions continue to innovate, it's clear that majority of attackers are leveraging on weak systems and poorly integrated services. Institutions need to pay close attention to new systems integrated into their network and also apply QUALITY ASSURANCE before, during and Post implementation.

Application software concerns to consider:

1. System integration testing

Core banking applications are now integrated to numerous other systems such as Mobile money, ERP, ATM Switches etc. This interdependency allows for faster transaction processing from multiple channels but also introduces new risk areas that need constant assessments. The most common interactions occur as follows:

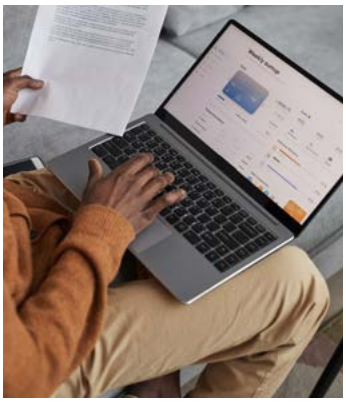
- **File based interaction:** Files in excel, csv, xml formats can be used to send instructions between systems, the challenge with this mode of integration is also depended on the security during transit of files. Files would require some level on encryption and decryption depending on the sensitivity of data.
- **Web services:** Used for communication between online systems.
- **Direct database connection:** Application is allowed to update another application's database.

Consequently, System Integration Testing has become a Must Do for banking organisations. This would typically cover:

- Interface testing
- Logical controls review
- Data integrity and confidentiality reviews
- API Testing: APIs facilitate communication between different tiers or applications, this separation enable easy understanding of application for new entrants, easy to make changes and track its effect in the application.

DATA PROTECTION – IT'S RELEVANCE AND IMPACT TO THE BANKING SECTOR

In this age of mobile banking, the Data Protection Act acts as another line of defense, helping to ensure the survival of banking platforms operating online. The law reinforces the procedures to follow in the event of a breach, which will prove vital in avoidance of reputational damage and demonstrating practical techniques to the regulator and ultimately to the customer.



Andrew Walusimbi

Head, Information Security, Ecobank Uganda

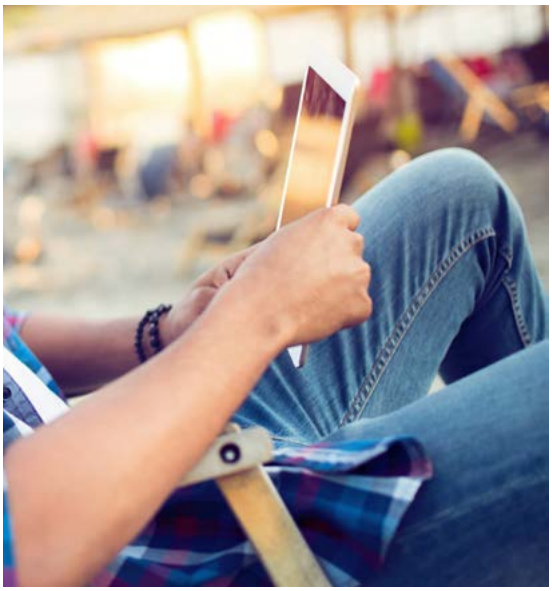
It is evident that banks are innovating more than ever – a true testament to their increasing technological and data expertise.

The data protection and privacy act can be a genuine strategic move banks can use to integrate data protection into their processes and core development strategies creating bolder opportunities for innovation, differentiation, and strategic advantage in an increasingly competitive sector.

The DPPA will improve the already high standards of financial services in the handling of customer data for example, under this law, institutions must clearly outline the purpose for which personal data is collected and seek additional consent if they want to further share the data with third parties.

The enactment of the law opens doors for legal action against organizations that will not comply. For example, unlawfully obtaining or using personal data by an individual warrants a 245,000 currency points fine or ten years in prison. Courts are also at liberty to issue institutions fines not exceeding 2 per cent of an organization's annual gross turnover depending on the gravity of the offense.

As we anticipate the enforcement authority - National Information Technology Authority (NITA-Uganda) to determine the regulations for all matters necessary to advance this law, Banks can prepare by establishing what type of personal data they collect, store and process, know where it is, how it is protected and how it flows within and outside the organization, keeping an eye on the supply chain ecosystem as well.



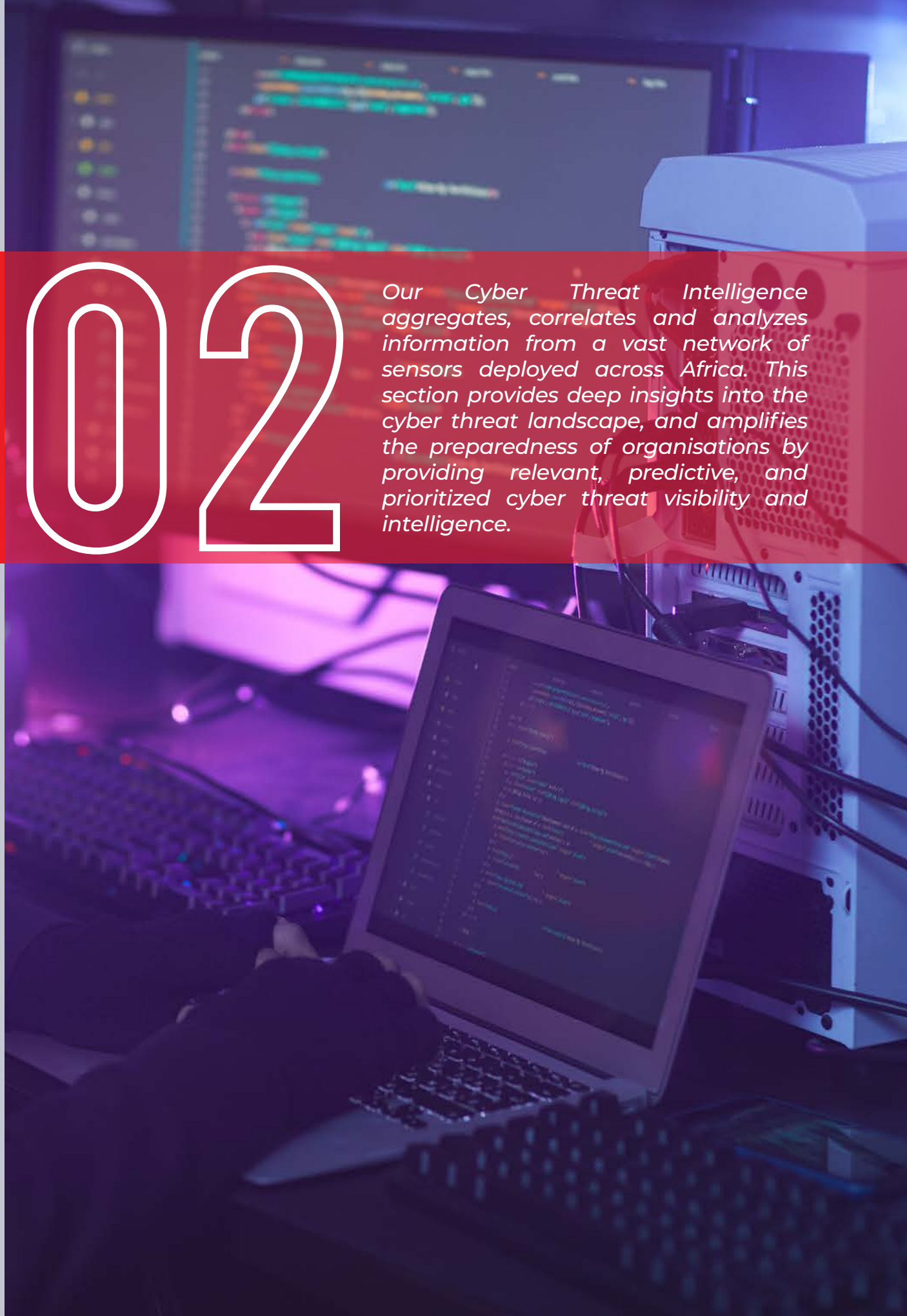
Banks should consider providing for a Data Protection Officer role; whose primary task is to help the institution comply with this law. This person is also responsible for creating awareness among staff, operationalizing breach detection and response planning by Implementing security technologies that can map and protect personal data. This will greatly help institutions on their journey to compliance.

If correctly enforced and implanted, this will have a domical effect across the region by encouraging the growth of digital banking, driven by high levels of consumer trust in technology and data protection.

The enactment of the law opens doors for legal action against organizations that will not comply.

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 can be contaminated with malware that permits programmers to remotely assume responsibility for various devices one after another, for the most part without the information on the gadget owner.

Approaches to prevent botnet malware:

- Introduce trusted, powerful antivirus applications on your PC.
- Set your software settings to update automatically.
- Be cautious what you click, download, or open.

Ransomware

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

Users are told guidelines on the best way to pay an expense to get the decoding key. The expenses can go from a couple of hundred dollars to thousands, payable to cybercriminals in Bitcoin.

Approaches to prevent a ransomware:

- Always make sure your operating system is kept upto date.
- Try not to introduce a software except if you know precisely what it is and what it does.
- Introduce antivirus software, which detects malicious programs like ransomware as they show up, and whitelisting software, which keeps unapproved applications from executing in any case.
- What's more, obviously, back up your documents, oftentimes and automatically. That won't stop a malware attack, yet it can make the harm brought about by one considerably less significant.

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.

TABLE 5: *Top 10 malware families in Q1-2019.*

	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 Q2-2019.*

	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 Q3-2019.*

	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 2019.*

	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.OCKKltr	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.lA93!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

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 to know what to share and what not to share?" African Culture and Privacy is a good and timely theme because one of the key concerns when dealing with privacy is foreign ideals, because these technologies were not developed in the continent. The understanding of privacy differs from continent to continent.

Noah Balesanvu

Chairperson, National Information Security Advisory Group(NISAG)

When you look at Europe, it is one of the most privacy eccentric continents we have on earth. Their culture is heavily privacy dependent.

Privacy concerns grow softer when you get to USA and when you go to Asia, it completely takes a different turn, because privacy is handled by the state on behalf of the people.

In Africa, we are yet to define our own culture. Our African culture is largely social where the economy is built around sharing. When we talk about policy, we need to put into context, what that means in our culture. We need to define for ourselves what data privacy is in light of the way African culture is, our social fabric.

It's important to get certain basics out of the way. Africans can no longer be isolationists, meaning that this technology actually brings people together. How do we define for ourselves the rules of engagement when it comes to these technologies? There are certain personal identifiable basics for personal information. Information that is build private, , needs to be protected by the terms and conditions of the person that holds that information, and the system that holds that information should be designed in such a way that it respects those privacy lines. Africans have to be cognizant of the fact that conversations about privacy cannot be hard without the concerns of security being raised.

Africa is still defining its role in cyber security and being able to protect systems because the continent, is rapidly adopting digitalization and present conditions notwithstanding, the trajectory is still an accelerated slope, meaning that in a few years the entire government will be running online ,and majority of businesses will be conducted digitally. These businesses are not only offering services, they are thriving on the continent, meaning that there is an increasing number of subscribers, users, clients on the African continent that are consuming services digitally.

It's important that their privacy and security be taken into consideration. That's a balancing act that is sharply going to come into focus.

Africans lean toward a high breed where personal liberty and personal information is appropriately protected. However, there's going to be a greater mandate to organizations and states to protect data that's digitally captured. In terms of us getting into a culture of data privacy we need to be intentional about bringing this reality to Africans. That digital interaction is different from physical interaction, where you have the comfort of meeting face to face, seeing a person having a conversation and reading the body language. That doesn't exist in the digital realm and as such, appropriate measures must be taken to protect yourself and to protect your data.

These days' data is monetary and so, as professionals we are tasked with acclimatizing our people, subscribers, users, customers, citizens that their personal data is of value. Value has moved to the digital realm. Your data is valuable, your data is your identity, and your protection of it must be taken with the same rigor and the same conviction as your physical security.

A lot of education and awareness is needed to correlate physical security and privacy, with the digital realm. The strategy for us to adopt is to bring up the new reality to the citizens of the continent that we are now in the digital age, where data is a currency.

Your data is valuable, your data is your identity, and your protection of it must be taken with the same rigor and the same conviction as your physical security.

