

## Africa Cybersecurity Report

Kenya, 2019/2020

### Local Perspective on Data Protection and Privacy Laws

*Insights from African SMEs*



2019/2020





## **Africa Cybersecurity Report**

Kenya, 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 ..... 6  
Acknowledgements..... 8  
Foreword ..... 11

## **01** 1. Threats Indicators and Emerging Areas..... 13

1.1. Innovations in Kenyan Banking Sector ..... 16

## **02** 2. Cyber Intelligence ..... 21

2.1. Top Malwares ..... 21  
2.2. Increase in Attacks during COVID ..... 28  
2.3. Remote Connection Vulnerabilities in 2020 ..... 28  
2.4. The Risk..... 33  
2.5. How Can Organisations Protect Themselves? ..... 33  
2.6. Everything You Need To Know About ATM Security ..... 36

## **03** 3. Survey Analysis ..... 39

3.1. Data Protection Awareness ..... 39  
3.2. Implementation of Data Protection Best Practices..... 41  
3.3. Cybersecurity Profile..... 44

## **04** 4. Data Protection Law ..... 55

4.1. Principles Of Data Protection..... 56  
4.2. How To Protect Personal Identifiable Information? ..... 58  
4.3. Support System For Data Protection ..... 58

**05** **5. Impact Of Data Protection Laws To Various Departments..... 67**

- 5.1. Finance Department ..... 67
- 5.2. Human Resource Department ..... 68
- 5.3. Use Cases: Customers Management, Marketing and Suppliers ..... 69
- 5.4. Access Control ..... 71
- 5.5. Health Sector ..... 74
- 5.6. Education Sector ..... 75
- 5.7. Review of GDPR ..... 76

**06** **6. Risk Quantification, Cyber Insurance and Cost of Cybercrime..... 81**

- 6.1. What will it cost your organisation NOT TO HAVE Cyber Insurance?..... 82

**07** **7. 2021 Priorities ..... 93**

**8. Appendix..... 98**

- References ..... 102

# EDITOR'S NOTE



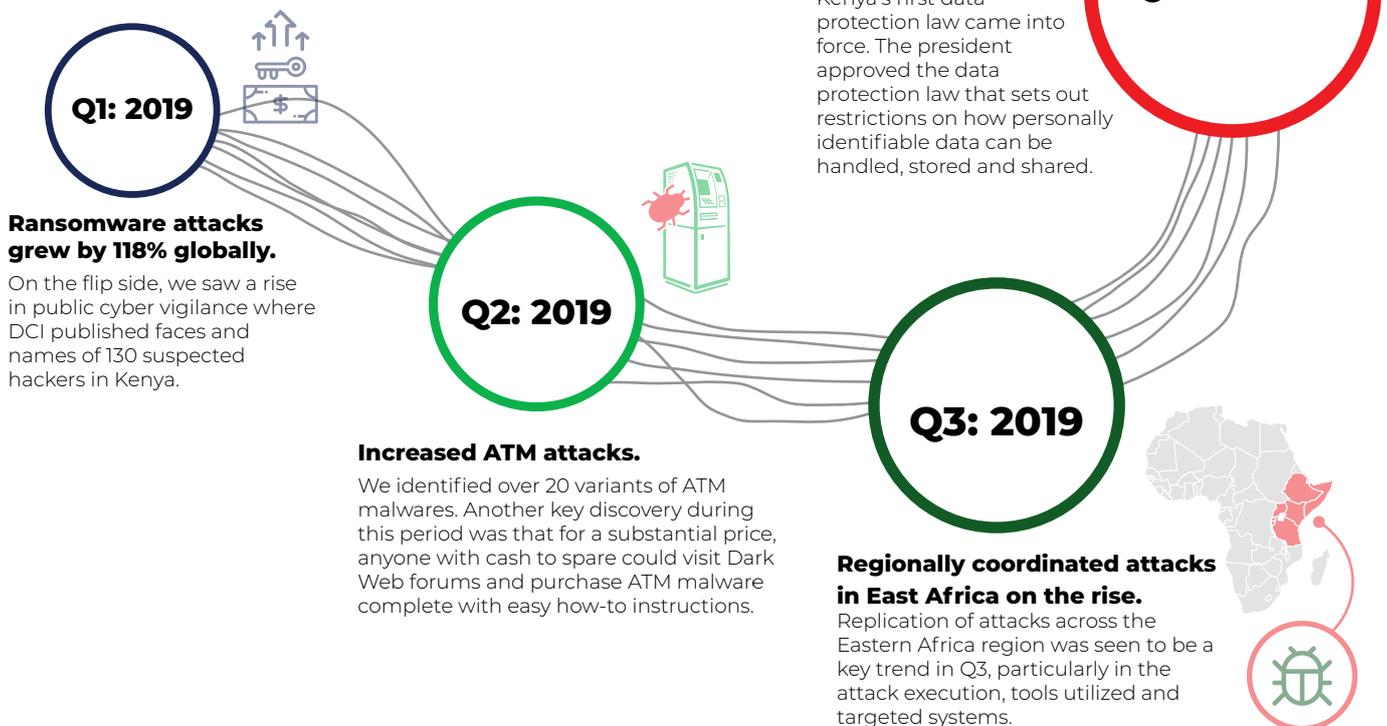
**Brencil Kaimba**

*Editor-in-chief and Cybersecurity Consultant,  
Serianu Limited*

Welcome to the Kenyan 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 and Cyber Intelligence teams in Q1 of 2019 through to Q3 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: 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. On a positive note, we saw yet another display of vigilance where DCI arrested individuals suspected of hacking into NTSA and TIMS databases and issuing fake documents to Kenyans.

### **Unsecured remote connections grew by over 50%.**

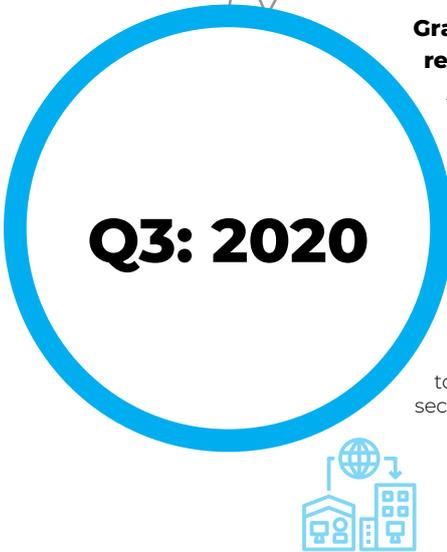
The use of remote access technologies like RDP (Remote Desktop Protocol), VPN (Virtual Private Network) skyrocketed 41% and 33%, respectively globally. Kenya registered 50% increase in unsecured connections.



## Q2: 2020

### **Gradual adoption of remote working.**

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



## Q3: 2020

## 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 - Kenya 2019/2020, the Serianu CyberThreat Intelligence Team received invaluable collaboration and input from key partners as listed below;



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.



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



## The Serianu CyberThreat Intelligence Team

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

### Co-Authors

- 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 University-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

→ **Mercy Wanjau**

Acting Director General  
Communication Authority of Kenya

→ **Wairimu Wahome Mwangi**

IT Security expert  
NCBA Bank, Nairobi, Kenya

→ **Joseph Nyambok**

Head of SOC  
Equity Bank (K) Limited

→ **Douglas Mwaniki**

Network & Security Administrator  
Capital Markets Authority, Kenya

→ **William Maema**

Senior Partner, IKM Kenya

→ **Dr. Paula Musuva**

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

→ **Michael Abuli**

Nairobi Securities Exchange, Kenya

## Africa Cyber Immersion (ACIC) Coordinators and Contributors

→ **Brilliant Kaimba**

ACIC Training Assistant

→ **Walter Ombiro Head of IT**

Alliance Boys High School, Kenya

→ **Geoffrey Manoti Maina**

Network/Information Security Engineer  
Multimedia University of Kenya

→ **Daniel Kihia Tech Educator**

Nova Pioneers Girls, Kenya

## Africa Cyber Immersion (ACIC) Student Contributors

→ **Lorena Munene**

Student, Multimedia University of Kenya

→ **Mercy Chebet**

Student, Multimedia University of Kenya

→ **Kevin Kattam**

Student Alumni, Alliance Boys High School

### Building Data Partnerships



In an effort to enrich the data we are collecting, Serianu continues to build corporate relationships with like-minded institutions. We partnered with The HoneyNet Project™ and other global Cyber intelligence organisations that share our vision to strengthen the continental resilience to cyber threats and attacks. As a result, Serianu has a regular pulse feeds on malicious activity into and across the continent. Through these collaborative efforts and using our Intelligent Analysis Engine, we are able to anticipate, detect and identify new and emerging threats. The analysis engine enables us identify new patterns and trends in the Cyber threat sphere that are unique to Kenya.

Our **new** Serianu CyberThreat Command Centre (SC<sup>3</sup>) 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](mailto: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](mailto:info@serianu.com) | [www.serianu.com](http://www.serianu.com)

Copyright © Serianu Limited, 2020

All rights reserved

# FOREWORD

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.

A handwritten signature in black ink, appearing to read 'William Makatiani', with a horizontal line underneath.

**William Makatiani**  
CEO, Serianu Limited

# 01

*What's new on the scene?*

*Cybersecurity is a Constantly Evolving Puzzle*

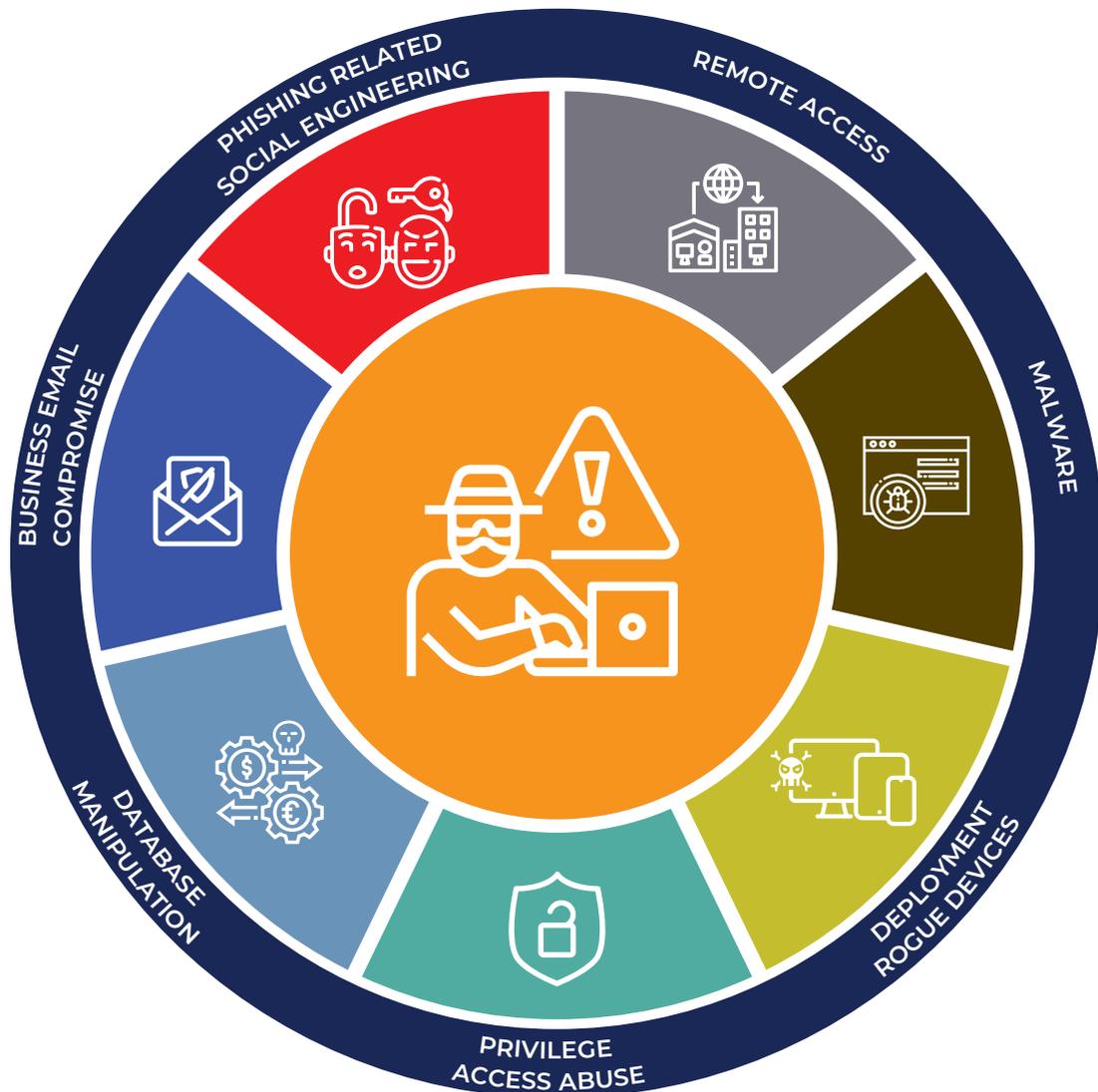
*In this section we highlight the top trends, innovations and their impact to the overall security posture of organisations.*



# 1. THREATS INDICATORS AND EMERGING AREAS

2019/2020 was marked by an increase in attacks across all key sectors from financial services, government, manufacturing and insurance. These attacks were perpetrated through the following vectors:

**FIGURE 1:** Attack vectors across key sectors



### Industry Analysis: Top Attack Areas

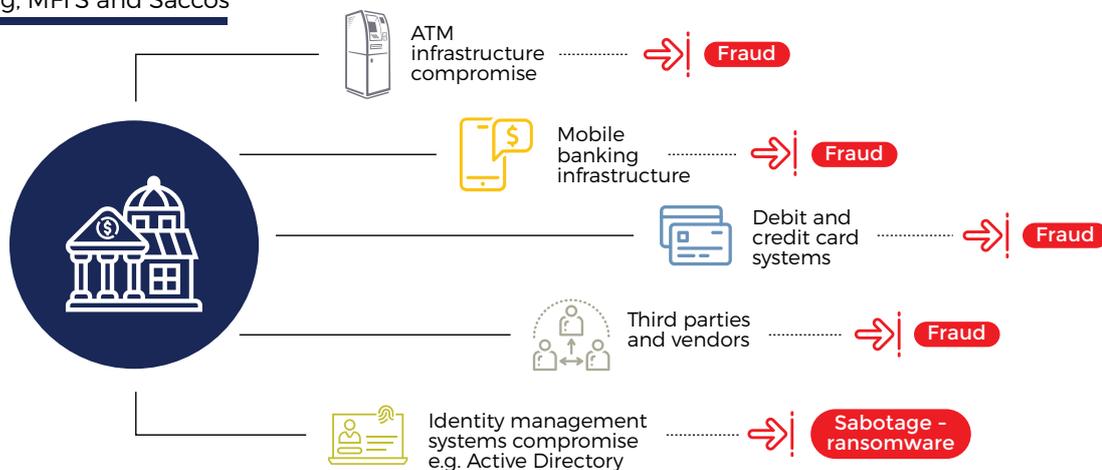
Different sectors have experienced various threats.