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 Uganda, the statistics are as equally staggering. Our research team's analysis revealed the following:

FIGURE 3. *Remote Connection Vulnerabilities in 2020.*

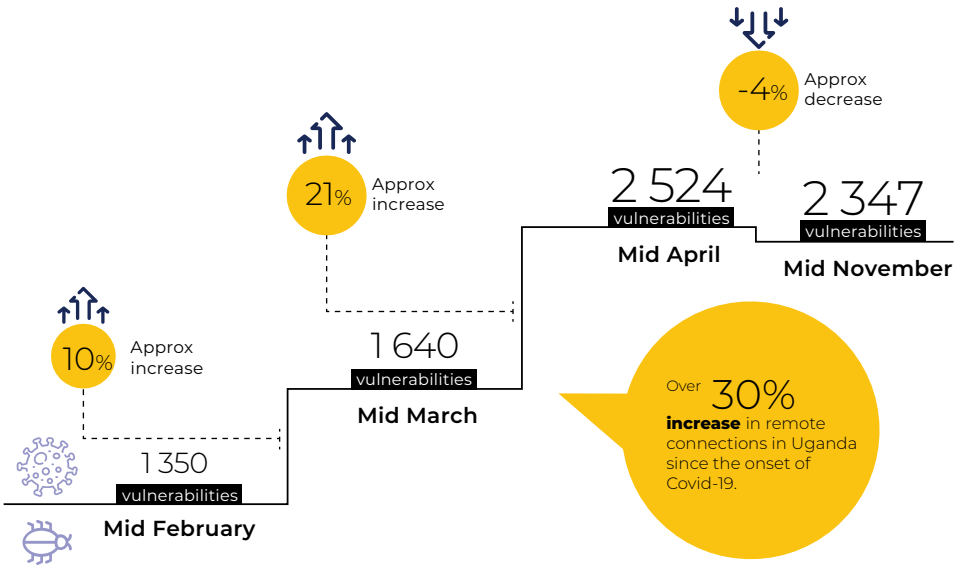


FIGURE 4. *Publicly Accessible Remote Connection Ports in Uganda (as at November).*

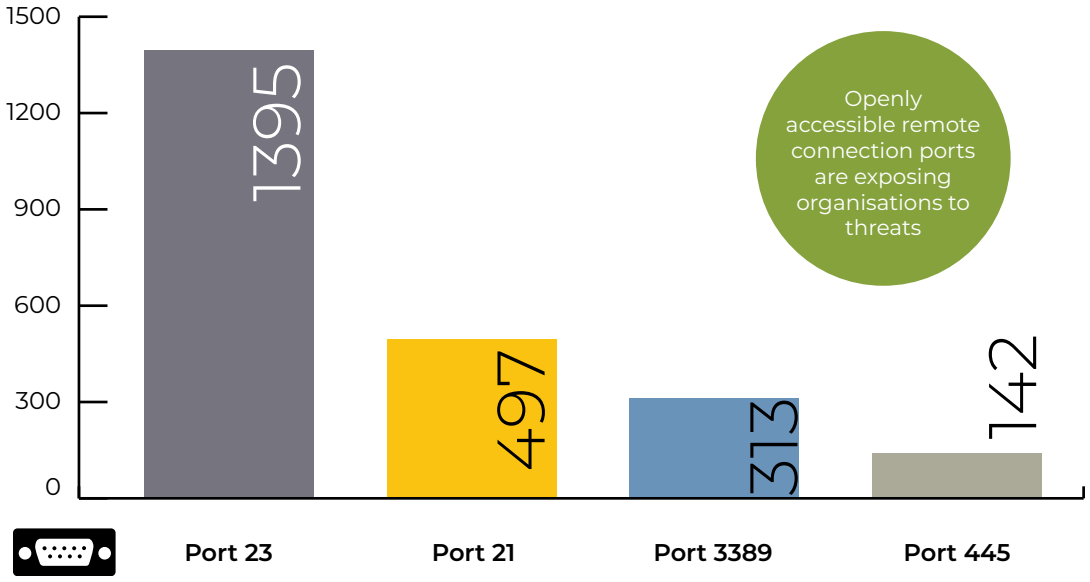


FIGURE 5. *Vulnerable Remote Connections.*

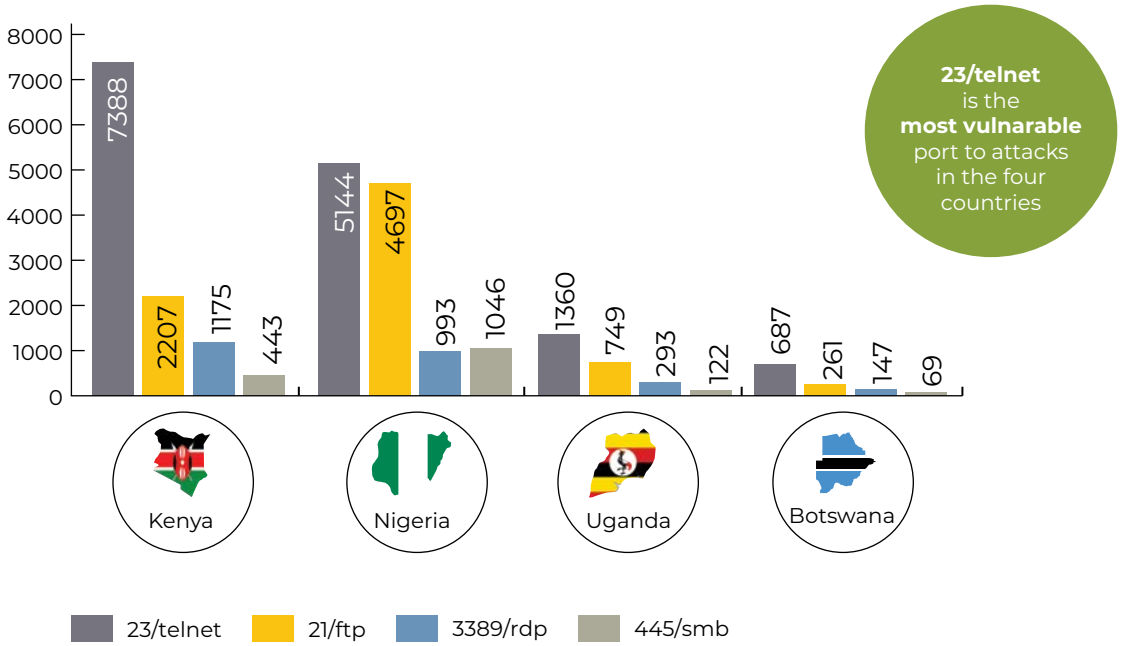
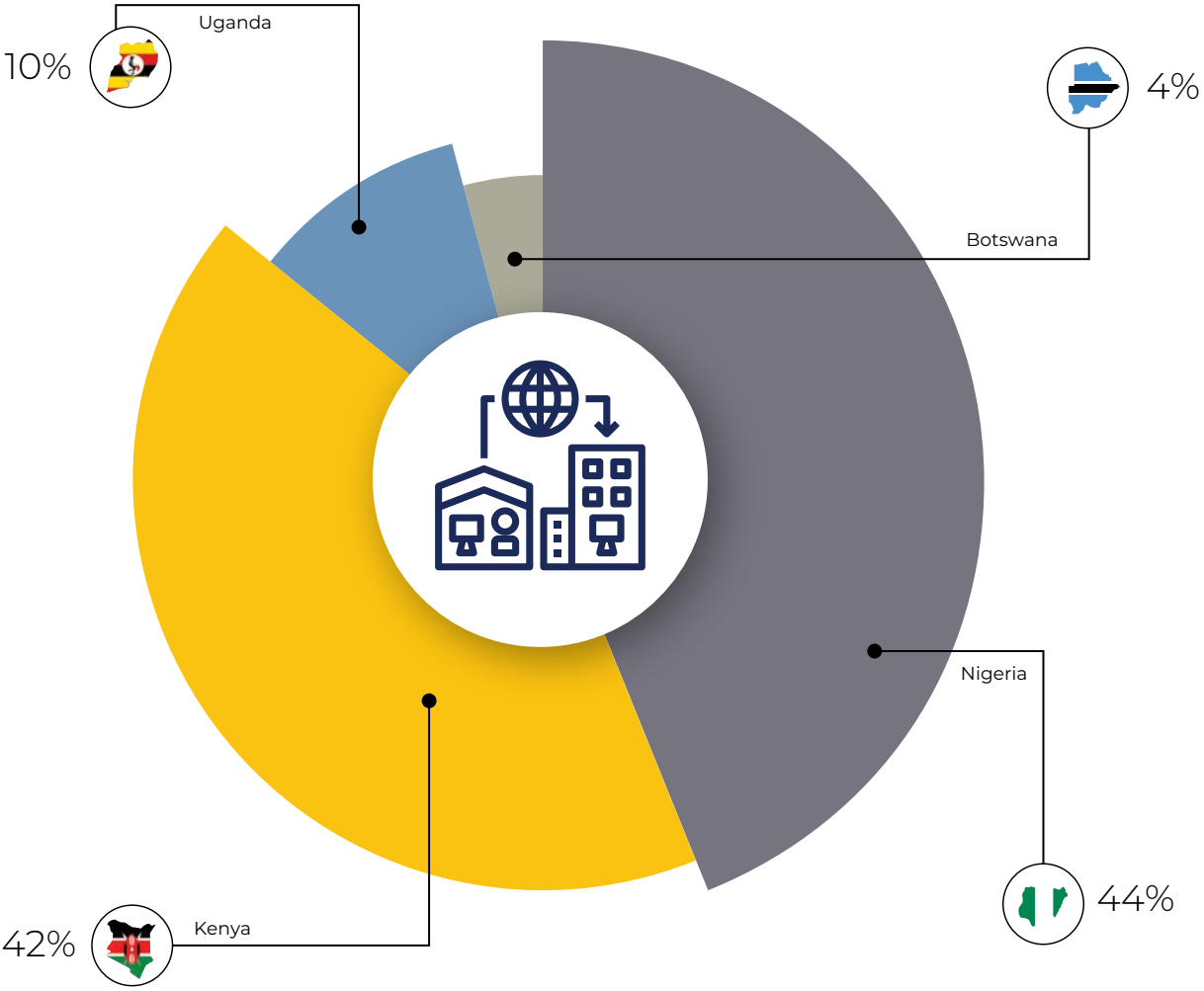


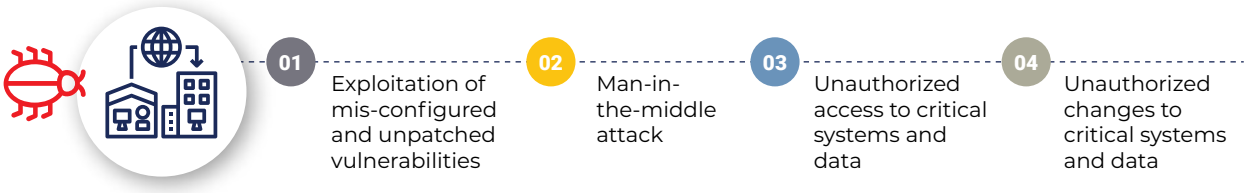
FIGURE 6. *Country Analysis – Insecure Remote Connections.*



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.

DATA PROTECTION LAW AND THE INSURANCE SECTOR

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

Paul Kavuma

Chief Executive Officer, Uganda Insurers' Association

This is certainly a good innovation and the current times require a close risk examination for efficiency.

From both a practice and industry perspective, cloud computing is indeed a growing space that cannot be ignored by any organization that is serious about growth and expansion. The world we now live in and the current working trends fully support the adoption of cloud computing technology.

Any organizations that are intending to transition into the cloud have got to take note of the cyber risks that are eminent from such a move and hence take full cognizance of these risks with good mitigation strategies. It is important to appreciate that not even a massive investment in Information security will totally eliminate cyber risk. As such the same importance should be attached to ensure that there is sufficient risk transfer to protect the business in the event of a breach. Cyber risks faced by the organization will range from operational disruption and regulatory compliance to lawsuits and reputational damage.

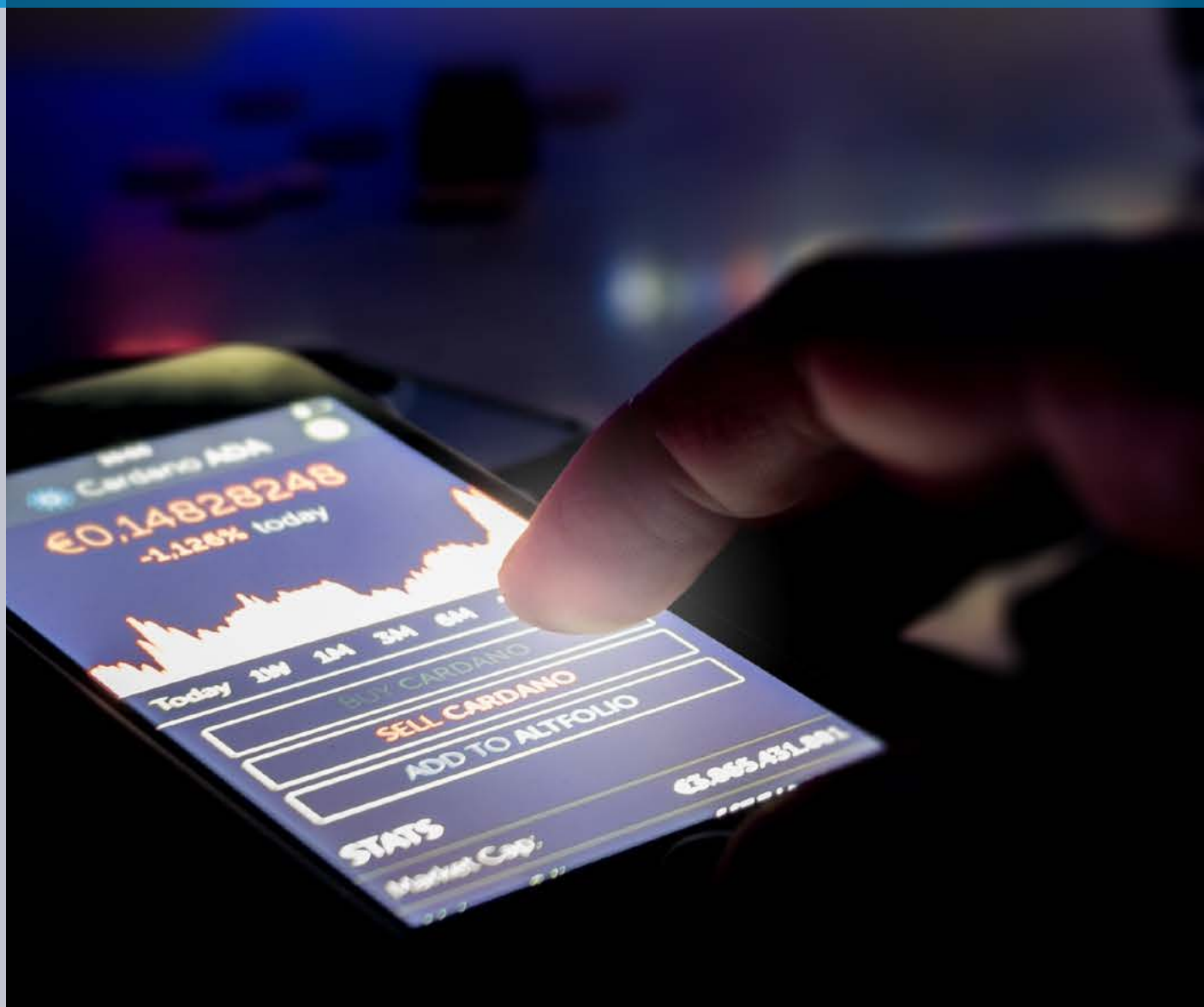
Our best advice as a sector is that when going into cloud computing one should seek professional counsel on risk mitigation measures on their cyber risks exposure. Additionally, they should seek out various options of remediating these risks via a well-structured and well thought out insurance cover. This is readily available in our market.

Cyber risks faced by the organization will range from operational disruption and regulatory compliance to lawsuits and reputational damage

03

The 2019 Cybersecurity Survey provides insight into what Ugandan 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.



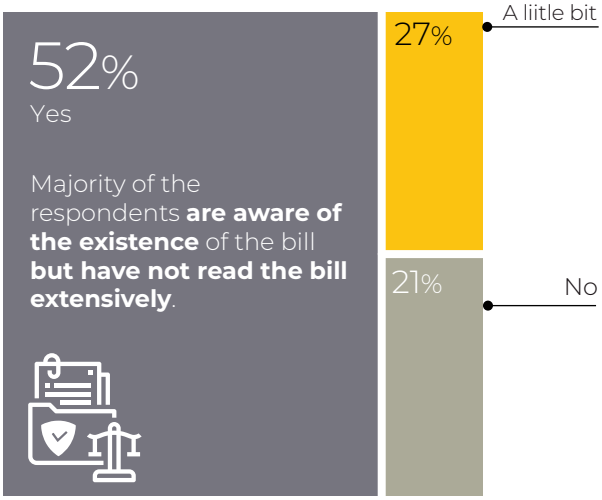
3. SURVEY ANALYSIS

3.1. DATA PROTECTION AWARENESS

3.1.1. Familiarity with Data Protection Bill

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

Are you familiar with any data protection bill?



What does it mean to be familiar with the data protection bill?

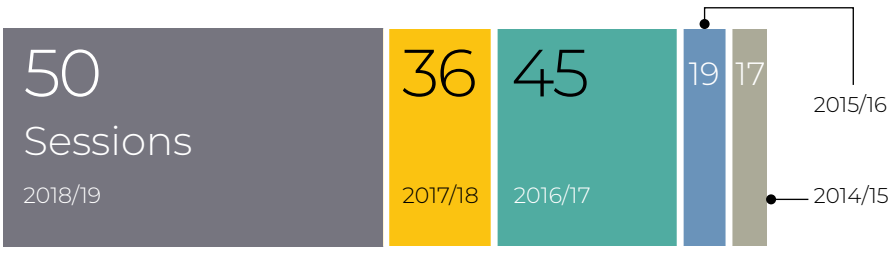
According to the respondents of the survey, it means ***"to be aware of its existence".***

The data protection bill tackles key data privacy issues ranging from data transmission, processing and storage requirements. The bill also defines critical roles for data protection in the organisation.

Important note:

A review of NITA statistics report 2019 indicates Sensitization activities to enhance awareness of the existence and application of the cyber laws have been conducted over the years by National Information Technology Authority.

In FY 2018/19, there was an increment of 20 percent in the number awareness sessions conducted across the MDAs and Local Governments from thirty six (36) sessions conducted in FY 2017/18 to fifty (50) sessions as shown below.



Source: National Information Technology Authority (NITA) - Uganda

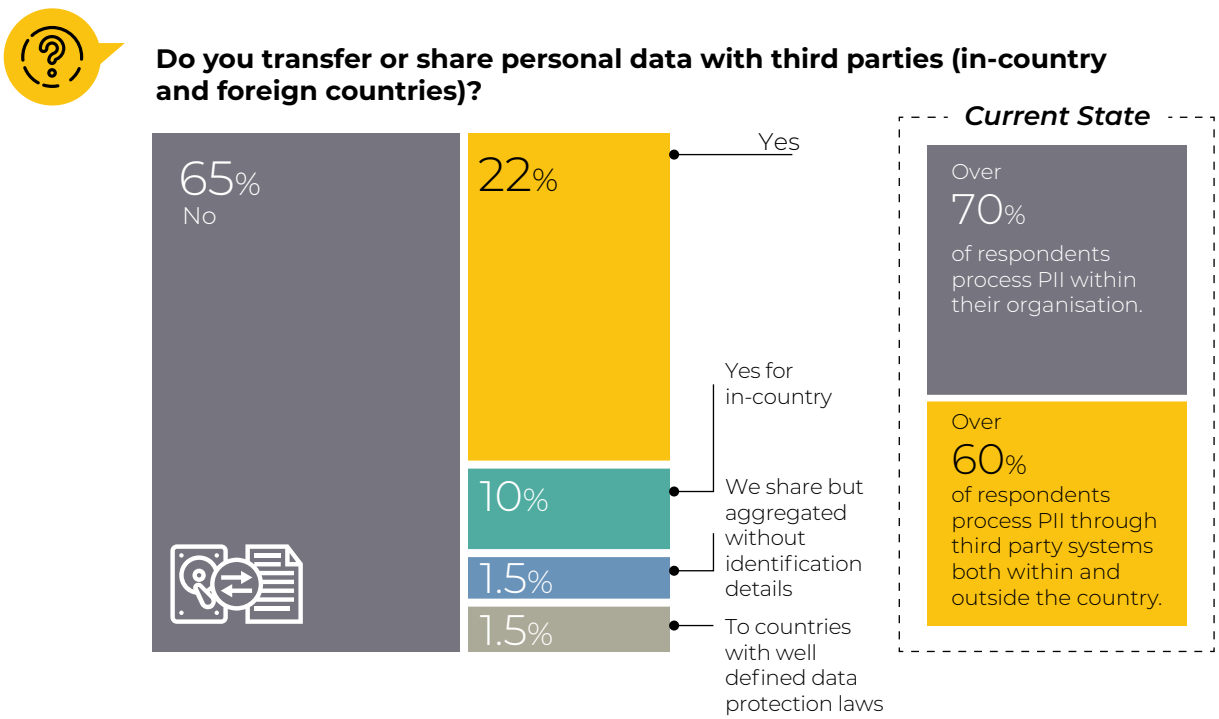
3.1.2. Processing of Personal Data

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:-

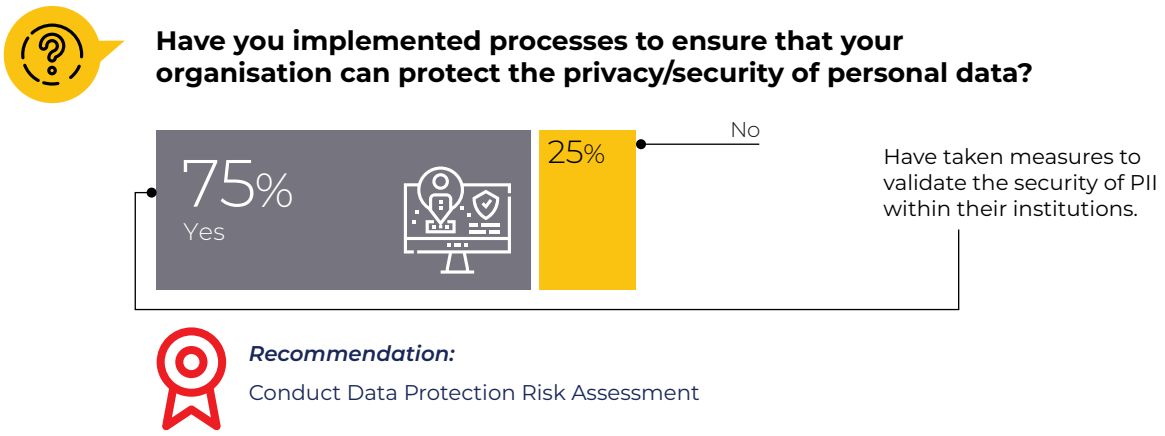
- Has sought and obtained express consent from a data subject; or
- Is authorized to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject

Requirement for data transfer: The transfer of personal data outside Uganda 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 Uganda.