The illustration below shows the target areas for the different industries;

FIGURE 2: Target attack areas for different industries.

#### Financial Sector:

Banking, MFI'S and Saccos



#### Others:

Manufacturing/Insurance/Healthcare/Government

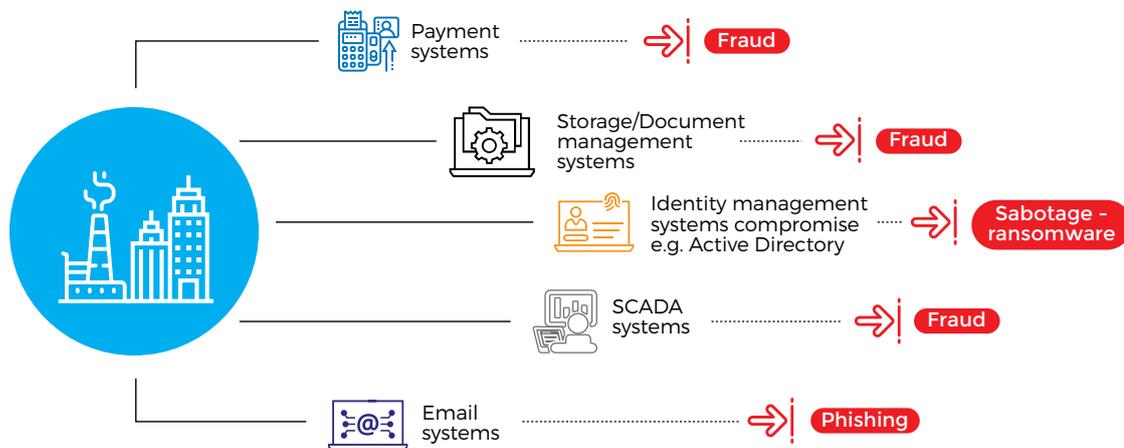


FIGURE 3. Emerging areas.



# Emerging Areas



Organized crime on the rise.

Kenya cyber criminals migrating to neighboring countries.

Cyber criminals moving from financial services to other sectors.

Social media related web scams – virtual accounts.

API integration weaknesses.

ATM attacks.

Third Party attacks.

Cloud perpetrated attacks.

Crypto-mining activity on local system.

Ransomware and end user system hijacking.

## 1.1. INNOVATIONS IN KENYAN BANKING SECTOR

**Kenya's financial industry is the one of the most ever-changing industries. There is continuous adoption of agency banking, mobile banking and internet banking. The industry's continuous growth is very notable given that there is now inbound release of innovative financial products from network operators in the telecommunication industry.**



PDQs machines and cards



ATM bulk note acceptors



Kenya interbank transaction switch



Agency banking



Whatsapp banking



Now as adoption of these and other various innovations continues to be rapidly taken up concerns over quality assurance of application software, begin to come up.

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.



# THE STATE OF CYBERSECURITY IN THE ICT SECTOR

The Communications Authority of Kenya (CA) is mandated with developing a national framework for cybersecurity management in Kenya. Towards this end, the Authority, through the National KE-CIRT/CC, has put various initiatives covering people, processes and technologies that are aimed at enhancing Kenya's national cybersecurity readiness and resilience, as well as to ensure the optimization and sustainability of the gains that Kenya has so far made in ICT.



## Mercy Wanjau

*Acting Director General at Communication Authority of Kenya.*

The Authority through the National KE-CIRT/CC has observed the significant increase in cyber threats both globally, regionally and locally.

Further, the Authority takes cognizance of the dynamic cyber threat environment that is characterized by highly skilled and well-organized cyber crime networks that seek to optimize vulnerabilities for fraudulent purposes. In response to these and in an effort to secure Kenya's cyber space against these growing cyber threats, the Authority has enhanced the people, process and systems capabilities of the National KE-CIRT/CC with objective of boosting Kenya's cyber threats detection, prevention and response capacity.

Noting the importance of skilled front line cybersecurity workforce in building our cyber readiness and resilience, the Authority has earmarked cybersecurity capacity

building as a strategic deliverable. In this regard, the Authority continues to invest in capacity building of cybersecurity professionals working in critical infrastructure through training and up-skilling as a critical component in enhancing Kenya's cyber readiness and resilience.

Further, the Authority hosts various fora such as the Cybersecurity Fireside Chats, County Cyber Clinics, the Annual National Cybersecurity Conference amongst others. These fora bring together the local cybersecurity community to share insights, challenges, network and propose solutions geared towards enhancing cyber readiness and resilience.



The Authority also carries out continuous cyber awareness through various channels, with the objective of empowering the end user to be cyber smart and cyber vigilant. This is in cognizance of the fact that a cyber-aware and cyber-vigilant consumer is our best bet in ensuring Kenya's cyber resilience, especially as we move towards becoming a digitally transformed nation.

The data protection framework in Kenya has gained appreciation with the approval of the Data Protection Policy 2019 by the Cabinet on 18th April 2019 and subsequent enactment of the Data Protection Act No. 24 of 2019 on 8th November 2019. The Data Protection Act has raised awareness on the potential viability both economically and technologically of personal data in enhancing the livelihoods of Kenyans.

As a consequence and in an effort to be more transparent in their processing activities, most data controllers and processors are developing data privacy statements outlining how they are dealing with personal data within their control.

The Government is in the process of establishing the Office of the Data Commissioner. It is expected that once the office has been established, there will be staggered approach in the implementation of the law in order to ensure effective compliance. The Authority envisages a collaborative engagement with the office of the Data Commissioner in ensuring compliance with the Data Protection Law within the ICT sector.



The Authority continues to invest in capacity building of cybersecurity professionals working in critical infrastructure through training and up-skilling as a critical component in enhancing Kenya's cyber readiness and resilience.

# 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

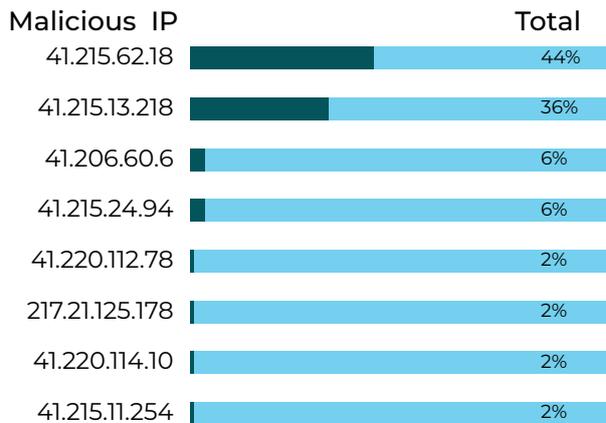
Trojan that can disable Windows Defender. The trojan deploys 17 steps to disable Windows Defender's real-time protection. Trickbot trojan affected nearly 250 million Gmail accounts last time it gained cookie stealing abilities.

3. Ryuk Ransomware

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

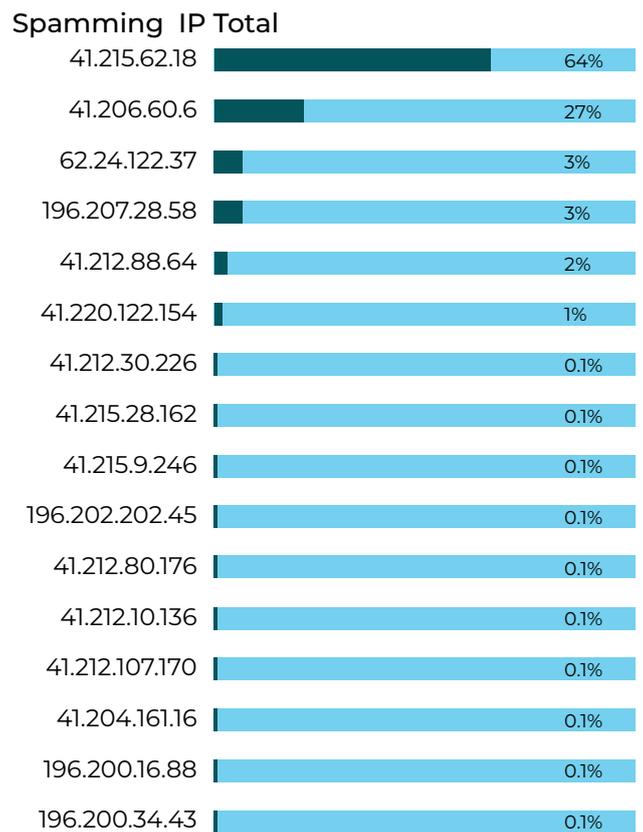
**Top Dictionary Attackers**

**FIGURE 4.** Top Kenyan Dictionary Attackers.



**Top Email Spammers**

**FIGURE 5.** Top Kenyan Email Spammers.



### 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

### 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.Request	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

### 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.Bl!exploit	7.90%	Multiple.Vulnerabilities	29.60%

9	Andromeda	27.40%	HTML/Phish.EMW!tr	8.20%	Script.Injection	25.10%
10	Salicy	12.30%	JS/Agent.OCQ!tr	5.90%	Argument.Injection	24.80%

Source: Fortinet Analysis

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/Wintr!tr			32.4
5	Apache.Struts	29.40%	HTML/ScrInject.OCKK!tr			9.7
6	MS.Windows	28.90%	VBA/Agent.NVE!tr.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!tr.dldr			5.9
11	PhpMoAdmin.moadmin	16.60%	Adware/AdblockPlus			11.9
12	Java.Debug	18.30%	VBA/Agent.D5CD!tr			5
13	Red.Hat	15.60%	VBA/Agent.F36A!tr.dldr			11.3
14	WIFICAM.P2P	13.20%	MSOffice/CVE_2017_11882.C!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.INF!tr			9.1

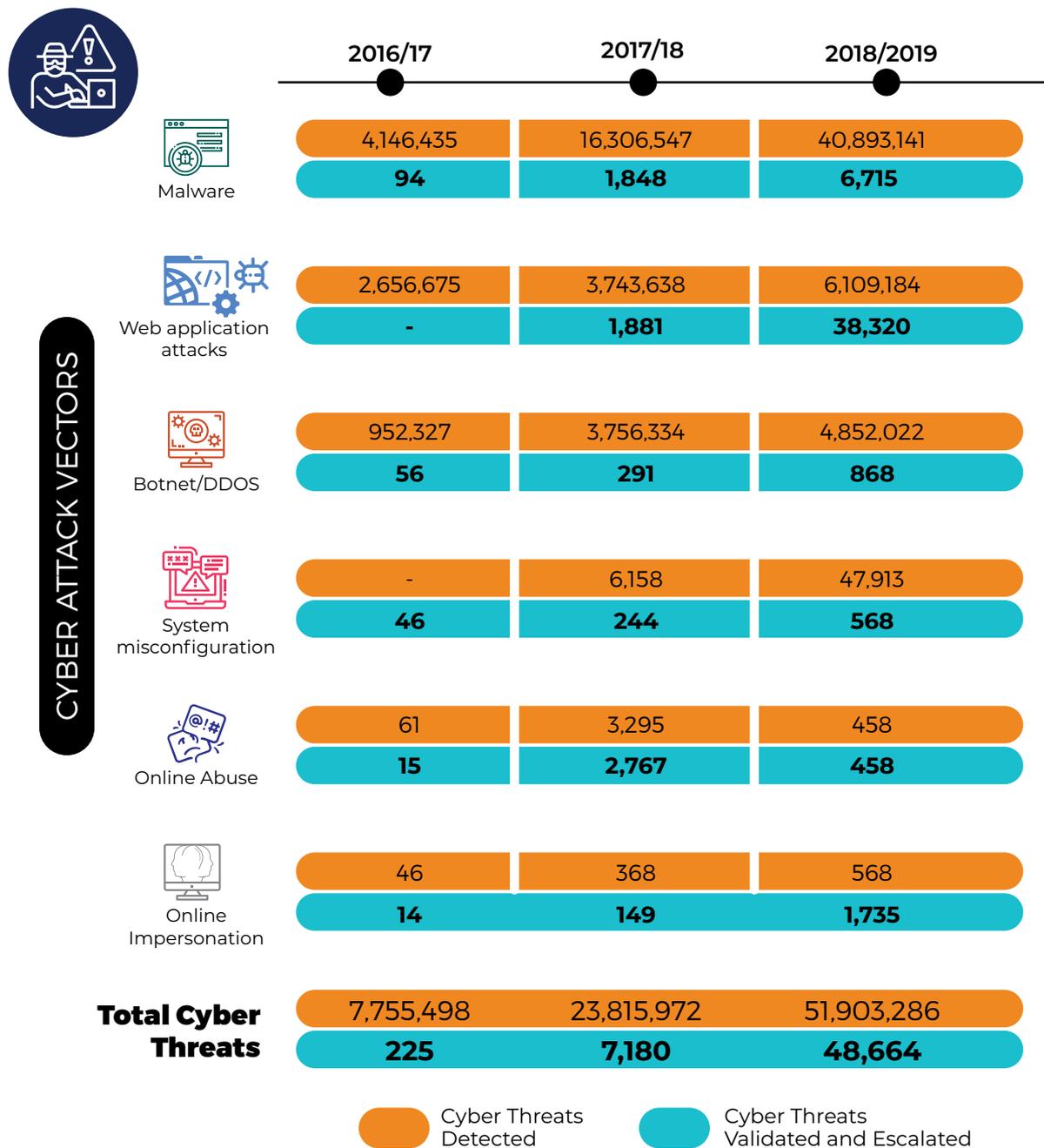
Source: Fortinet Analysis

## Q1-Q3 2020 Identified Kenyan Attacks

	Attack Name	Count
1	Sality.Botnet	319
2	WebRTC.Local.IP.Addresses.Disclosure	125
3	Mirai.Botnet	32
4	Masscan.Scanner	29
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	24
6	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	21
7	Nmap.Script.Scanner	19
8	ZGrab.Scanner	13
9	PHP.Diescan	12
10	ThinkPHP.Controller.Parameter.Remote.Code.Execution	12
11	D-Link.DSL-2750B.CLI.OS.Command.Injection	11
12	PHP.CGI.Argument.Injection	9
13	TCP.Split.Handshake	7
14	MS.Windows.MHTML.XSS.Attempt	6
15	OpenSSL.Heartbleed.Attack	5
16	MikroTik.RouterOS.Arbitrary.File.Read	5
17	Huawei.HG532.Remote.Code.Execution	5
18	Java.Debug.Wire.Protocol.Insecure.Configuration	4
19	Bladabindi.Botnet	4
20	Gh0st.Rat.Botnet	2
21	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	2
22	Avtech.Devices.HTTP.Request.Parsing.Multiple.Vulnerabilities	2
23	Xtreme.RAT.Botnet	1
24	Web.Server.Password.Files.Access	1
25	HTTP.URI.SQL.Injection	1
26	WIFICAM.P2P.GoAhead.Multiple.Remote.Code.Execution	1
27	Dahua.IP.Camera.Unauthorized.File.Access.Information.Disclosure	1
28	DDWRT.HTTP.Daemon.Arbitrary.Command.Execution	1
29	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	1
30	Dasan.GPON.Remote.Code.Execution	1

Source: Local Analysis

Figure 6. Cyber threats detected, validated and escalated.