3.2. IMPLEMENTATION OF DATA PROTECTION BEST PRACTICES

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

Protection of personal data



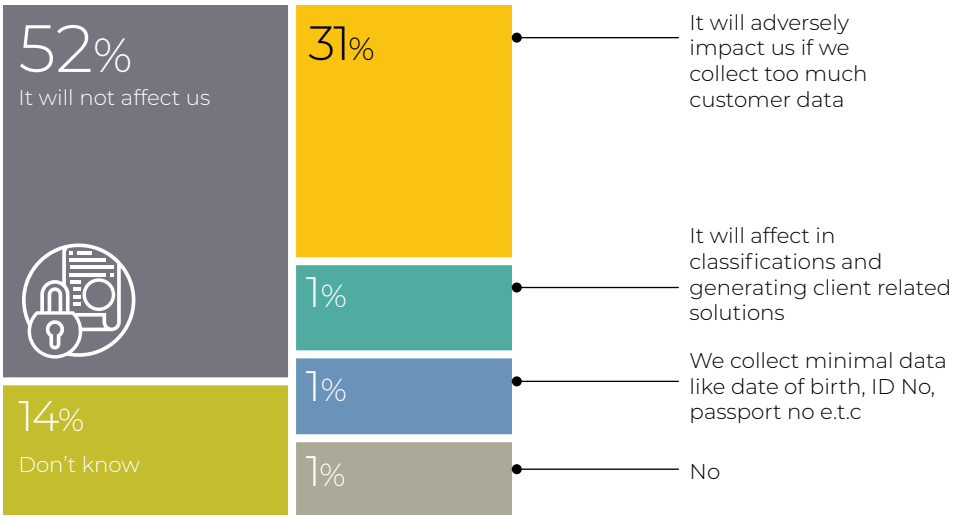
Requirement: An agency shall take the necessary steps to ensure the integrity of personal data in its possession or control through the adoption of appropriate, reasonable, technical and organisational measures to prevent:

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

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

Impact of Data Protection Law

How will the implementation of data protection law affect your organisation?



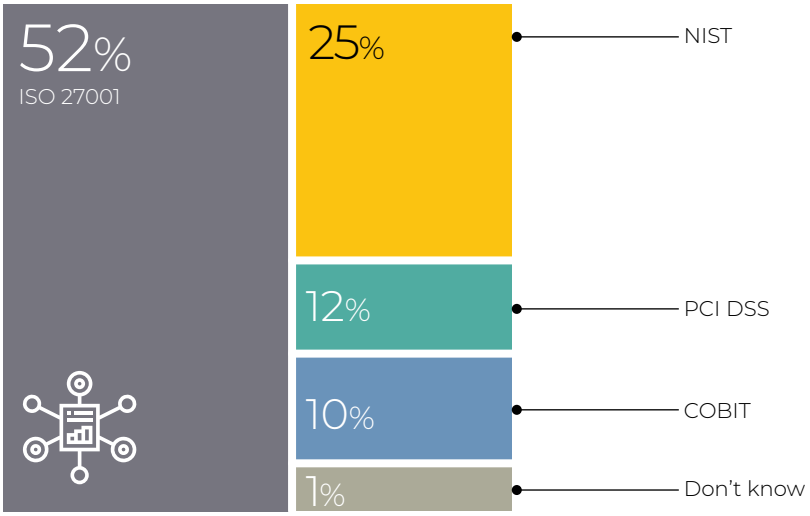
Recommendation:

Conduct an Impact Assessment to determine the extent of compliance/non-compliance. The law provides for fines of up to 5 million in cases of non-compliance.

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

Framework for data protection

What cyber risk management framework does your organisation use to assess and benchmark its approach and risk profile?



Important note:

The law doesn't prohibit or limit the adoption of other frameworks.

Why use a Cybersecurity Framework?

Cybersecurity frameworks 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

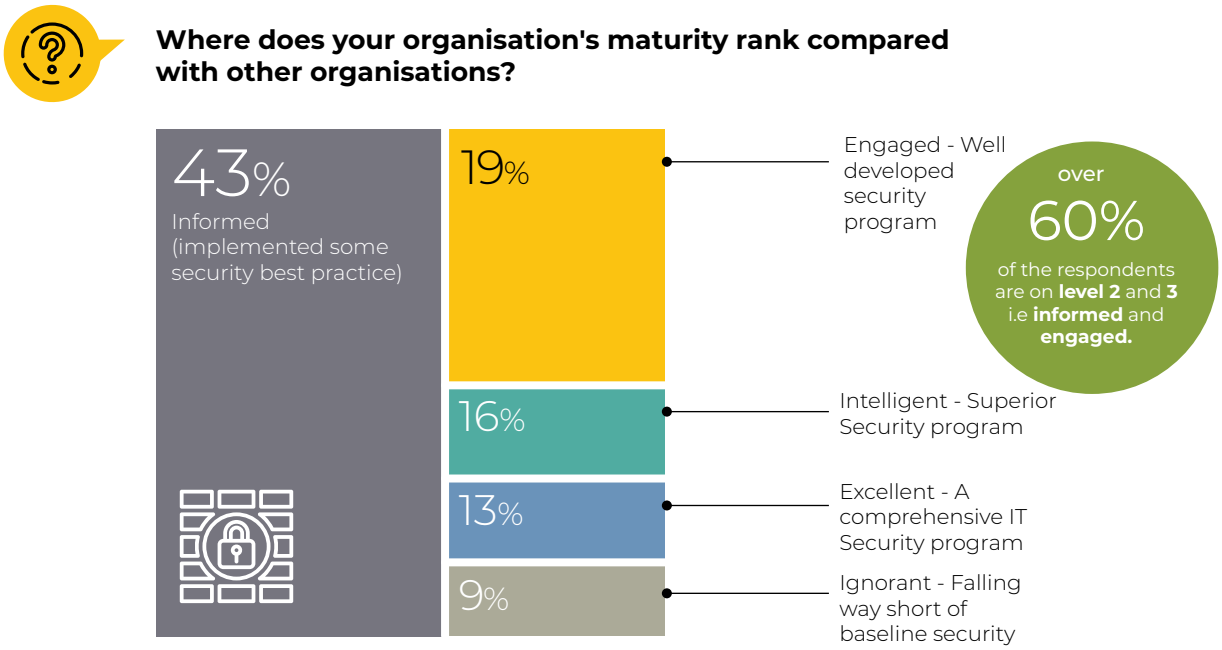


FIGURE 15. *Organisation's cybersecurity profiles.*

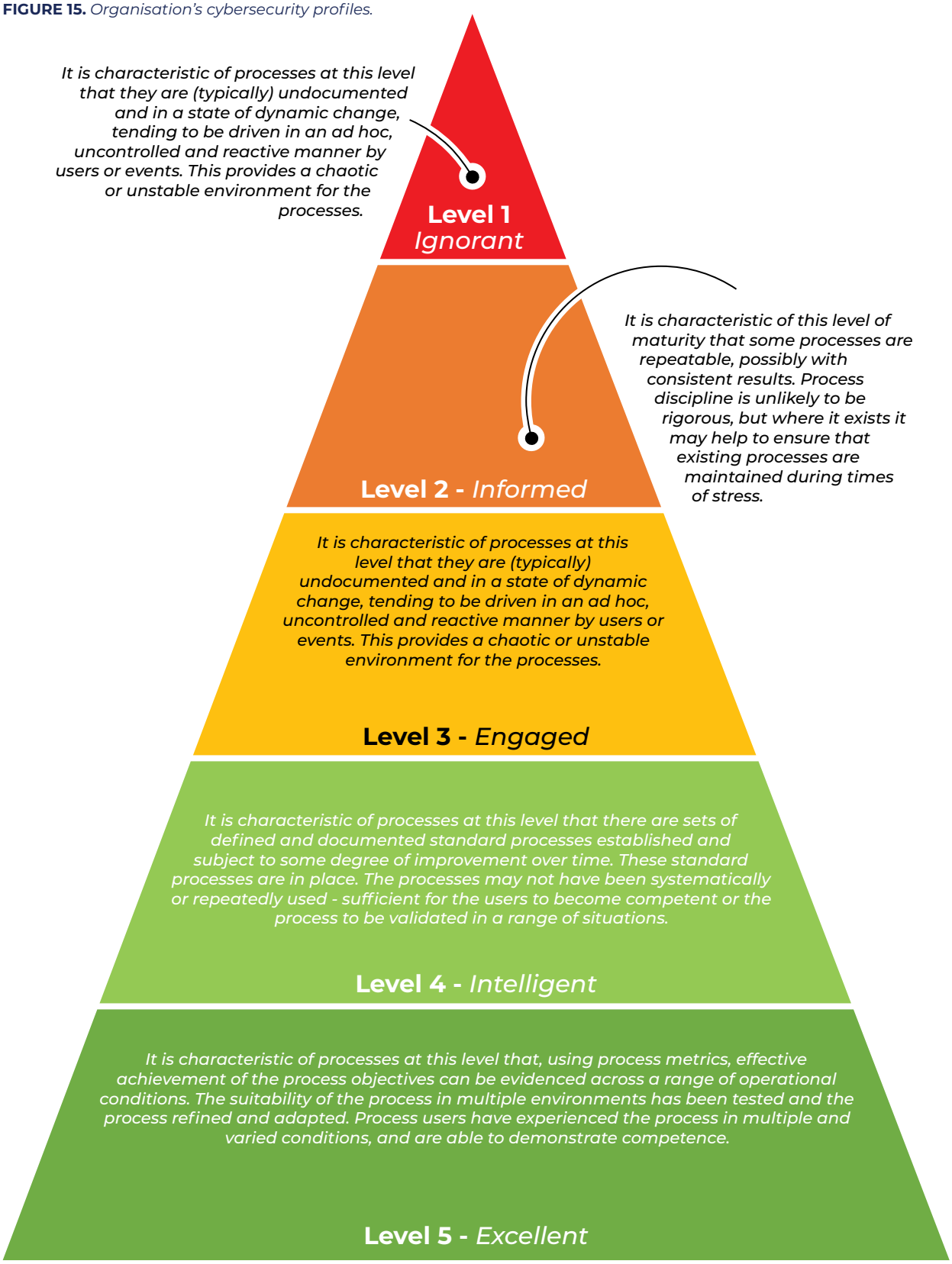
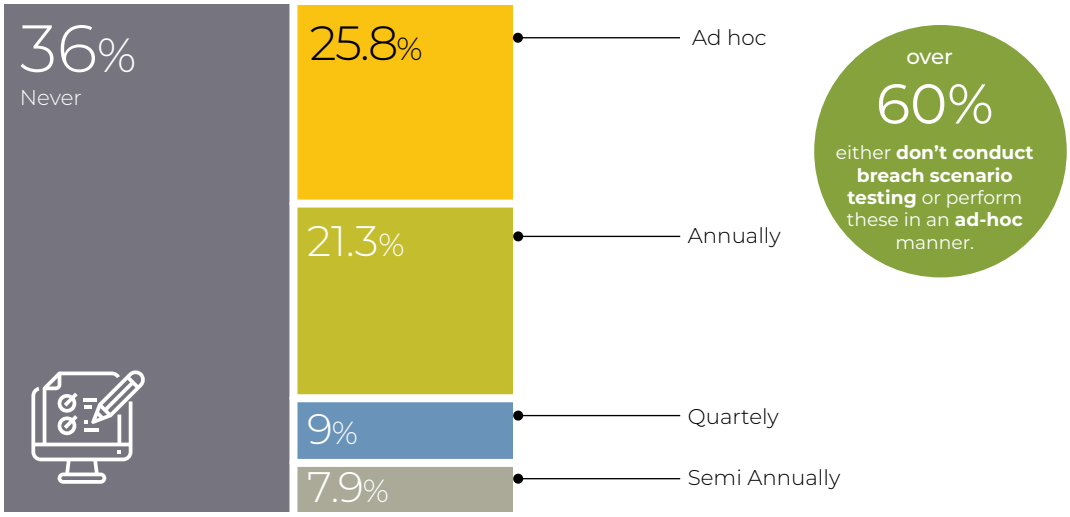


FIGURE 16. *Organisation's frequency of performing cyber breach scenario testing.*

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?

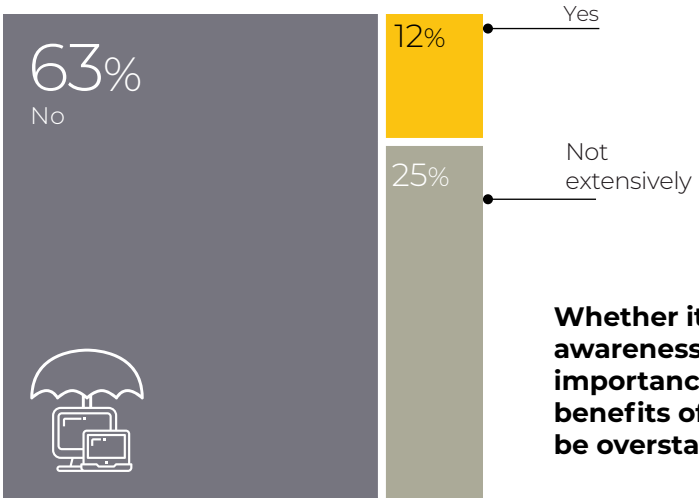
Important note:

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?