## 2.2. INCREASE IN ATTACKS DURING COVID



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



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



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



**Exploitation of new teleworking infrastructure.**



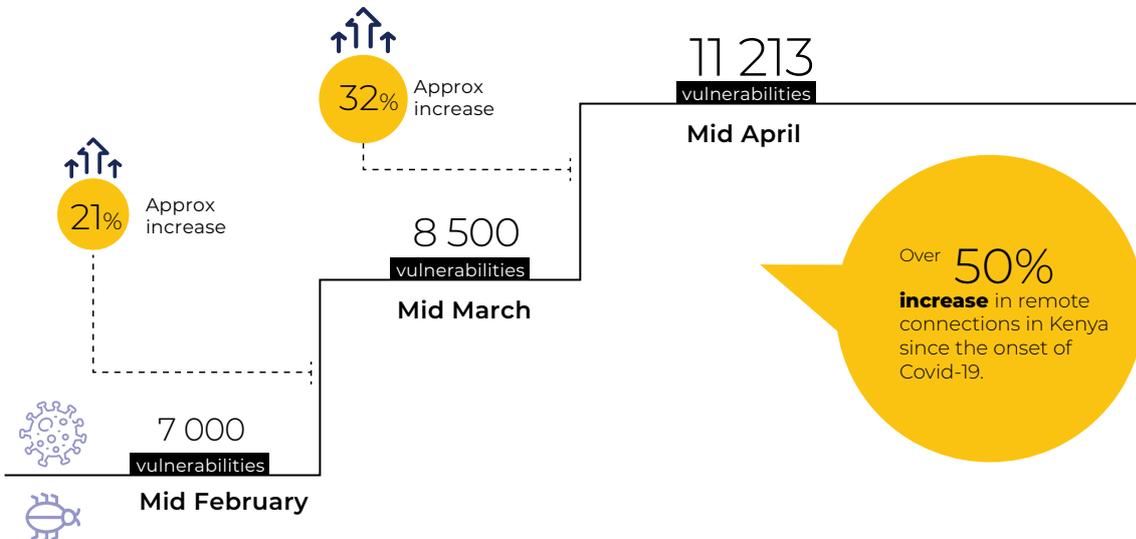
**Malware distribution:** Creative campaigns and new malware variants are on the rise.



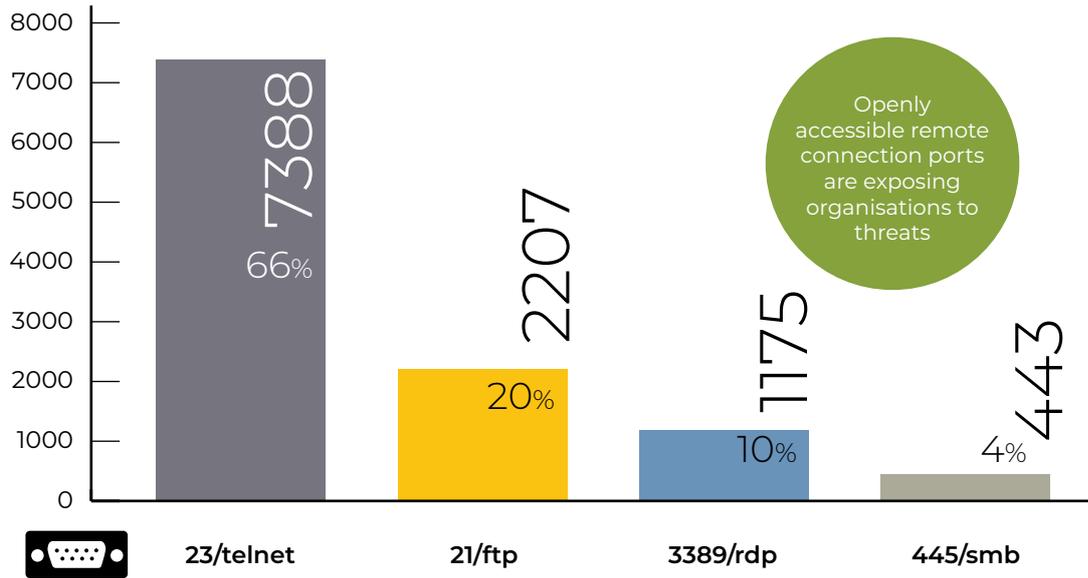
## 2.3. REMOTE CONNECTION VULNERABILITIES IN 2020

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

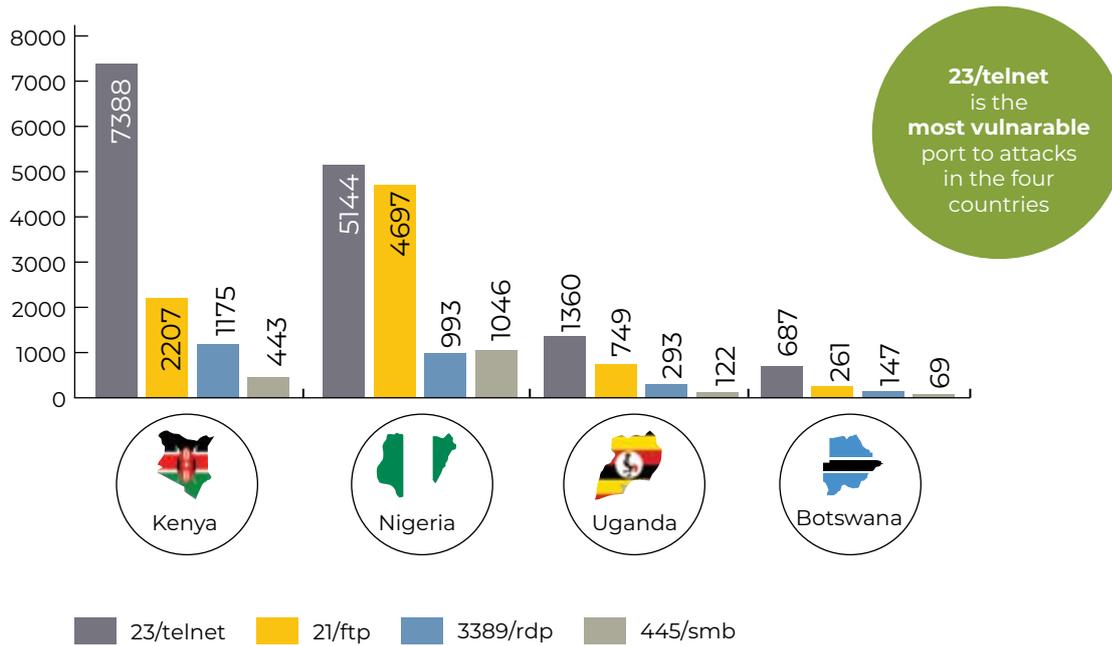
**FIGURE 7.** Remote Connection Vulnerabilities in 2020.



**FIGURE 8.** Publicly Accessible Remote Connection Ports in Kenya.



**FIGURE 9.** Vulnerable Remote Connections.



# EFFECT OF THE DATA PROTECTION LAW ON THE BANKING SECTOR

Kenya's Data Protection Act was adopted in November 2019. The regulation is aimed at providing guidance and best practises for the organisations handling and processing personal data. It also aims to establish structures to support proper data governance within these organisations and at the government level.



## Wairimu Wahome Mwangi

*An IT Security expert at NCBA Bank, Nairobi, Kenya.*

The new data protection law has added to the ever-rising compliance challenges in this era characterized by the evolution of digital banking. Some of its unique compliance challenges include Know Your Customer (KYC) directives, data retention, and incident reporting among others.

To ensure compliance, financial institutions have had to redesign their core applications and how they integrate to each other to ensure personal data is maintained in very few places.

Most banks have also had to redesign the system roles to avoid the risk of exposing too much information to their employees. There is now stronger appreciation of access to personal information as in many institutions, this data has always been lying around, in the drawers and on desks. Now, they have been forced to redefine clean desk and clear screen policies which have in turn shifted in degree of importance from nice to have, to a critical policy.

New job roles have also emerged with many organisations now establishing a data governance and management office tasked with among other tasks harmonizing all data and related policies to ensure they are all well aligned and do not conflict in complying with other regulations. In other cases, some roles have been added the responsibility of looking into data governance.

I anticipate that the industry will get expect more data and privacy related regulations so the players need to be proactive and relook at their architecture principles and adopt privacy principles to ensure their systems are flexible enough to accommodate emerging regulations.

The industry players will have to move away from implementing security and privacy controls for the sake of compliance and make it a convention to design processes, policies and applications that uphold privacy and security at large..

The data protection law gives people control of their information. They have the right to know what data the banks have in custody, what they are using it for and they can disapprove the use of their data. This poses a challenge. How do we ensure people are aware of their rights as far as data act and their role is concerned?

Engaging customers at every interaction point with easy to understand terms and conditions will enlighten customers on their rights. The office of the Data Commissioner needs to promote public awareness to ensure these provisions are well understood by Kenyans.

Data controllers can use their own platforms to raise awareness on the expectations and the processes they have put in place to ensure they are able to comply with the regulations.

## MEETING DATA REGULATIONS STANDARDS

In order to comply with these high standards, organisations need to ensure that they have the right technology, processes and people in place to handle the data governance and compliance roles. Among others, they will also have to regularly evaluate the quality of the data they hold and collect. This can be done at the data entry points and have processes where customers can easily review the data they have.

They may need to put in place initiatives to invite customers to do this more often.

In establishing the data governance office, they have to identify the right roles and responsibilities and that the individuals are properly trained. This includes having a comprehensive knowledge on other complementing regulations and how they affect the data in the organisation.

I also recommend that they frequently analyse and profile their data, preferably using an external party to identify potential gaps or issues that could lead to non-compliance.



The data protection law gives people control of their information. They have the right to know what data the banks have in custody, what they are using it for and they can disapprove the use of their data.

FIGURE 10. Publicly Accessible Remote Connection Ports in Kenya - Industry Analysis.

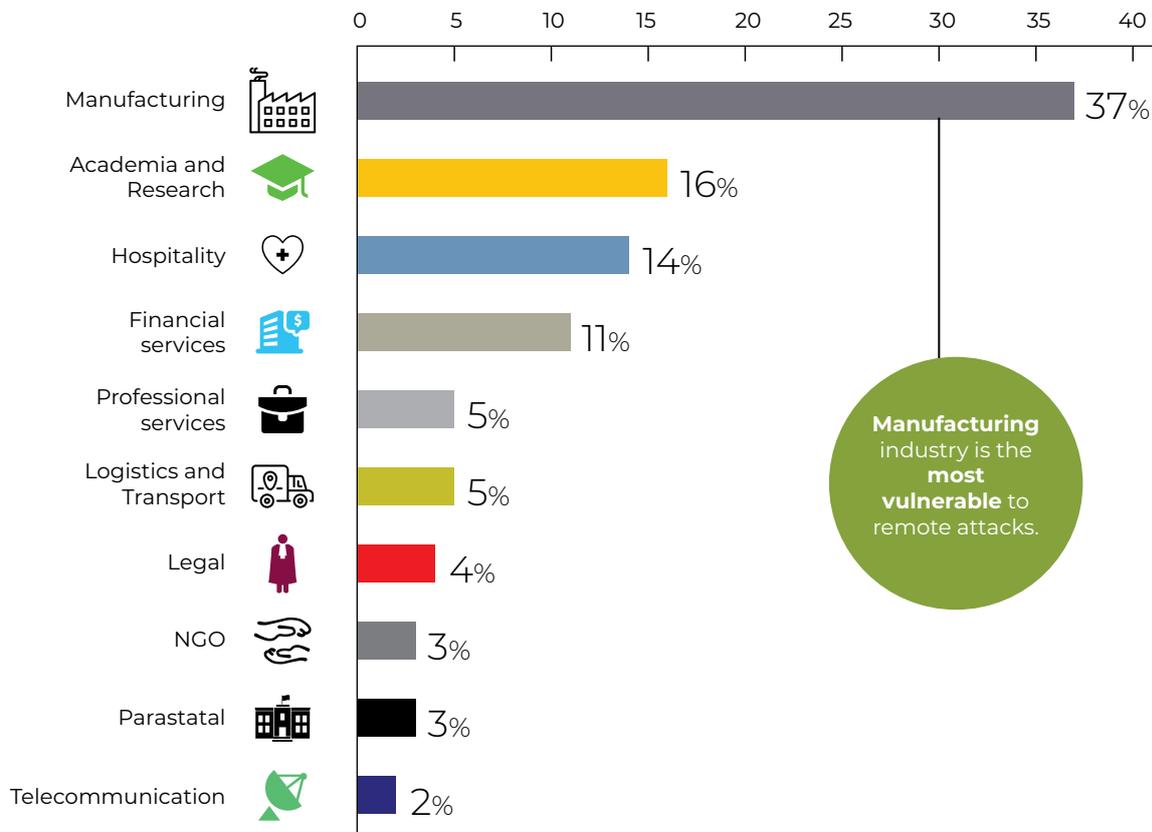
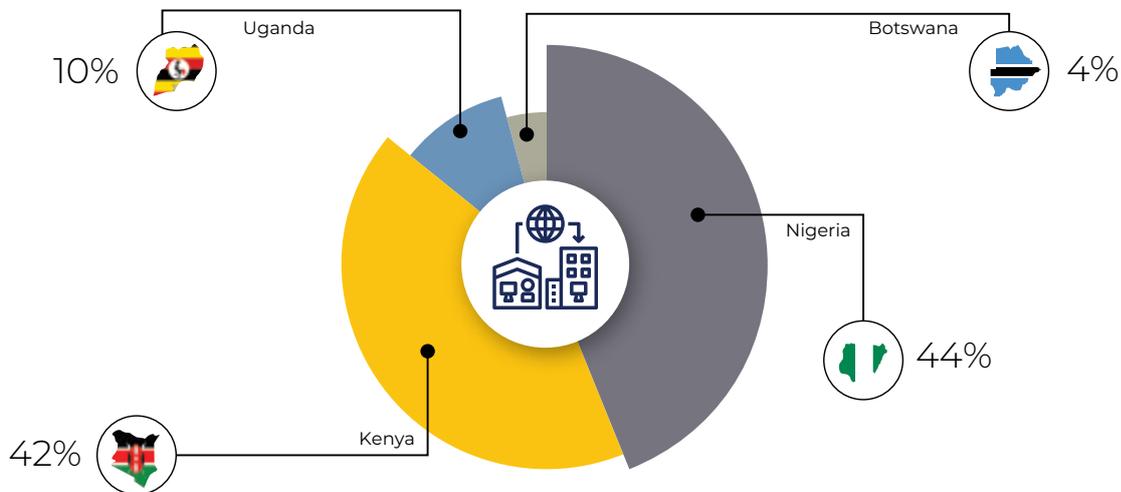


FIGURE 11. Country Analysis - Insecure Remote Connections.