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

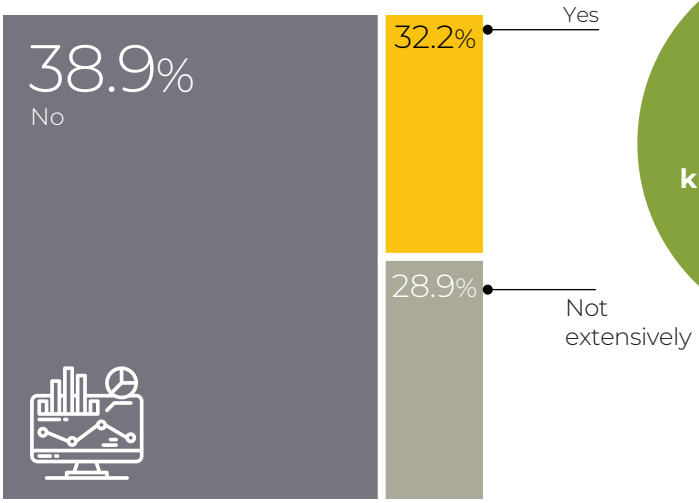
Total Target paid out of pocket

$162m

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

Reports and Metrics

Do you prepare reports and metrics to measure cybersecurity 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

Have you established benchmarks or target performance metrics for showing improvements or regressions of the security posture over time?

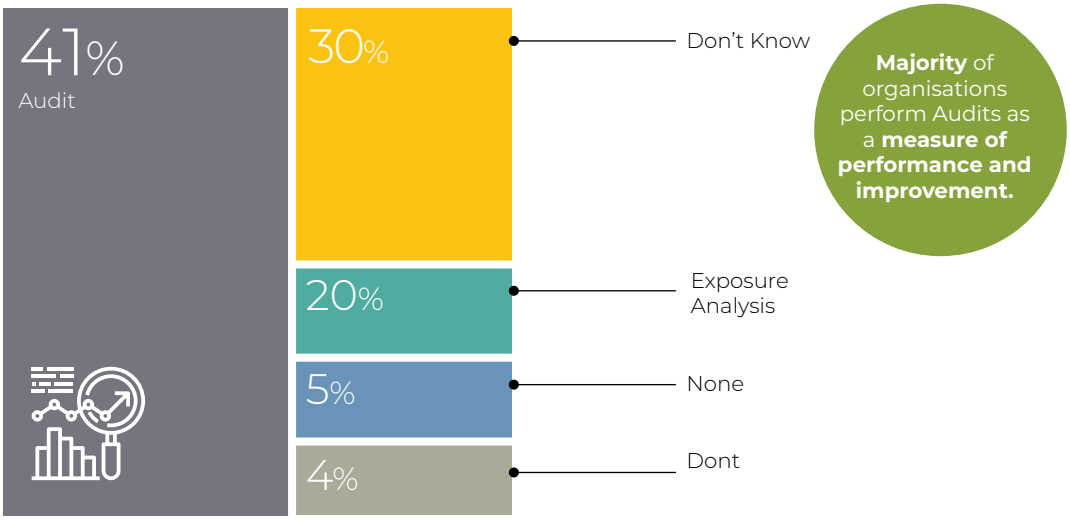


FIGURE 20. *Use of security testing techniques.*

Security Testing Techniques

Which of the following security testing techniques does your organisation use?

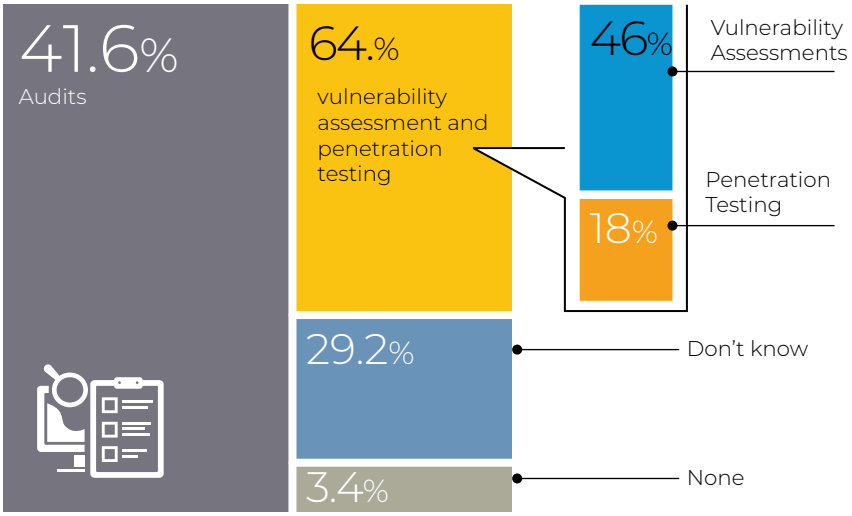
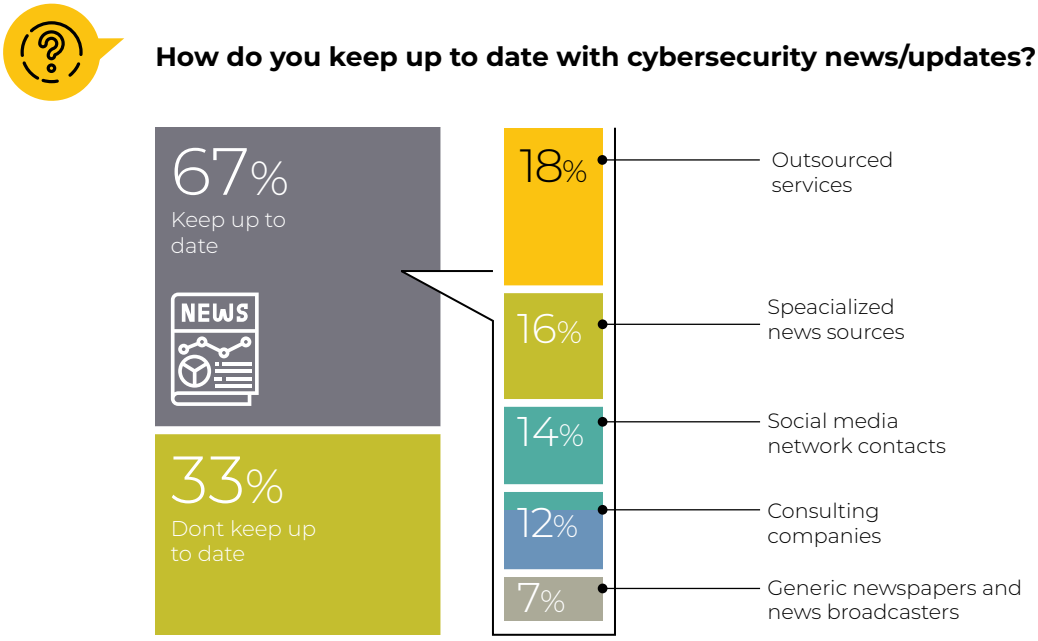


FIGURE 21. *Keeping up with cybersecurity news/update.*

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

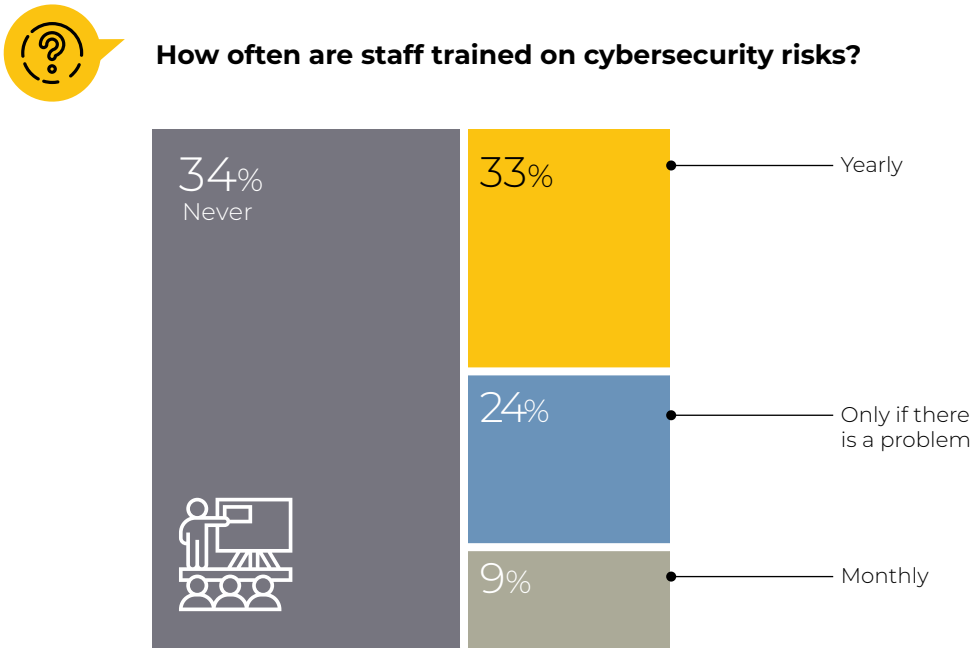
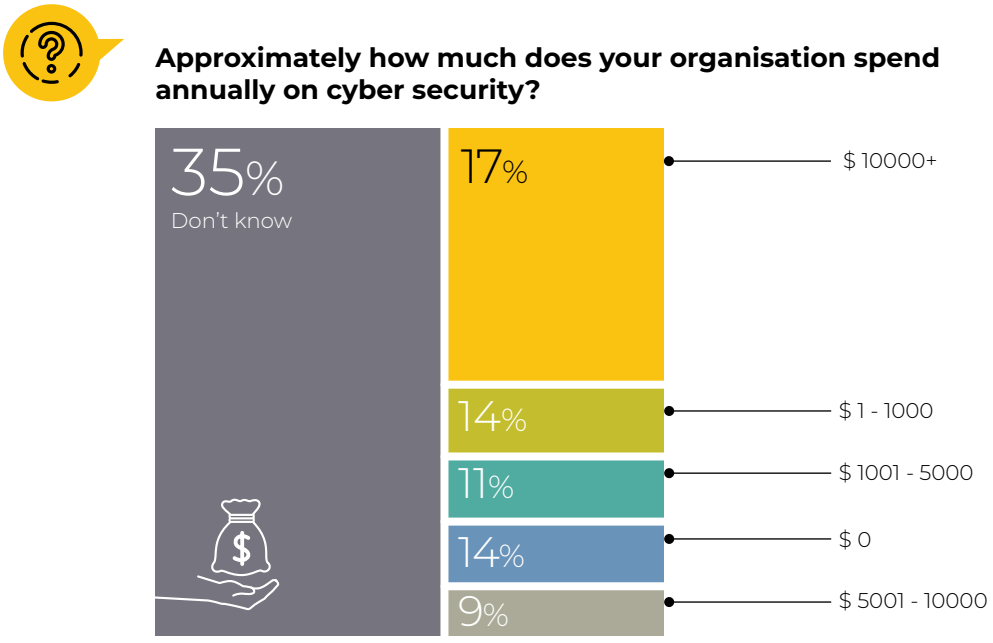


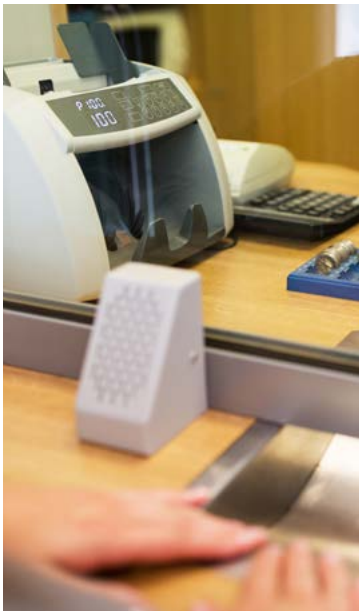
FIGURE 23. *Staff training on cybersecurity risks.*

Cybersecurity Expenditure



EFFECT OF THE DATA PROTECTION LAW ON THE BANKING SECTOR

Many people are still unaware of data protection and the various data protection laws that have been enacted to protect the data collected from them in their respective jurisdictions. We need to invest sensitization so that there is a better understanding data collection and protection, as well as the rights and penalties involved in the event of a breach of these rights.



Wilbrod Owor

Executive Director, Uganda Bankers' Association.

A huge aspect of data protection is consent. The data protection and privacy Act, 2019 of Uganda defines consent to mean any freely given, specific, informed and unambiguous indication of the data object's wish which he or she by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her.

While individuals need to be sensitized and made aware of the measures in place to protect any data collected from them, data collecting agencies or organisations need to ensure that they are legally protected while executing their duties. Consent is a focal part of data collection and any organisation needs to have measures in place that they have obtained the right level of consent when collecting data. To achieve this, organisations need to update all the forms used in data collection and ensure that they conform to the standards required by law in their respective jurisdictions.

In as far as consent is concerned, these forms need to be plain and clear to the data subject so that he or she is able to understand that his or her data is being collected and for what purpose and thereafter make a clear decision on whether or not to give consent or even withdraw where it could have already been given. Additionally, organizations should put in place data protection departments with officers that will oversee issues of consent and data protection and make sure that there is strict compliance to the respective laws.

In the banking sector, we are constantly sensitizing our officers & the rest of teams on this important piece of legislation vs our operations and revising the applicable documentation and processes therein accordingly. We are then reaching out to our service providers, partners & other stakeholders to embrace the demands therein of DPPA.

Consent is a focal part of data collection and any organisation needs to have measures in place that they have obtained the right level of consent when collecting data.

04

Uganda is the first East African country to recognize privacy as a fundamental human right, as enshrined in Article 27(2) of the 1995 Uganda Constitution as well as in regional and International laws.

4. DATA PROTECTION LAW

The Data Protection Act comes in to provide a legal framework on personal data usage, especially on digital platforms. Last year, the European Union passed the General Data Protection Regulations (GDPR) and the Ugadan data protection law is said to be GDPR compliant. The Bill recognizes that data protection forms part and parcel of the expectation of the right to privacy. The data protection laws will bring about several changes in the business environment.

One is that almost all businesses will have to put in place structures and operations to ensure compliance. Most businesses handle data. For example, when a client procures your services, you usually have a client database containing information about the client.

Therefore, this law will be applicable to businesses that either control or process data. As long as you are in direct control of another person's data then the law applies to you. The law sets out several requirements that must be put in place when handling another's personal data and this includes processing and profiling. The data must be handled lawfully, accurately and the data subject's consent must be given before it is shared with third parties.

STAY IN THE KNOW

GET TO KNOW

WHAT QUALIFIES AS PERSONAL IDENTIFIABLE INFORMATION ACCORDING TO THE LAW?

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.

4.1. 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).

4.2. 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.

4.3. SUPPORT SYSTEM FOR DATA PROTECTION

Presence of National CERT/CIRT/CSIRT

A computer incident response team (CIRT) is a group that handles events involving computer security breaches.

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 a 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).

Training and awareness

An awareness programme 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, individual rights.

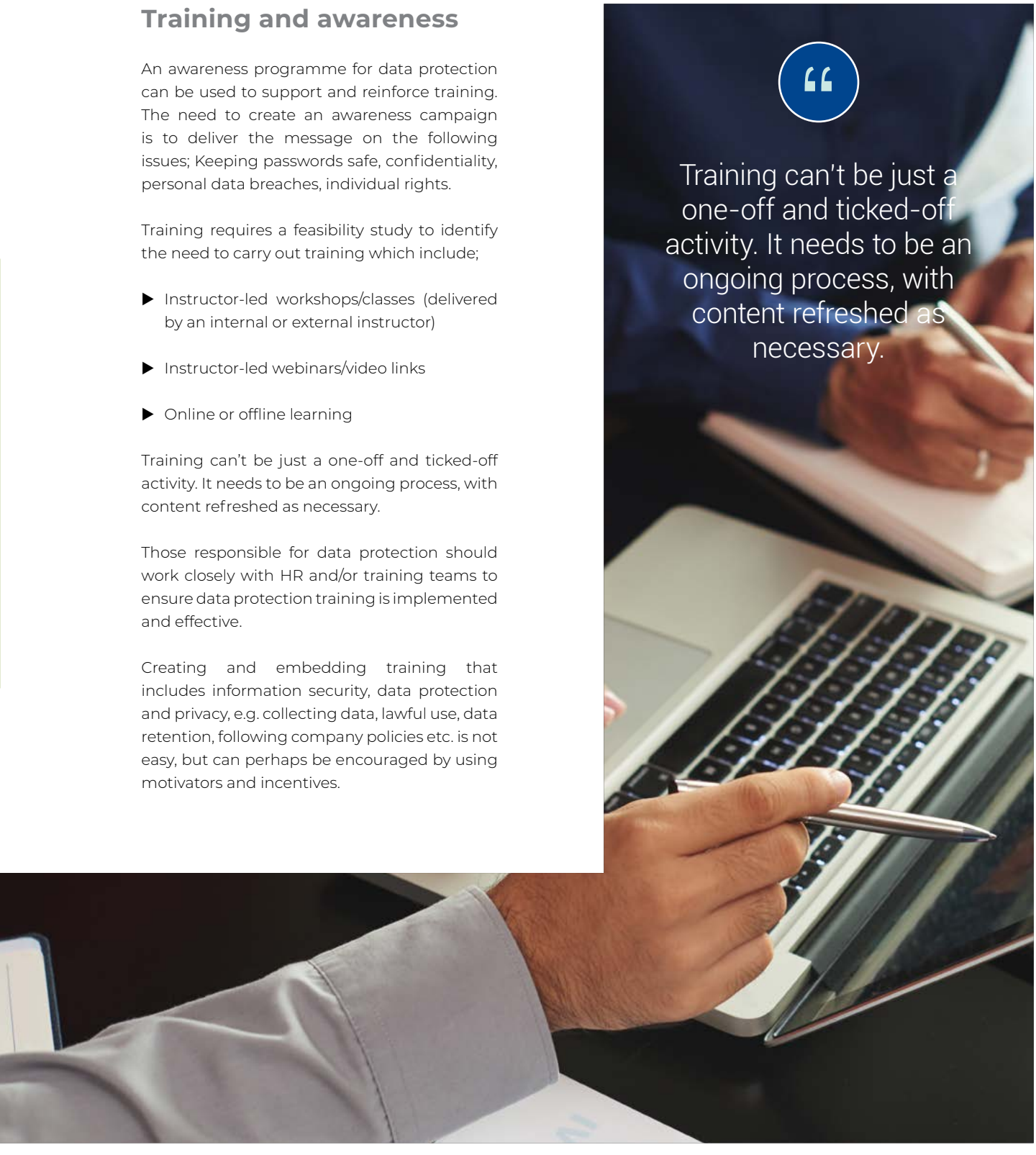
Training requires a feasibility study to identify the need to carry out training which include;

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

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.



UNDERSTANDING CYBER LAW

Uganda's data protection regime has been uncertain for a longtime now. It was not until the recent promulgation of the Data Protection and Privacy Act in 2019 that some of the long unknown duties and obligations of both stakeholders were clearly spelt out.

Simon Peter M. Kinobe

Partner, Ortus Africa Advocates

This year 2020 marks exactly one year since Uganda passed its data protection law, becoming the first East African country to recognize privacy as a fundamental human right, as enshrined in Article 27(2) of the 1995 Uganda Constitution as well as in regional and International laws.

The objective of the Data Protection and Privacy Act, 2019 is to protect the privacy of individuals by regulating the collection and processing of personal information in Uganda and outside Uganda if the information relates to Ugandan citizens; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processers and data controllers; as well as to regulate the use or disclosure of personal information.

The Act gives individuals whose personal information has been requested, collected, collated, processed or stored, powers to exercise control over their personal data including consent to the collection and processing, or to request for the correction and deletion of personal data.

The Act is in line with a number of international conventions including; Article 12 of the Universal Declaration of Human Rights to which Uganda is a signatory. It is also in line with the European Union General Data Protection Regulation (GDPR) which gives control to European Union (EU) citizens and residents over their personal data, and applies to every global organization that may hold or process data on EU citizens and residents.

Across the African continent, Data protection law has been gaining ground over the past 20 years. As of 2019, out of 54 countries, 25 of these countries had passed data protection laws, the latest countries being Uganda, Nigeria and Egypt.

Other countries have introduced data protection bills which are under discussion or waiting to be on the legislative agenda. A regional analysis showed that in 2010, the Economic Community of West African States (ECOWAS) adopted a Supplementary Act on Personal Data Protection followed, a year later, by a Supplementary Act on Cybercrime. The year 2013 saw the Southern African Development Community (SADC) also publish a Model Data Protection Act. While in 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection (the Malabo Convention), a comprehensive document covering electronic transactions, privacy and cybersecurity.

The above mentioned have therefore showed the proactiveness of African nations in embracing the fundamental right of data protection and privacy as an essential tool given the recent lightning transition of services and amenities from analog modes to more digital and cyber ways of handling issues.

Analysis of the Data Protection and Privacy Act

Although one could ably argue that the enactment of this long-awaited Act is a digital milestone in itself given the timing, it would be remiss of us not to assess and evaluate the impact of this Act so far. What has the law actually changed? An article from the Unwanted Witness[i] indicated that unregulated data processing is still on-going and augmenting despite the existence of this relevant Act. So far, the existence of Uganda's data protection law has not in any way resulted in state or non-state actors taking measures to change their policies and practices as per the obligations under the Act.

Businesses will need to be strategic as far as the countries the data collected is stored in order to ensure proposed transfers are not barred by the DPC for lack of proper safeguards.

Incredible amounts of personal data, including sensitive personal data continue to be collected by both government and companies in a manner which disregards the standards set by the data protection law. These include the mandatory collection of National ID data, as well as different government agencies like the Uganda Police Force already unveiling plans to integrate CCTV forensic systems with National ID data and immigration. Furthermore, through the centralized local data Centre for all government agencies and departments was built with the aim of increasing efficiency and effectiveness of government.

i https://privacyinternational.org/news-analysis/3385/one-year-what-has-ugandas-data-protection-law-changed

Different government agencies and departments share information about citizens without their knowledge. This for instance infringes Section 10 of the Data Protection and Privacy Act, 2019 prohibiting the collection and processing of personal data in manner that infringes on the privacy of a data subject.

Similarly, the trend of collecting personal data has increased among companies particularly telecommunication service providers countrywide. The 2018 report by Unwanted Witness pointed to weak policies and terms of reference of telecommunication providers which were compromising costumers' communication privacy and personal data, but even with the data protection law in place, we have not seen companies reviewing their policies and practices to ensure that they meet the standards and obligations provided by the Act. Nonetheless the telecommunication providers continue to collect biometric and bio-data as a requirement for SIM card registration, which has been reported to result into repeated identity theft scandals.

The Absence of regulations by the relevant Ministry[ii] has been the biggest impediment over the past year. This in turn continues to expose millions of citizens to data exploitation. The Data Protection Office, who should be in charge of the overall implementation of the law, providing for administrative, civil or criminal sanctions and penalties among others, has yet to be established.

The prolonged and unnecessary delays in formulating regulations for effective implementation of Uganda's data protection law, is not only a continuous threat to citizens' right to privacy and dignity but compromises the country's trade relations and investors' confidence. Unauthorized processing of personal data can lead to grave violation of human rights; therefore, a data protection law becomes critical in safeguarding fundamental rights and freedom of persons.

Involvement of different stakeholders through an open and transparent process of drafting regulations is key to ensuring an effective implementation of the law.

[ii] *Ministry of Information Technology and National Guidance*

Conclusion

Despite the promulgation of this law, there is still a lot that leaves to be desired in regards to implementation and enforcement.

I am however confident, that going forward and given the immediate need for this law, the government will provide a better platform for its enforcement as the case may be. This is particularly based on recent technological adoptions by government including the recent adoption of various fora such as the Online Case Management System, E-filing services and the Video Teleconferencing by Courts of Law which require strict privacy and confidence of both the litigants and the public at large. This is simply because we have reached an era where digital is not only the way to go but the gate way to a more cost effective and efficient service provision by government.