## 2.4. THE RISK

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



## 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.

Education Social

# Interpol Names Juja A 'Global Cyber-Crime Hotspot'

May 15, 2020 Editor Comments Off

The International Criminal Police Organization is raising concern that a little known town in the outskirts of Nairobi, Juja, is quickly becoming a global hub for cybercrime activities.

# NYS and IFMIS among government websites hacked

MONDAY JUNE 03 2019

f in

# Three suspected hackers arrested in Ngara hacking NTSA, TIMS databases

By Tonny Ndungu For Citizen Digital  
Published on: February 21, 2020 13:32 (EAT)

f in

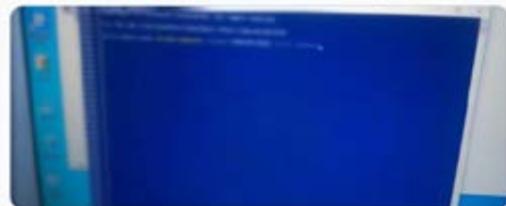


## Email of London-Ba Worth Sh43 Million

897 views - 2 comments



Earlier today, a team of Digital Forensic Experts and Serious Crime Unit detectives working on intelligence raided an office in Ngara within Nairobi County. Upon gaining entry, the team found two suspected hackers actively on @ntsa\_kenya database and TIMS system.



# Barclays loses Sh11m after heist at bank's four teller machines

SUNDAY APRIL 21 2019

f in

Re:SAFTY CORONA VIRUS AWARENESS WHO

World Health Organization



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download



Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulbies.

Regards,

Dr. Stella Chungong  
Specialist wuhan-virus-advisory



# NYS and IFMIS among government websites hacked

MONDAY JUNE 03 2019

f in

Re:SAFTY CORONA VIRUS AWARENESS WHO

World Health Organization



Dear Sir,

Go through the attached document

## Kenyan Fraudsters Hack into Email of London-Based Company, Order Bulldozers Worth Sh43 Million

By John Wanjohi - Sun, 09/08/2019 @ 07:30am - 897 views - 2 comments



Education Social

# Interpol Names Juja A 'Global Cyber-Crime Hotspot'

May 15, 2020 Editor Comments Off

The International Criminal Police Organization is raising concern that a little known town in



DIRECTORATE OF CRIMINAL INVESTIGATIONS



# WANTED

## PERSONS IN CONNECTION WITH ELECTRONIC FRAUD BY HACKING INTO BANK SYSTEMS

The suspects listed here are wanted by the Directorate of Criminal Investigation pursuant to a warrant of arrest issued by CM's Court Kiambu on 24th January 2019 vide case reference number CR 121/17/2019, CF 100/2019.



LINCOLN WARIWA NGONYO  
ID No. 20580806



PATRICK KARIUKI NDIRITU  
ID No. 24077559



LILIAN WANJIRU MAKIPONYA  
ID No. 30382436



BRYAN OKOMBO ONJULA  
ID No. 29739550



KEVIN GATTITU  
ID No. 28617130



PATRICK KUPALLA TUNE  
ID No. 22060152



JOHN GITONGA KAHARA  
ID No. 11447545



RICHARD KASELE MUTINDA  
ID No. 2608423



PETER GITHURI NGORA  
ID No. 27633708



HUMPHREY OMOLO OLLILO  
ID No. 29684182



JOHN MUNAZA SEKA  
ID No. 13635362



PETER WARERU KARANJA  
ID No. 29440733



PATRICK WAFULA SHAKABA  
ID No. 27352970



AHMED MOHAMED HASSAN  
ID No. 29775821



ABDIKARIM YUSSUF ABDI  
ID No. 34253427



PAUL NJOROGE NANGA  
ID No. 4277477



BENSON MUTUA ISEU  
ID No. 23912808



LABAN MAINA NJUGUNA  
ID No. 22843511



DENNIS MAINA KIULOBA  
ID No. 26047011



SERAH WIKTIRI GATHURA  
ID No. 22498325

Any person with information to contact DCI Hqrs-  
ECCU section, the nearest police station, call or sms  
0772 627435, 020 334 3412, 020 286 1097 or email Us  
on [eccu-cyber@outlook.com](mailto:eccu-cyber@outlook.com)

## 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.

Malware	Description
<i>WinPot ATM malware</i>	Forces ATM machines to empty their cassettes of all funds.
<i>GreenDispenser Malware</i>	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.
<i>Ploutus</i>	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.
<i>Anunak/Carbanak</i>	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.
<i>Cutlet Maker</i>	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.
<i>SUCEFUL</i>	Designed to capture bank cards in the infected ATM's card slot, read the card's magnetic strip and/or chip data, and disable ATM sensors to prevent immediate detection.



# PRACTITIONER'S VIEW ON DATA PROTECTION

The new data protection and policy states that every organisation should conduct a detailed audit of their privacy and data protection practices.

## Joseph Nyambok

*Head of SOC, Equity Bank (K) Limited, Nairobi, Kenya*



For a start and at minimum, the main focus of the audit should be on reviewing the comprehensiveness of the compliance risk assessment with the data protection law and whether the organisation has formulated and implemented policies and procedures to regulate the processing of personal data. It should also cover the extent to which processing is being carried out in accordance with such policies and procedures. The audit outcome should clearly answer one key question: Is the organisation compliant with the law?

I however expect that majority of organisations will find it challenging to find the financial and technical resources necessary to conduct such audits internally. The current slowdown in business activities due to the ongoing pandemic has shifted priorities and budgetary allocations. Many organisations may therefore not afford to partner with competent independent firms with required know how in conducting data protection audits.

If organisations are forced by prevailing business conditions to look inward for such audits, the results may not be satisfactory leading to non-compliance with the law.

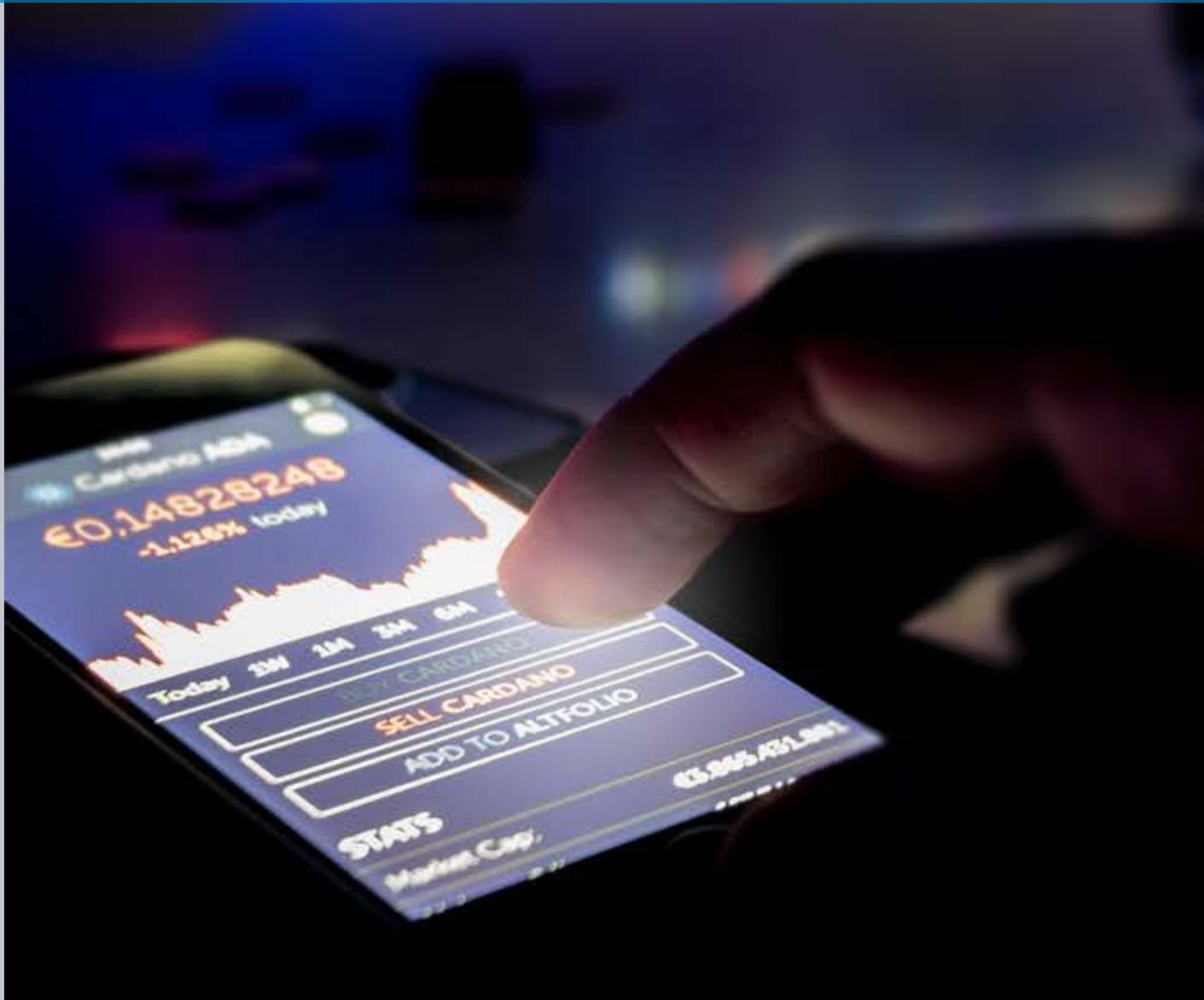
Audit outcome should clearly answer one key question: Is the organisation compliant with the law?



# 03

*The 2019 Cybersecurity Survey provides insight into what Kenyan organisations are doing to protect their information and assets, in light of increasing cyber-attacks and compromises impacting them.*

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

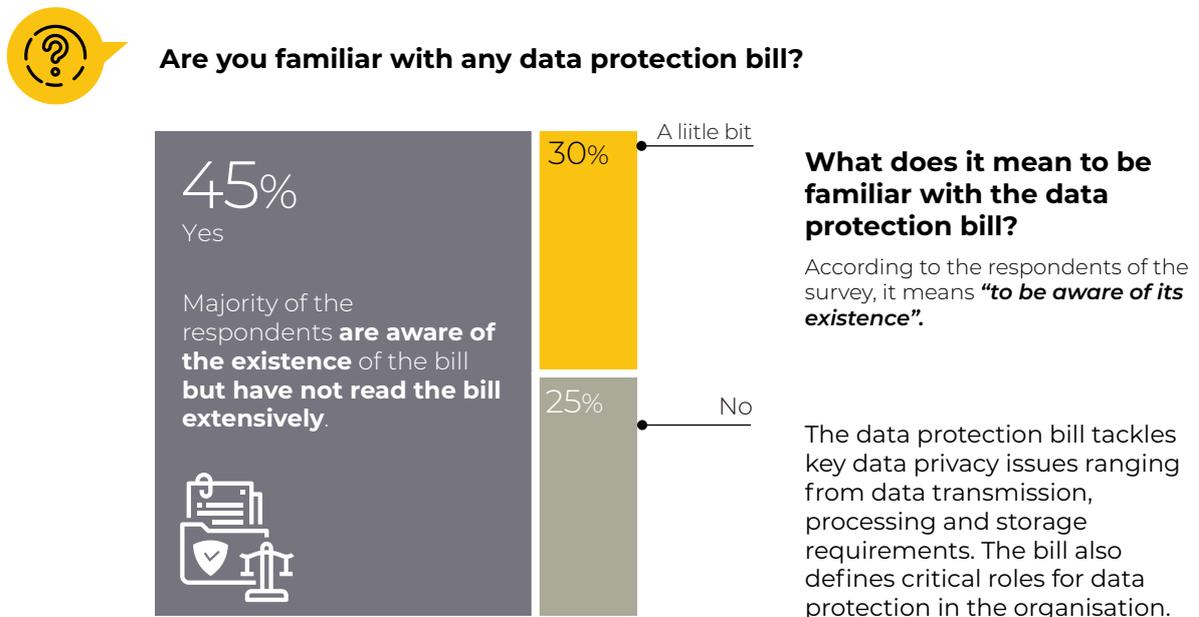


# 3. SURVEY ANALYSIS

## 3.1. DATA PROTECTION AWARENESS

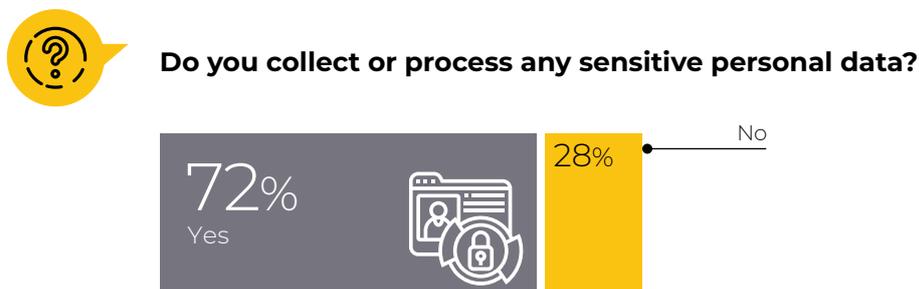
### 3.1.1. Familiarity with Data Protection Bill

FIGURE 7. Familiarity with the data protection bill.