MASTER
Master
0
35
30
25
20
15

05

The Data Protection Law outlines the conditions for the transfer of personal data outside of Uganda 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).

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

[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*

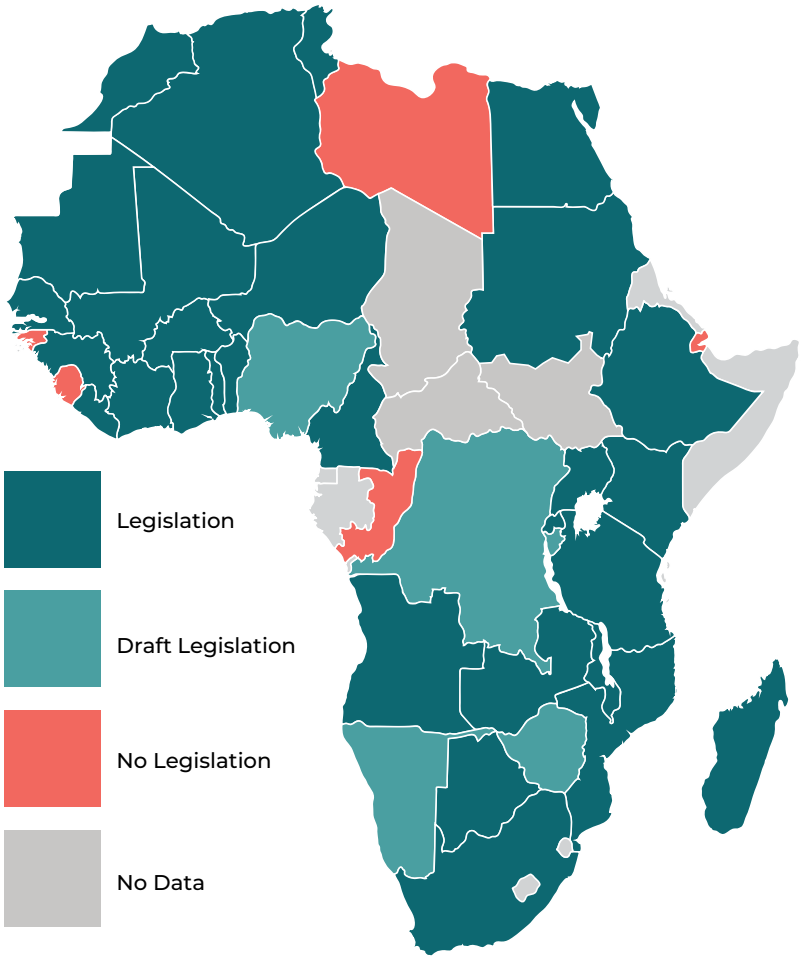
will be crucial in driving economies in the fourth industrial revolution[6]. Therefore, it is important that African countries take up these legislative provisions around data protection because it is possible that Africa can end up as a testing ground due to an increased uptake of smart phones and increasing 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*

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.

FIGURE 24: *Data Protection and Privacy Legislation in Africa (UNCTAD, 2020)*



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


General Data Protection Regulation (GDPR)

IMPLEMENTING CYBERCRIME AND DATA PROTECTION LAWS IN UGANDA

Uganda's legal framework on cybercrime and data protection has been progressive. The first tripartite set of laws for the digital space (Electronic Transactions Act, Electronic Signatures Act and Computer Misuse Act) are now almost a decade old.

Robert Kirunda

Kirunda & Wasige Advocates

These laws are now complimented by the Data Protection and Privacy Act of 2019. The content of these four laws is broad and addresses a number of the contemporary challenges that many countries world over are facing.

A number of the provisions of these laws are yet to be implemented and tested. Some institutional structures envisaged under these laws are yet to be operationalized. In some cases, such as with respect to the Personal Data Protection Office under the Data Protection and Privacy Act, 2019, these institutions may require the creation of new or separate offices, which will be done by furthering the legal regime. In other cases, such as with regard to the Controller under the Electronic Signatures Act, 2011, however, where the law does not specifically require independent offices, it remains unclear why these structures are not yet operational.

The legal framework anticipates the mass adoption of electronic services, but this is not yet the case. E-government as anticipated in the Electronic Transactions Act, 2011, remains largely unimplemented. There are a number of reasons for this. First, institutions in Uganda generally tend to take a siloed approach to change and functionality. Each institution is keen to develop its own systems and protocols, without harnessing areas of mutual operation. Second, technology seems to still be viewed as an option rather than a necessity. It would have been helpful at the enactment of all these laws, to set a time frame within which legacy systems should have been replaced with more agile, tech-based systems of work. Third, there has not been a clear quantification of the adjustment dividend that the country can reap from harnessing technology.

Thus, by not quantifying the opportunity cost of sticking to legacy systems, Ugandan government institutions cannot visualize the difference. As a result, they have traded the benefits of technology for the convenience of traditional systems and ways of operation.

Further, the laws cited above do not operate independent of the broader legal, social, political and administration of justice frameworks. Politics, technical deficiency and inefficiency also remain main hinderances to proper implementation of the digital legal framework. For instance, rather than focus on using the Computer Misuse Act, to deal with the challenges such as child pornography, the law has been used for more politically inclined purposes. All but one of the cases brought under this law so far have been politically motivated. Even then, in doing so, there is a clear lack of the requisite technical capacity.

Politics, technical deficiency and inefficiency also remain main hinderances to proper implementation of the digital legal framework.

The decision in Stella Nyanzi v. Uganda Criminal Appeal 0079 of 2019 introduced questions of digital identity and evidence in the process of judicial consideration. From this decision, it is apparent justice system has to go in appreciating the intersection between judicial process and computer related legislation. The cases of Amongin Jane Francis v. Lucy Akello HCT 01 CV EP 0001 of 2014 and Nakato Mary Annet v. Babirye Veronica Kadogo EP 18 of 2016 both of which dealt with questions of admissibility of digital evidence show that the courts in Uganda are only starting to define the key terms on what amounts to digital evidence. All these court decisions reflect an abiding challenge with regard to technical capacity among stakeholders, and with defining scope and implementation.

Cybercrime and data protection are complex subjects. Uganda's laws may not be on par with those in the most advanced legal systems in the world, but they are far more progressive in their scope than most African jurisdictions. However, implementation remains peripheral if not skewed. This note highlights only a few aspects of the challenges that inhibit the exploitation of the true pith and marrow of these laws.

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

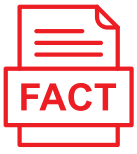
DAWIT INSURANCE AGENCY LIMITED
Your Insurance Department

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.



Cybercrime damages

will cost the world

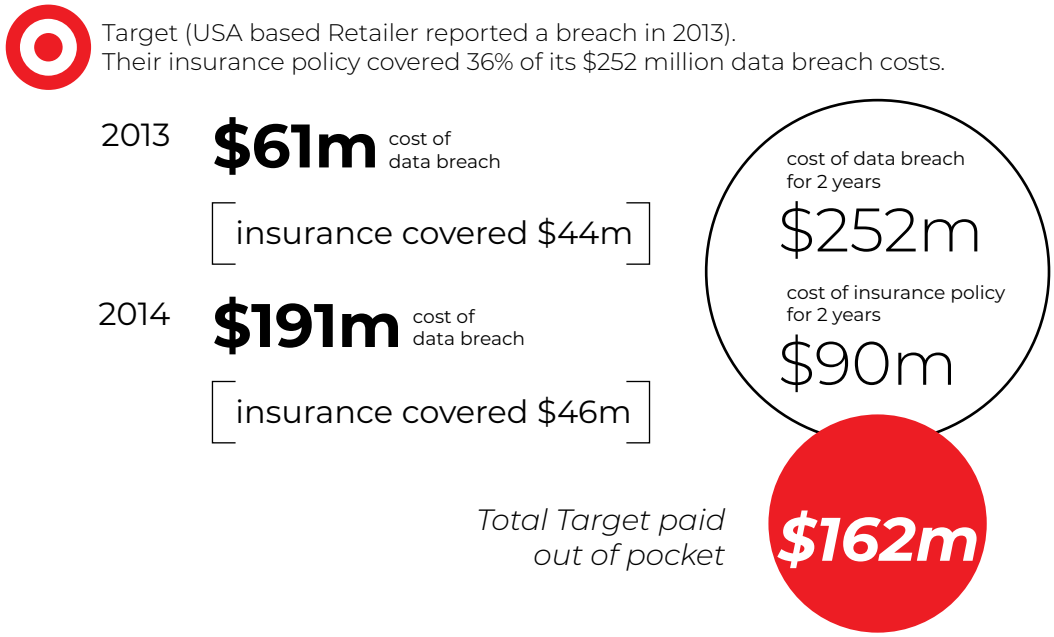
$6 Trillion
annually by 2021

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.*

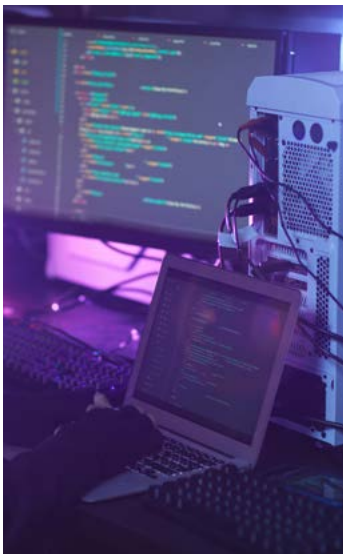


Detailed breakdown of Risk Quantification, Cyber Insurance and Cost of Cybercrime will be provided in the Cost of Cybercrime - Africa Report.


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 V2.384
Computer Usage
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

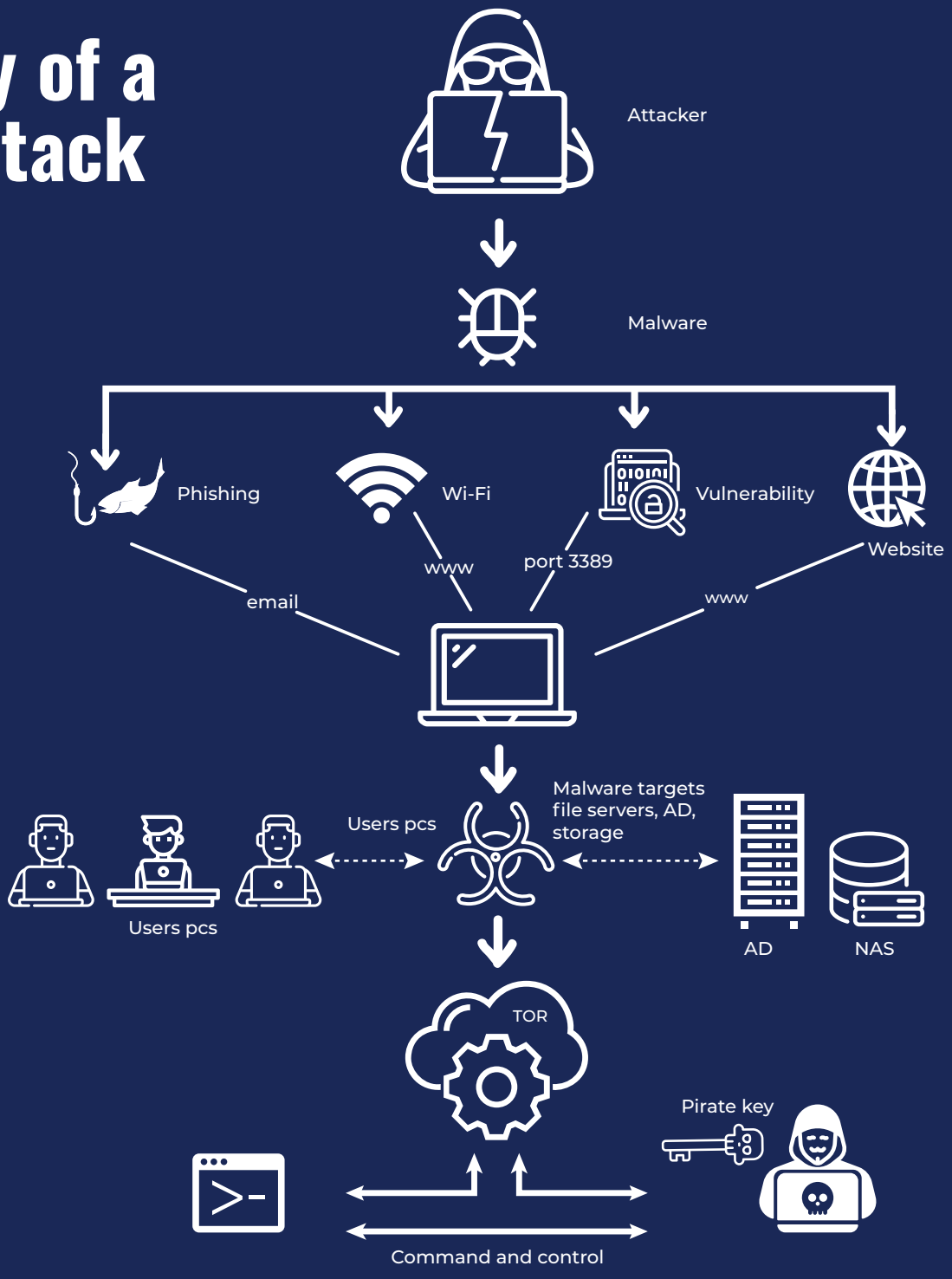
Students from Alliance High school worked on a threat map project. A Threat Map is a visual representation of the source and destination locations around the world for malicious traffic and the exploit used during the interaction. The project lasted 5 weeks.