### 3.1.2. Processing of Personal Data

FIGURE 8. Processing of any sensitive personal data.



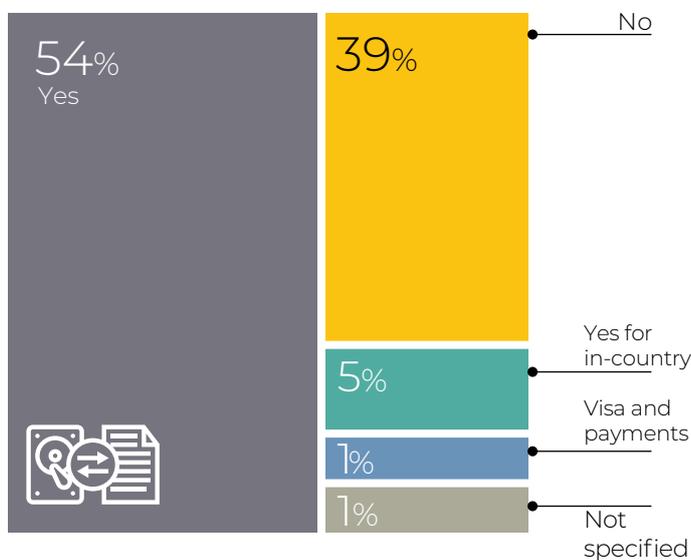
Information relating to natural persons who are identifiable, directly or indirectly from the information in question; or in combination with other information.

### 3.1.3. Transfer of Personal Data

FIGURE 9. Transfer of personal data with third parties.



#### Do you transfer personal data with third parties?



**Current State**

Over 70% of respondents process PII within their organisation.

Over 60% of respondents process PII through third party systems both within and outside the country.

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 Kenya 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 Kenya.

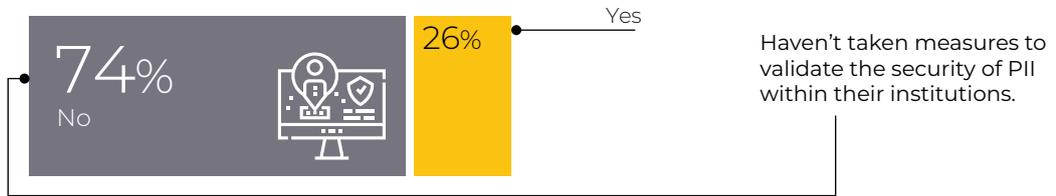
## 3.2. IMPLEMENTATION OF DATA PROTECTION BEST PRACTICES

FIGURE 10. Implementation of processes in an organisation.

### Protection of personal data



**Have you implemented processes to ensure that your organization can protect the privacy/security of personal data?**



**Recommendation:**

Conduct Data Protection Risk Assessment

**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:

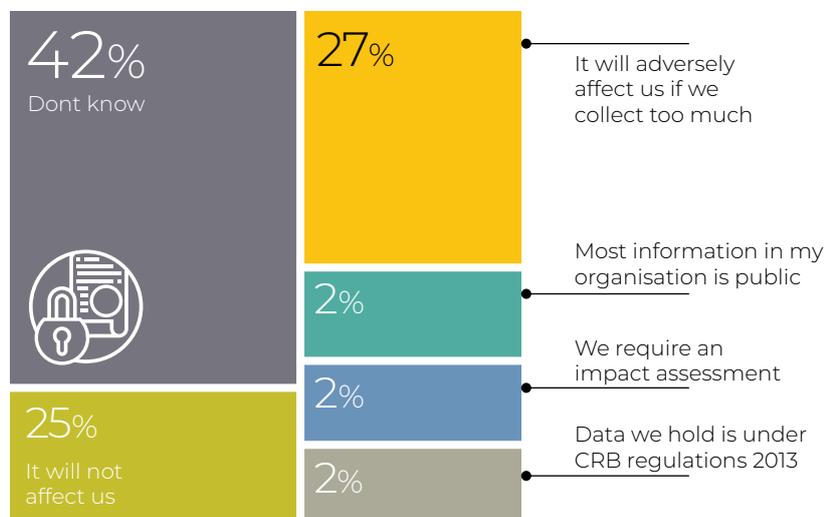
- ▶ Loss, damage or unauthorized destruction
- ▶ Unlawful access or processing

FIGURE 11. Effect of of data protection law Implementation.

### Impact of Data Protection Law



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



**Recommendation:**

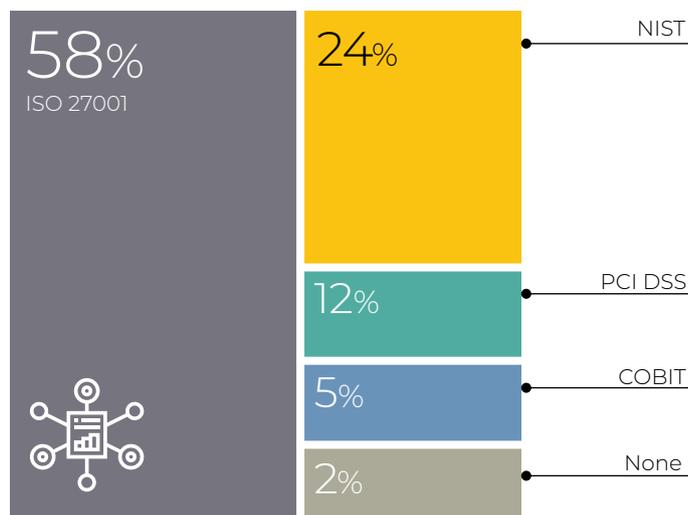
Conduct an Impact Assessment to determine the extent of compliance/non-compliance. The law provides for fines of up to 5 million in cases of non-compliance.

FIGURE 12. Cyber Risk management frameworks use in organisations.

### Framework for data protection



**What cyber risk management framework does your organization 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.

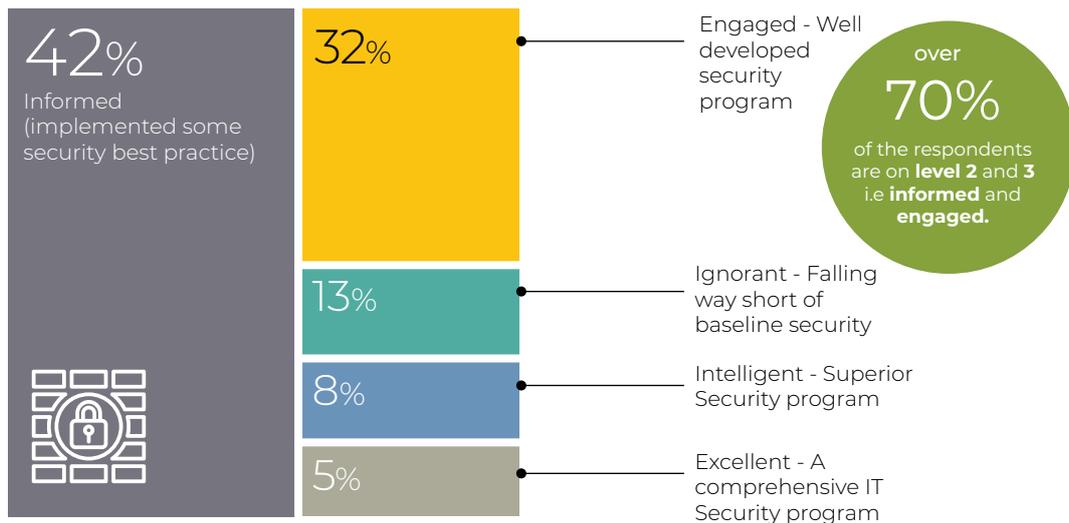
### 3.3. CYBERSECURITY PROFILE

FIGURE 13. Organisation's maturity rank.

#### Benchmarking Cybersecurity Maturity



**Where does your organisation's maturity rank compared with other organisations?**



**FIGURE 14.** Organisation's cybersecurity profiles.

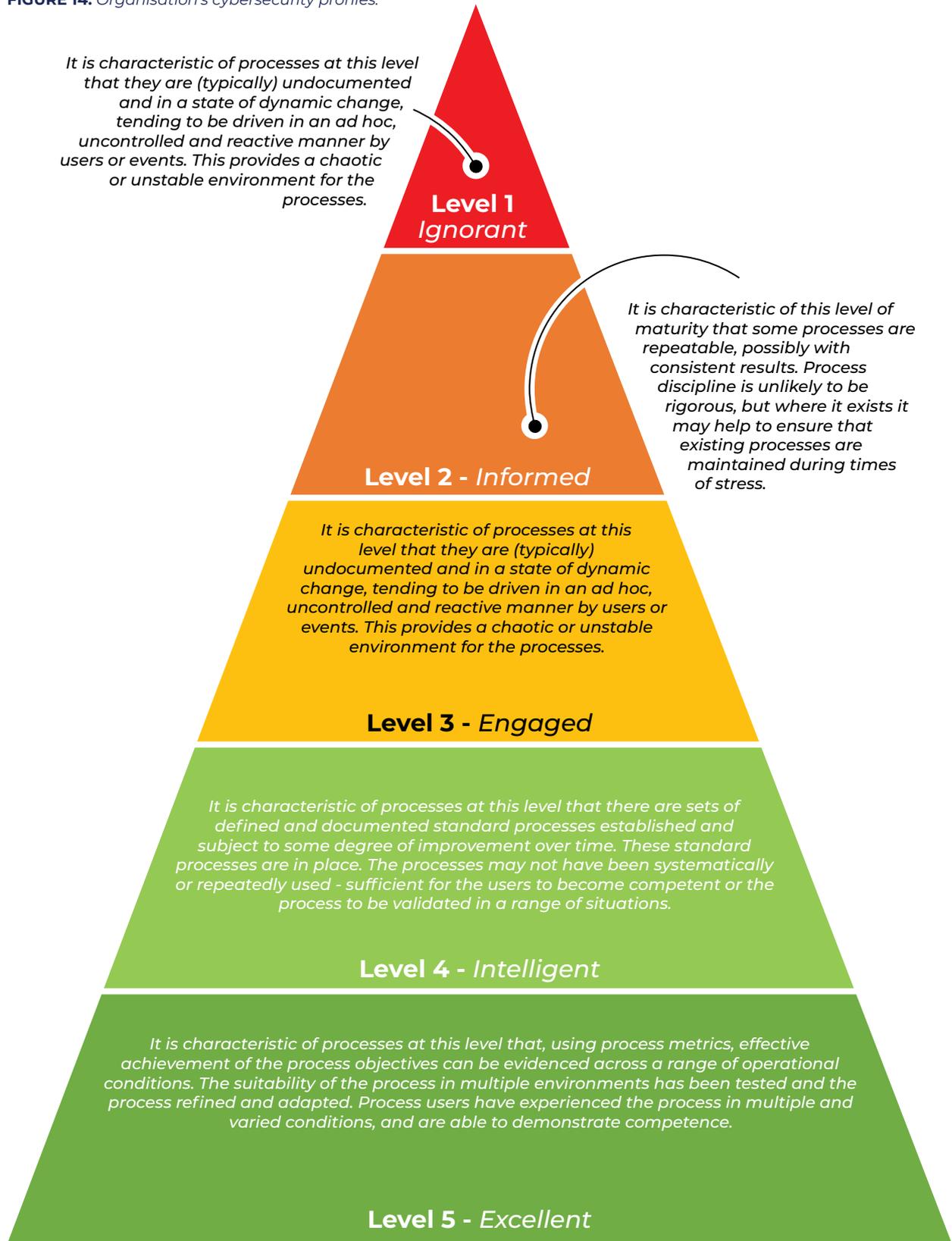
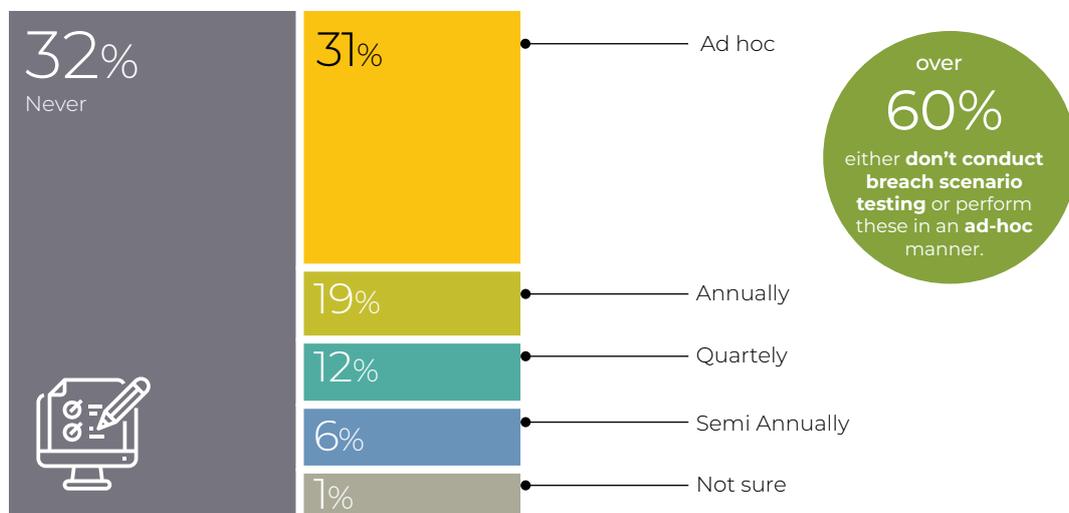


FIGURE 15. Organisation's frequency of performing cyber breach scenario testing.

**Breach Scenario testing**



**How frequently does your organization 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:**

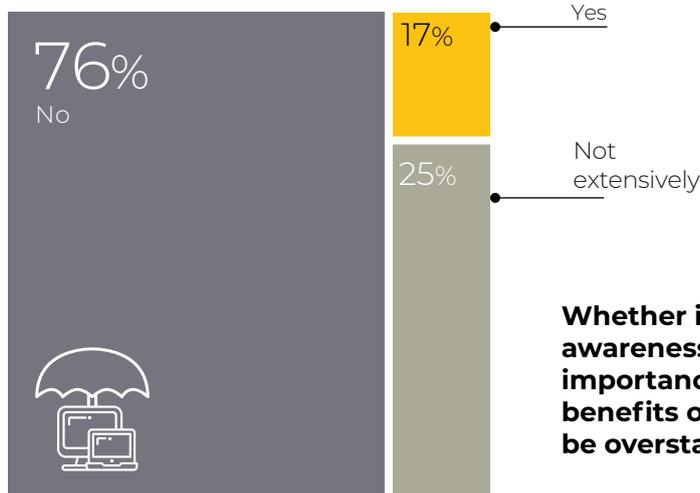
Testing your Incident Response plan through breach scenario testing provides employees the opportunity to understand how to respond in the event of an incident. Participating in table top exercises to simulate a real-world scenario is the best way to prepare.

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

Cyber Insurance



Does your organization 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.

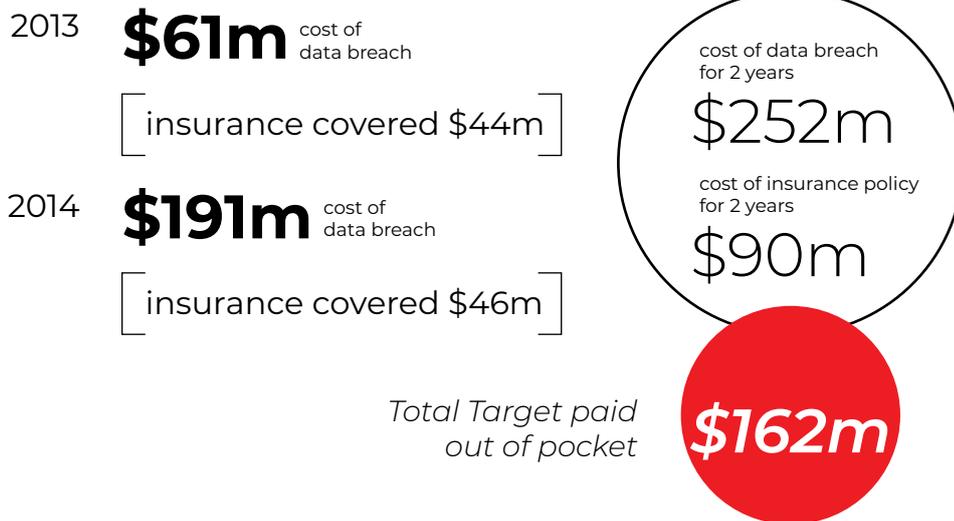
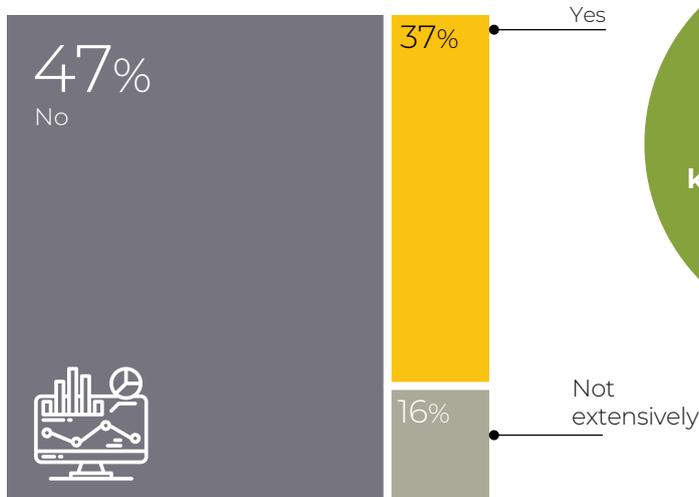


FIGURE 15. Reports and metrics to measure cybersecurity posture.

### 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 15. 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?

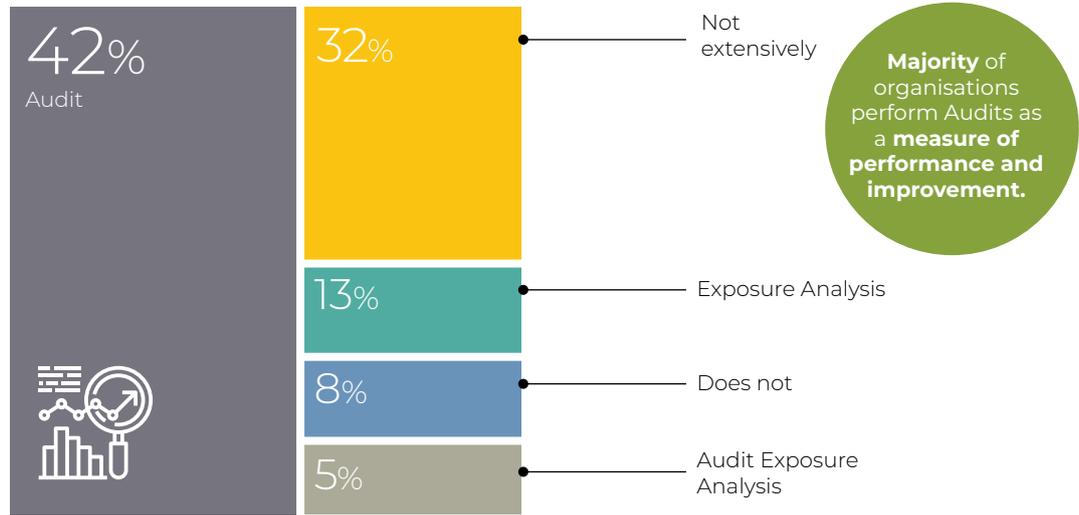


FIGURE 16. Use of security testing techniques.

Security Testing Techniques



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

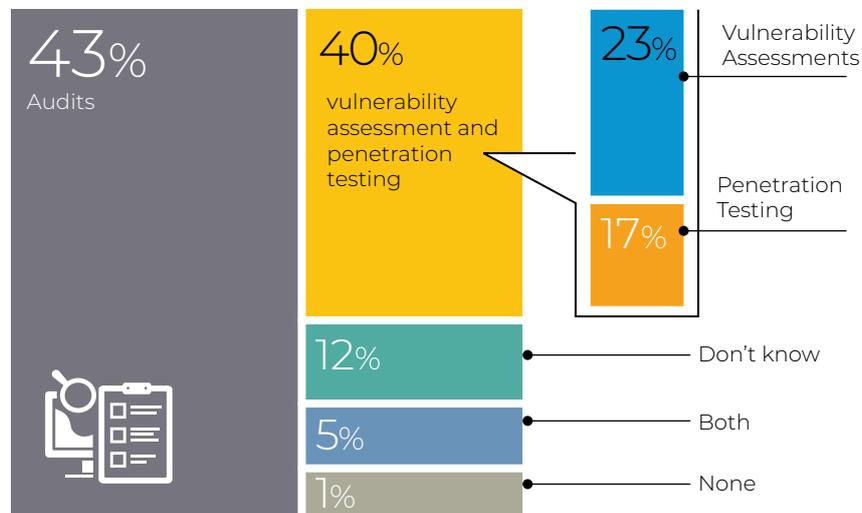
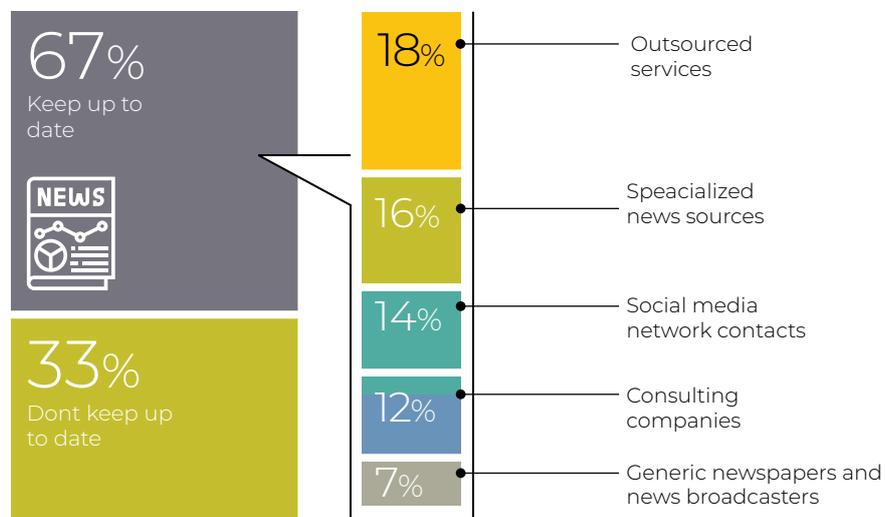


FIGURE 17. Keeping up with cybersecurity news/update.

**Cybersecurity News**



**How do you keep up to date with cybersecurity news/updates?**



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 18. Staff training on cybersecurity risks.

### Cybersecurity Training



How often are staff trained on cybersecurity risks?

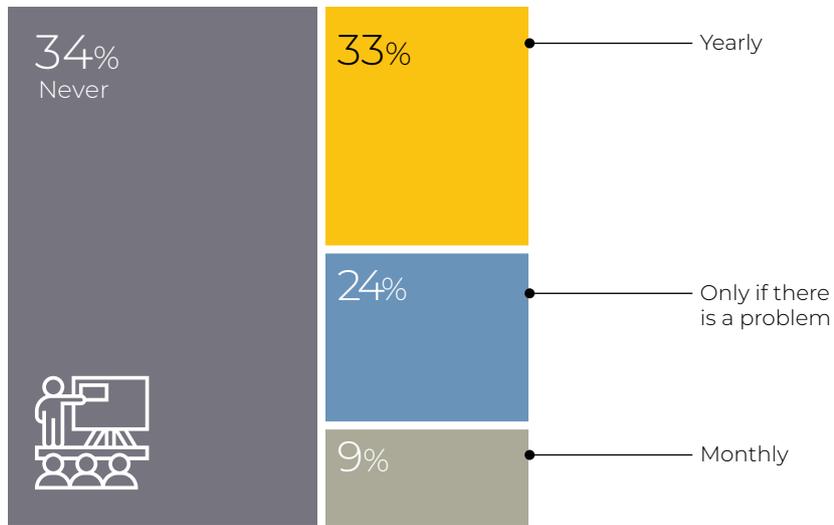
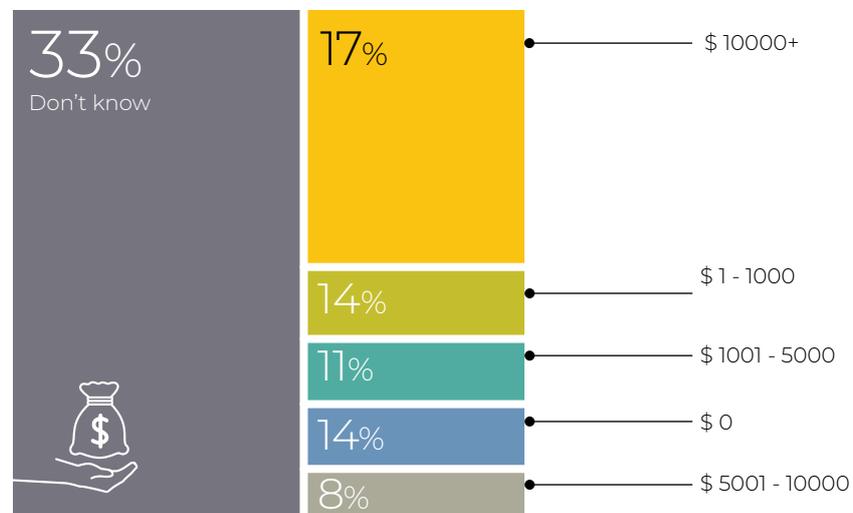


FIGURE 19. Staff training on cybersecurity risks.

### Cybersecurity Expenditure



Approximately how much does your organization spend annually on cyber security?



# HOW CAN ORGANISATIONS STAY AHEAD OF CYBERCRIMES?

Organisations and businesses of all types and sizes all over the world face the risks of cybersecurity breaches. In fact, security analysts emphasize that it is not a question of, but when these threats will be manifested.



---

## Douglas Mwaniki

*Network & Security Administrator, Capital Markets Authority, Nairobi, Kenya.*

---

The emergence of Web 2.0 and the Internet of Things (IoT) have increased these threats in magnitude and severity.

With an understanding of the potency, disruption and damage that cybersecurity threats can cause, that they are automated and indiscriminate, exploiting known or unknown vulnerabilities, organisations need to employ a multi-layered approach to protect critical services, applications and assets and thus stay ahead of the actors.

We have seen that some of the more common threats include, but are not limited to; ransomware, phishing, malware, social engineering, Denial of Service (DoS) and Distributed Denial of Service (DDoS). However, there are newer threats that have recently emerged, such as Cloud Vulnerability, (as a result of rapid adoption and leveraging of Cloud computing technologies by many organisations), Machine Learning poisoning, Artificial

Intelligence (AI) enhanced threats and Smart Contract hacking among others.

For organisations in Africa to stay ahead of these ever-evolving cybercrimes, there is a fundamental need to employ a structured security strategy that is championed from the top management and cascaded down to every level. A successful and solid cybersecurity strategy is only as strong as the weakest link. Organisations need to be able to identify their most critical information assets and data, establish relevant measures and mechanisms to protect them, have the ability to detect threats the moment they occur, respond to the threats by either delaying, slowing or stopping the attacks altogether, and finally recover from an attack.



In addition to the structured approach above, all communications should be protected by end-to-end encryption and backups. Redundancies in the infrastructure are a must. It is crucial to employ an effective cybersecurity awareness program for the entire organisation, adopt stringent standards, policies or frameworks that support the above mitigations, implement identity and access management with specific attention to multi-factor authentication, enforce the concept of Least Privilege and continuously audit the security measures in place to ascertain their effectiveness.

There are tools, appliances and applications that are available to support different types of businesses and organisations to be able to maintain an effective cybersecurity program.