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.

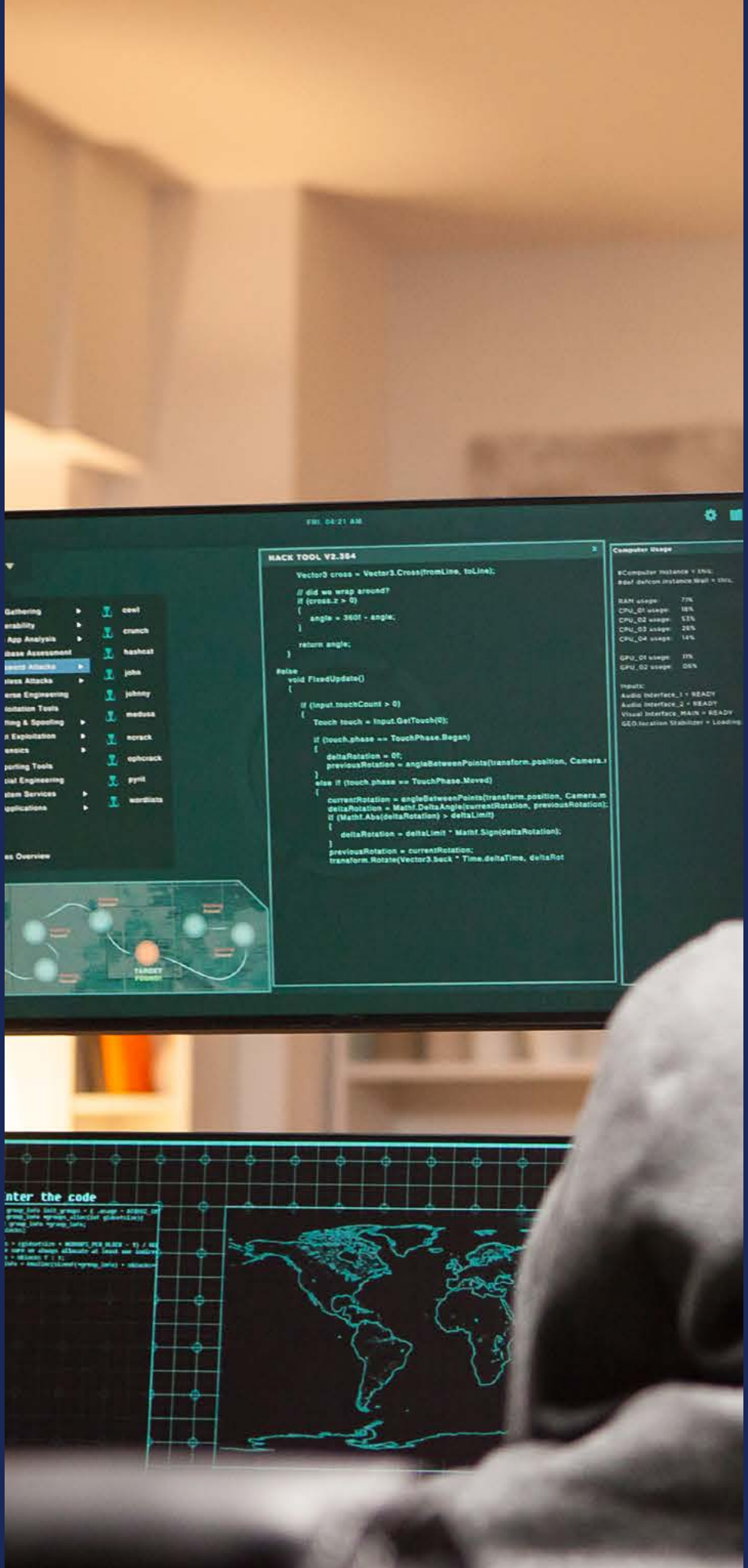
Anatomy of a cyber attack



Initial

Gaining access

Maintaining & encryption



Milima Cyber Academy®

Milima Cyber Academy is a specialized Cybersecurity training academy redefining professional skilling through hands-on training programs.

The Academy is joining hands with industry experts from both the private and government sectors to help close the looming shortage of specialized Cybersecurity professionals in the industry.

https://mca.ac.ug

Uganda's Premier Cybersecurity and Digital Forensics Academy

07

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

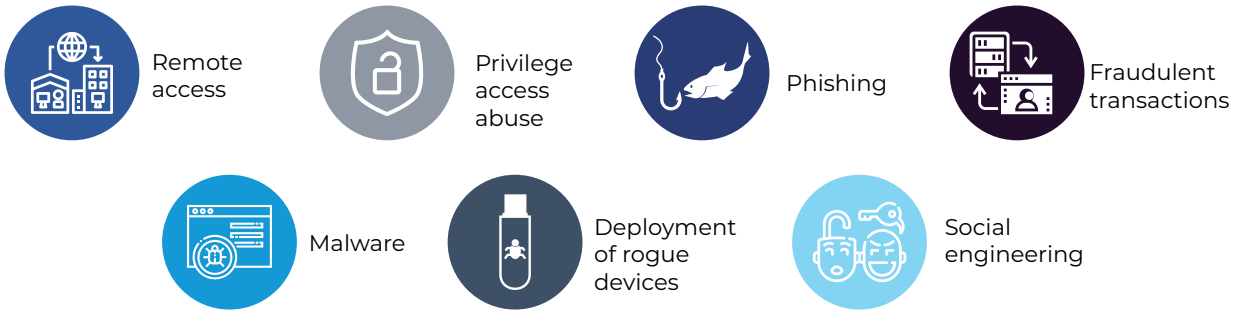
7. 2021 PRIORITIES

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.

2019/2020 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:



As we prepare for 2021 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 2021

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 2021

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 2021

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. APPENDIX

Country: Uganda

Name of Bill/Law/Act: Data Protection and Privacy Act (DPPA).

Year drafted/Enacted: 2019

Status: Enacted to law

Summary:

On the 25th of February 2019, the President of Uganda approved on the Data Protection and Privacy Act (DPPA) that had been in development for several years. This act was set up to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected (Ugandan citizens) and the obligations of data collectors, data processors and data controllers; to regulate the use or disclosure of personal information; and is inspired by the GDPR of the European Union. ("THE DATA PROTECTION AND PRIVACY BILL", 2019)

Qualities of personal Identifiable Information according to the law

According to THE DATA PROTECTION AND PRIVACY ACT, 2019, Personal Identifiable Information is information about a person from which the person can be identified.

Personal Identifiable Information can be recorded in various ways and includes data related to

(a) The nationality, age or marital status of the person;

(b) The educational level, or occupation of the person;

(c) An identification number, symbol or other particulars assigned to a person;

(d) Identity data; or

(e) Other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

How to protect Personal Identifiable Information

There are several ways of protecting Personal Identifiable Information. In Uganda, the following rules have been put in place to protect such data.

(1). Anyone who collects data, processes, holds or uses personal data shall:

(a) be accountable to the data subject for data collected, processed held or used;

(b) Collect and process data fairly and lawfully;

(c) Collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data;

(d) Retain personal data for the period authorized by law or for which the data is required;

(e) Ensure quality of information collected, processed, used or held;

(f) Ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and

(g) Observe security safeguards in respect of the data.

The Authority shall ensure that every data collector, data processor or any other person collecting or processing data complies with the principles of data protection and this Act..

REFERENCES

Call For Life Uganda. Retrieved 8 February 2020, from https://theacademy.co.ug/index.php/call-for-life/

Committee, 1. (2019). 100 Innovators begin pitching their innovations to the Selection Committee – Ministry of ICT & National Guidance. Retrieved 8 February 2020, from https://ict.go.ug/2019/04/16/100-innovators-begin-pitching-their-innovations-to-the-selection-committee/

Cyber Crime Insurance | Gold Star Insurance. Retrieved 6 February 2020, from https://www.goldstarinsurance.com/cyber-crime-insurance/

DFCU bank in crisis as over Shs10b is hacked - Eagle Online. (2019). Retrieved 7 February 2020, from https://eagle.co.ug/2019/07/13/DFCU-bank-in-crisis-as-over-shs10b-is-hacked.html

Draku, F. (2019). Hacker steals sensitive data from govt website. Retrieved 9 February 2020, from https://www.monitor.co.ug/News/National/Hacker-steals-sensitive-data-govt-website/688334-4954262-ylmdad/index.html

Gerberding, K., & Gerberding, K. (2020). Incident Response (1/5): The 5 Benefits of an Incident Response Plan. Retrieved 7 February 2020, from https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan/

Kamoga, J. (2019). Nile breweries website hacked, brewer confirms. Retrieved 6 February 2020, from https://www.theeastafrican.co.ke/news/ea/Nile-breweries-website-hacked/4552908-5363288-2tonw2z/index.html

Reporter, V. (2015). AIG launches cyber insurance. Retrieved 6 February 2020, from https://www.newvision.co.ug/new_vision/news/1332440/aig-launches-cyber-insurance

Reporter, V. (2018). Innovations to improve health outcomes unveiled. Retrieved 5 February 2020, from https://www.newvision.co.ug/new_vision/news/1475336/innovations-improve-health-outcomes-unveiled

S. Wiedmaier, P. Digital Trends and Innovations in Uganda - ICT4D Conference. Retrieved 6 February 2020, from https://www.ict4dconference.org/digital-trends-innovations-uganda/

Ssebwami, J. (2019). Top emerging cyber-threats to worry about in 2019. Retrieved 4 February 2020, from http://www.pmldaily.com/business/tech/2019/01/top-emerging-cyber-threats-to-worry-about-in-2019.html

THE DATA PROTECTION AND PRIVACY BILL. (2019). Retrieved 4 February 2020, from https://ulii.org/system/files/legislation/act/2019/1/THE%20DATA%20PROTECTION%20AND%20PRIVACY%20BILL%20-%20ASSENTED.pdf

https://www.africanlawbusiness.com/news/9498-protecting-uganda-s-data

https://summitcl.com/wp-content/uploads/2017/01/Challenges-of-Implementing-Cyber-laws-in-Uganda.pdf.

Legislation

Data Protection & Privacy Act, 2019

https://www.monitor.co.ug/OpEd/Commentary/Fake-news-Where-does-it-start-who-spreads-it-/689364-5308006-j2u3xj/index.html

Pedrick, C. (2019). Big data for smallholder farmers: The case of MUIIS Uganda. CTA.

Munro, P. (2019). On, off, below and beyond the urban electrical grid the energy bricoleurs of Gulu Town. Urban Geography, 1-20.

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

SERIANU

Enhanced Visibility,
Better Insight

ADDRESS

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

TELEPHONE

General Information:
+254 (0) 20 200 6600

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

EMAIL

info@serianu.com

WEBSITE

https://www.serianu.com