With the digital transformation and globalization in the world today, organisations in Africa need to be constantly alert of the challenges presented and the growing number of vulnerabilities exposed every day.

A successful and solid cybersecurity strategy is only as strong as the weakest link.



# 04

*The Data Protection Bill was introduced to establish a comprehensive data protection regime in Kenya. Article 31 of the Constitution gives citizens some level of data privacy in communication.*



# 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 Kenyan 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.

## 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.

STAY IN THE KNOW

## 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.

#### GET TO KNOW

### Africa Cyber Immersion Centre 2021 Courses on Data Protection and Privacy

#### Employees: Data Protection Awareness Training

Practitioners:

“<https://firebrand.training/uk/courses/data-protection/certified-data-protection-officer-certification>”

#### Certified Data Protection Officer - CDPO (GDPR Compliance)

Practitioners:

#### Data Protection Laws and Security - A Technology Guide for Security Practitioners (African and European Data Protection Laws)

Practitioners: Data Security and Investigations

To enroll:  
email >> [info@serianu.com](mailto:info@serianu.com)

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

## 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).
- ☑ Having the expertise at hand to support and assist the users to quickly recover from security incidents.
- ☑ Centralized and specialized handling of and response to IT 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

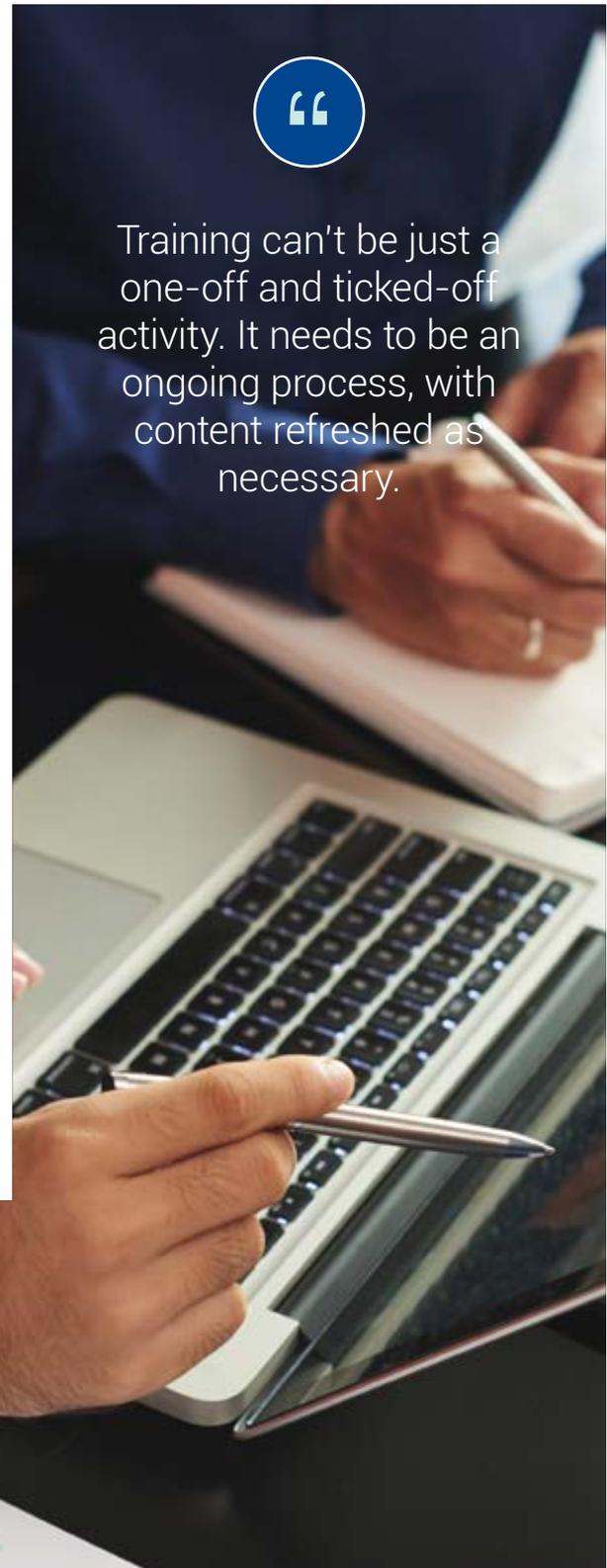
Training can't be just a one-off and ticked-off activity. It needs to be an ongoing process, with content refreshed as necessary.

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.



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



# DATA PROTECTION & COMPUTER MISUSE AND CYBERCRIMES ACTS



## Iseme Kamau & Maema Advocates

*IKM Advocates is a member of DLA Piper Africa, a Swiss Verein whose members are comprised of independent law firms in Africa working with DLA Piper.*

THE LEGAL IMPLICATIONS OF DATA PROTECTION LAWS IN KENYA.

The Data Protection Act ("DPA") came into force on 25th November 2019. It is intended to give effect to Articles 31 (c) and (d) of the Constitution of Kenya, 2010 which guarantees all persons the right to privacy. The DPA regulates the processing of personal data, sets out the principles of data protection and establishes the institutional mechanism to give effect to its provisions.

While the DPA is currently in force, the Government has yet to put in place the institutional framework necessary for its operationalisation.

We set out below the various legal implications of the DPA on businesses in Kenya.

### **a.) Implementation and Enforcement Institution**

Section 5 of the DPA establishes the office of the Data Protection Commissioner ("DPC") whose functions include overseeing the implementation and enforcement of the DPA. The DPC is also responsible for receiving and investigating complaints on infringement of the rights under the DPA, carrying out public awareness,

and conducting inspection of public and private entities, among others.

As soon as the DPC is appointed and the office becomes functional, businesses will need to start complying with the relevant provisions of the Act depending on their requirements.

We also expect that once the office becomes operational, the enforcement of the DPA provisions, including imposition of penalties for breach, will commence. It is yet to be seen if the DPC will grant businesses a moratorium for compliance, hence this is a good opportunity for businesses to get ready to be compliant from the first day of the DPC's appointment.

## **b.) Registration of Data Controllers and Data Processors**

Section 18 of the DPA requires persons acting as data processors and controllers to register with the DPC. However, not all persons are required to register with the DPC as the DPA mandates the DPC to prescribe the thresholds for mandatory registration. In coming up with the said thresholds, the DPC shall consider the following: -

- a.) the nature of industry;
- b.) the volumes of data processed; and
- c.) whether sensitive personal data is being processed.

Therefore, businesses which fall within either or both of the above categories should start making arrangements to register.

## **c.) Data Protection Principles and Lawfulness of Processing**

The DPA requires that the processing of personal data be done in accordance with the principles of data protection as set out in Section 25. This section provides, "every data controller or data processor shall ensure that personal data is: -

- a.) *processed in accordance with the right to privacy of the data subject;*
- b.) *processed lawfully, fairly and in a transparent manner in relation to any data subject;*
- c.) *collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;*
- d.) *adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;*
- e.) *collected only where a valid explanation is provided whenever information relating to family or private affairs is required;*
- f.) *accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;*
- g.) *kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and*
- h.) *not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.*



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.

All these principles must be adhered to whenever a business processes personal data. The rights of data subjects contained in the DPA (including the right to: be informed of the use of personal data, access to data in the custody of data controllers and processors, to object to processing, to correct false or misleading data and deletion of misleading data) are sourced from these principles and it is paramount for businesses to ensure that all processing is compliant with the principles.

#### **d.) Processing of Personal Data of Children**

The DPA defines personal data as *“any information relating to an identified or identifiable natural person.”* Therefore, any information processed by a business would qualify as personal data as long as it can be associated with an identifiable natural person or child.

Section 33 of the DPA provides: *“every data controller or data processor shall not process personal data relating to a child unless—*

- a.) consent is given by the child’s parent or guardian; and*
- b.) the processing is in such a manner that protects and advances the rights and best interests of the child.”*

The DPA requires the existence of two conditions prior to the processing of the personal data of a child, namely, a) parental/guardian consent and b) advancement of the rights and best interests of the child. Consequently, even where a business has obtained the consent of the parent/guardian to process the personal data of a child, it will be required to demonstrate that such processing is in the best interests of the child. The principle of best interests of the child is contained in Article 53 (2) of the Constitution as well as Section 4 of the Children Act 2001.

Further, Section 33 (2) of the DPA provides, *“a data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.”* The onus will therefore be on the business to ensure that they have the operational and, in some cases technological measures to not only verify the age of the user but to also obtain consent of the parent or guardian where the user is below the age of 18 years.

#### **e.) Commercial use of Personal Data**

Under Section 37 of the DPA, the processing of personal data for commercial purposes is prohibited unless the data subject has consented to it. A business must therefore ensure that personal data is not used for such purposes unless there is express consent from the data subject or in case of minors, the parent or guardian.

#### **f.) Security of Personal Data**

The DPA places significant importance on the security of personal data. Section 41 provides, *“every data controller or data processor shall implement appropriate technical and organisational measures which are designed -*

- a.) to implement the data protection principles in an effective manner; and*
- b.) to integrate necessary safeguards for that purpose into the processing.”*

Every processing must therefore ensure that the appropriate safeguards exist to ensure the integrity of personal data is maintained. It is worth noting that incidences of hacking which lead to the exposure of personal data would not absolve the business of liability. Some of the recommended measures under the DPA include pseudonymisation and encryption.

The DPA defines encryption as *“the process of converting the content of any readable data using technical means into coded form.”* Pseudonymisation on the other hand is defined as *“the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.”* These measures are not exhaustive and therefore businesses have the discretion to come up with other technical measures to ensure that the personal data is secure.

Section 43 (1) of the DPA provides, *“where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, a data controller shall-*

- a.) *notify the Data Commissioner without delay, within seventy-two hours of becoming aware of such breach; and*
- b.) *subject to subsection (3), communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established."*

A business which qualifies as a data controller has an obligation to notify the DPC of any breaches within seventy-two hours of becoming aware of the breach. The notification must include information such as: -

- a.) a description of the nature of the data breach;
- b.) a description of the measures that the data controller or data processor intends to take or has taken to address the data breach;
- c.) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;
- d.) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and
- e.) the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.

Data controllers who rely on data processing entities must ensure that the processor selected has in place the relevant technical and organisational measures to ensure the security

and integrity of personal data. The processor must also be under a contractual obligation to inform the data controller of any breach within 72 hours of becoming aware of such a breach to ensure that the latter on its part informs the DPC within the stipulated timelines.

### **g.) Transfer of Personal Data outside Kenya**

The DPA sets certain requirements that must be met prior to the transfer of personal data outside Kenya. Section 48 of the DPA provides that a data controller or processor may transfer personal data outside Kenya if they give the DPC proof that the appropriate safeguards exist prior to the transfer of data outside Kenya including the existence of commensurate data protection laws. Therefore, 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.

The DPA also provides other grounds for the transfer of personal data outside Kenya which include the following:-

- a.) for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
- b.) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
- c.) for any matter of public interest;
- d.) for the establishment, exercise or defence of a legal claim;
- e.) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- f.) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

A business must therefore ensure that at least one of the grounds above exist prior to any proposed transfer of personal data outside Kenya.

### **h.) Liability for Non-Compliance**

The DPC is empowered to investigate complaints by any person for any violation of the provisions of the DPA. Upon investigation, the DPC may issue an enforcement

notice to any person deemed to be in violation of the DPA. Failure to comply with an enforcement notice is offence which attracts a fine not exceeding Ksh. 5,000,000/- or imprisonment for up to two years or both a fine and imprisonment.

The DPC also has the power to issue penalty notices for up to Ksh. 5,000,000/- or in the case of an undertaking up to 1% of its annual turnover of the preceding financial year, whichever is lower.

## The intention of Cybercrime/ data protection law in Kenya and whether it achieves its goal

### a.) The Data Protection Act

The DPA is intended to protect an individual's right to privacy. It is intended to regulate the processing of personal data in Kenya. Having come into effect in late 2019 and since the institutional framework is not in place, it is difficult to gauge its success in achieving the objectives set out in the DPA.

Having said that, it is noteworthy that the DPA is modelled around global best practices including the EU General Data Protection Regulation. If implemented to its spirit, the DPA has the potential to revolutionize data protection matters in Kenya.

There is also the need to pass Regulations and Guidelines to give effect to some of the provisions of the DPA. There has been some movement on this front with the ICT Ministry having recently published the Data Protection (Civil Registrations) Regulations, 2020 for public participation. However, more needs to be done in order to ensure that Kenya is at par with other developed markets.

### b.) The Computer Misuse and Cybercrimes Act

The Computer Misuse and Cybercrimes Act, 2018 ("CMCA") was assented to on 16th May 2018 and was intended to commence on 30th May 2018. However, the Bloggers Association of Kenya filed a Petition challenging some of the provisions of the CMCA which led to the suspension of some of the provisions of the CMCA.

In February 2020, the High Court dismissed the Petition and the CMCA is now effective. However, due to the suspension of the CMCA since 2018, its efficacy as far as punishing cybercrimes is concerned cannot be determined at this point.

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

The DPA defines consent as *"any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement*

*to the processing of personal data relating to the data subject."*

Section 32 of the DPA places the burden of proof for establishing a data subject's consent to the processing of their personal data for a specific purpose on the data controller or data processor.

There is no standard of ensuring that the right level of consent is obtained. However, it is important for the data controller to ensure that where consent is the lawful reason used to process the personal data, the data subject must be informed of their rights, the reasons for processing, the purpose of the processing and whether the personal data will be transferred to third parties. To minimize risk, we would recommend that the consent be in writing and that the above information is contained in a data protection/privacy policy which is always accessible to data subjects.

Having said that, it is worth noting that consent is not mandatory when processing personal data as the data controller or processor can rely on the grounds of processing personal data listed in section 30 of the DPA. These include: -

- a.) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
- b.) for compliance with any legal obligation to which the controller is subject;
- c.) in order to protect the vital interests of the data subject or another natural person;
- d.) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- e.) the performance of any task carried out by a public authority;
- f.) for the exercise, by any person in the public interest, of any other functions of a public nature;
- g.) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
- h.) for the purpose of historical, statistical, journalistic, literature and art or scientific research.



# 05

*The Data Protection Law outlines the conditions for the transfer of personal data outside of Kenya 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
<i>Personal Data Processed</i>	Contact information (last and first name, address, telephone number,) social security number, taxation Identifier, date of employment, salary information
<i>Processing Purpose</i>	Payroll management (payment of salaries, benefits and social security contributions)
<i>Data Subject</i>	Employees
<i>Processing Means</i>	Human Resources IT System
<i>Recipients of the Data</i>	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

<i>Personal Data Processed</i>	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
<i>Processing Purpose</i>	Managing candidate selection for recruitment Assessment of the performance and professional characteristics that arise in the execution of the work
<i>Data Subject</i>	Recruitment Candidates Employees
<i>Processing Means</i>	Recruitment IT platform Human Resources IT System
<i>Recipients of the Data</i>	Internal-Senior Management, Line managers
<i>Potential Gaps</i>	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.

<b>PROCESSING OPERATION DESCRIPTION</b>	<b>ORDER AND DELIVERY OF GOODS</b>	
<i>Personal Data Processed</i>	Contact information (last and first name, address, telephone number) payment data (credit card, bank account information)	
<i>Processing Purpose</i>	Order and delivery of goods	
<i>Data Subject</i>	Customers	
<i>Processing Means</i>	Order Management system	
<i>Recipients of the Data</i>	External	Payment service provider
	External	Delivery service provider
	Internal	Customer Relation Management (CRM) system
	Internal	Enterprise Resource Planning (ERP) system
<i>Processing</i>	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.	
<i>Potential gaps</i>	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	
<i>Personal Data Processed</i>	Contact name, postal address, telephone number, email	
<i>Processing Purpose</i>	Promotion of goods and special offers to possible customers	
<i>Data Subject</i>	Customers and potential customers	
<i>Processing Means</i>	Third party marketing campaign web service	
<i>Recipients of the Data</i>	External	Third party marketing campaign web service provider
	Internal	Marketing Department
	Internal	CRM IT system
<i>Data Processor Used</i>	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)
<i>Personal Data Processed</i>	First and last name, contact Information, tax and banking information (for supplier), picture and access credentials (for staff working on premises).
<i>Processing Purpose</i>	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)**

<i>Data Subject</i>	Employees working for suppliers of goods and services	
<i>Processing Means</i>	IT system	
<i>Recipients of the Data</i>	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    ACCESS CONTROL**  
**DESCRIPTION**

<i>Personal Data Processed</i>	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.	
<i>Processing Purpose</i>	Physical-logical Access Control Security	
<i>Data Subject</i>	Employees, visitors	
<i>Processing Means</i>	Access control management platform	
<i>Recipients of the Data</i>	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<sup>1</sup> 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"<sup>2</sup>.

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<sup>3</sup> and others by 2050<sup>4</sup>.

According to United Nations Conference on Trade and Development (UNCTAD)<sup>5</sup> 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

<sup>1</sup> <https://www.quora.com/Who-should-get-credit-for-the-quote-data-is-the-new-oil>

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

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

<sup>4</sup> [https://ec.europa.eu/clima/policies/strategies/2050\\_en](https://ec.europa.eu/clima/policies/strategies/2050_en)

<sup>5</sup> <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

will be crucial in driving economies in the fourth industrial revolution<sup>6</sup>. 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 digitalization of public services.

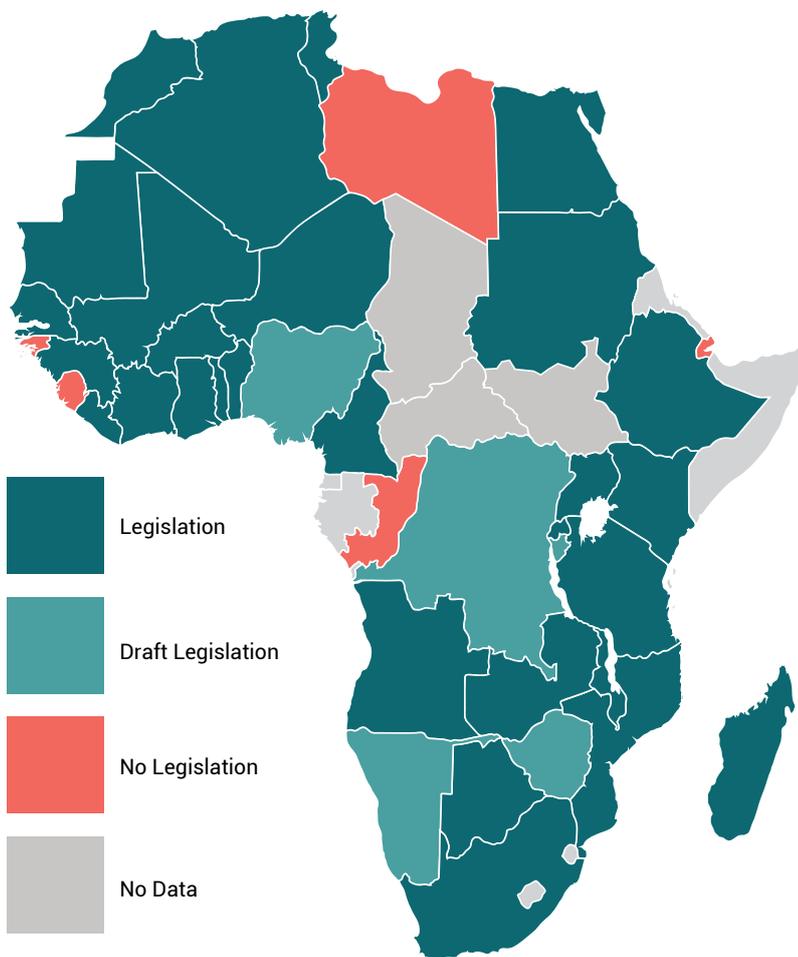
There needs to be increased collaboration between academia and the industry so that learning

institutions produce career-ready graduates with appropriate 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.

<sup>6</sup> <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 appropriate skills relating to data protection and privacy.





## 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
<i>Personal Data Processed</i>	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).
<i>Processing Purpose</i>	Provision of healthcare services (diagnosis, treatment an hospitalization)
<i>Data Subject</i>	Patients
<i>Processing Means</i>	Medical IT system
<i>Recipients of the Data</i>	Internal      Treating doctors and nurses
<i>Internal</i>	Administration and accounting IT system
<i>External</i>	Public Health System
<i>Potential gap</i>	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**

<i>Personal Data Processed</i>	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	
<i>Processing Purpose</i>	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	
<i>Data Subject</i>	Children, parents, students, professors	
<i>Processing Means</i>	Web based, e-Learning and course management platform	
<i>Recipients of the Data</i>	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 3:** 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 geolocation. La Liga used the information to sue 600 bars for pirating soccer games

General Data Protection Regulation (GDPR)



# IMPACT OF PRIVACY IN THE ERA OF DIGITAL ECONOMY

**In today's digital economy, customers can come from any part of the world. They may dial in, visit enterprises' online presence or walk-in physically to the premises. As they do this, enterprises from across the world are also able to collect and retain customer information to help improve their experience and for regulatory compliance.**



## Michael Abuli

*Information Security Manager, Nairobi Securities Exchange, Kenya.*

Customer data collection might seem counter-intuitive in an era where privacy is a major issue hence the coming into existence of data privacy laws in different jurisdictions. The most famous of them all is the General Data Protection Regulation (GDPR) issued by the European Union.

The deadline for enterprises to comply with GDPR was May 25th 2018. This statute affects both European and non-European based businesses which are subject to the GDPR.

Closer home, the Kenya Data Protection Act of 2019 mimics the European GDPR with negligible differences. The race is on to be compliant before the Kenyan Office of the Data Protection Commissioner (ODPC) is established and starts to bite with some organisations in Kenya advertising for data protection officers (DPO).

Consequently, most local companies have had to adjust their mindset on data privacy. This helps build customer trust and can save your business from a big headache down the road. To prepare for GDPR and the Kenya Data

Protection Act, Organisations should identify a cross-functional Data Privacy leadership team with C-suite/board representation to carry out assessment of the current state of data protection.

At the tail end of this endeavor, the leadership team should be able to answer the WHO, WHAT, WHERE and HOW questions about the enterprise's data. This will help the organisation to formulate a data privacy roadmap to shield personal information, obtain authority from data subjects during processing of personal data and enable them have the ability to access, correct and erase their information when necessary. At the same time the enterprise will strike an economic balance between the impact of the threat and the cost of the safe guards on the data.

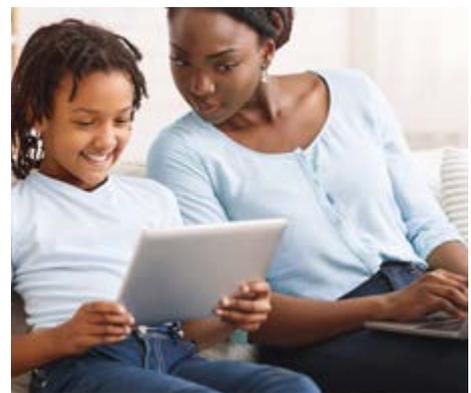


To determine the extent of the investment for prevention or mitigation, questions that the Data Privacy leadership team should be able to answer during this exercise include; where is the enterprise data? How is it collected, processed and stored? What is the value of this data to the enterprise? They should also seek to know who has access to the data including third-party suppliers and how are accessing this information.

Other considerations include the internal/external vulnerabilities and threats facing the data and the potential impact on the business. What appropriate and adequate security measures can be put in place to safeguard the data? What would the business do if they lost all its data? What are the data back up and testing strategies in place? What are the suitable business continuity and disaster recovery plans in place and what is the organisation's plan of action and responsibilities in the case of a data breach?

It is a new field that requires thorough assessment and attention to detail. There is no doubt that data privacy cannot be taken lightly by any organisation in possession of customer or staff personal, financial or other critical information. When data privacy is critical to any organisation, C-suite/board teams must support internal and external education, training and awareness campaigns for data privacy has become everyone's business.

There is no doubt that data privacy cannot be taken lightly by any organisation in possession of customer or staff personal, financial or other critical information.



# 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.



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

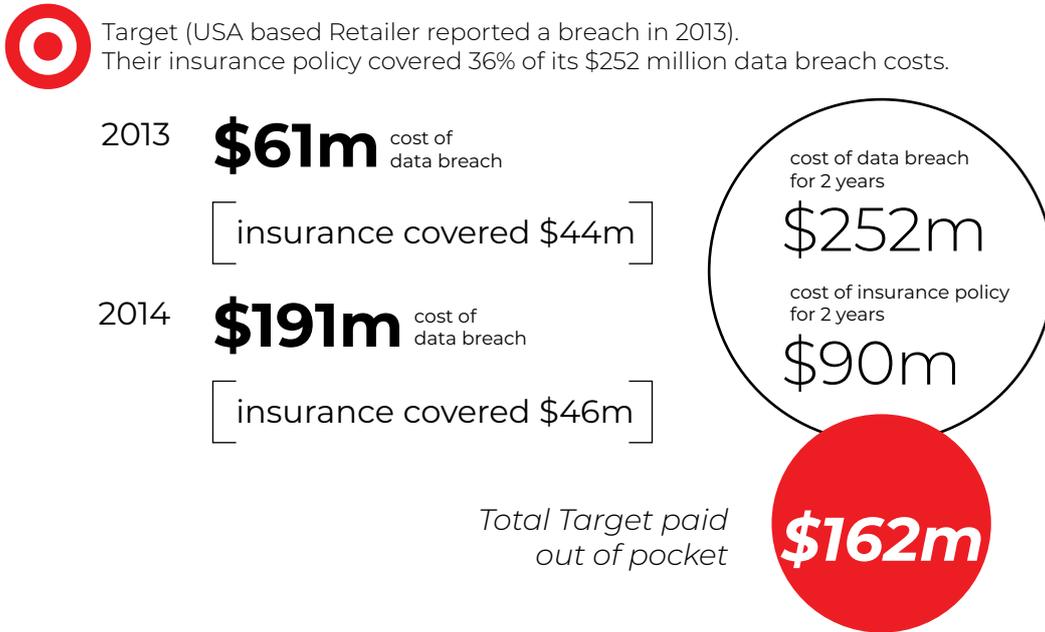


**\$6 Trillion**  
annually by 2021

## 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:



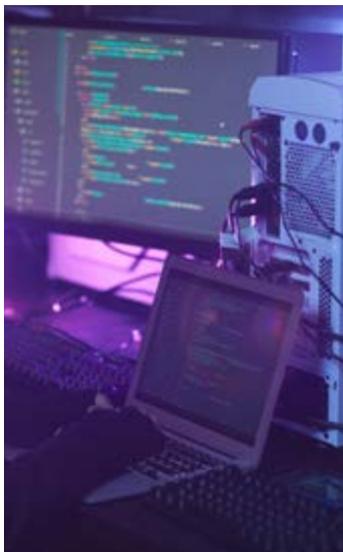
Detailed breakdown of Risk Quantification, Cyber Insurance and Cost of Cybercrime will be provided in the Cost of Cybercrime - Africa Report.



# 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.

# A NEW CHAPTER OF CYBERSECURITY CONCERN FOR ACADEMIA IS GRADE MANIPULATION.

## Walter Ombiro

*Head of IT, Alliance Boys High School*

Students can change their own marks or even edit report forms to acquiesce their tough parents at home.

Students gain access to the school systems and received payments from other students to alter scores or print new report forms to take home especially for those students whose scores are not too impressive.

Wi-Fi passwords are sold to other students to access networks using their illegally possessed phones. Many of those with internet access use it for betting, online games,

social media and watching pornographic content.

These are examples of the many cybersecurity related issues that have been reported especially touching on the youth. These young and smart chaps will use very small loopholes in our systems, phones, computers, Wi-Fi and other networks to wreak havoc on hardware, software and data therein.



Wi-Fi passwords are sold to other students to access networks using their illegally possessed phones.



# WHAT ARE THE BIGGEST CHALLENGES THAT THE ACADEMIA SECTOR FACES WHEN IT COMES TO CYBERSECURITY?

One of the biggest challenges that the academia sector has been facing is lack of awareness on cybersecurity.

## Geoffrey Manoti Maina

*Network/Information Security Engineer,  
Multimedia University of Kenya,*

Getting information to staff, students and stakeholders on how to secure themselves online has proved difficult. With this predicament there has emanated an opportunity to provide a solution.

From my expertise as a cyber-security specialist to secure university resources some of the recommendations include:

1. Document and implement cyber-security policies in institutions.
2. Advise the top management on the importance of cybersecurity.
3. Implement a Computer Emergency Response Team (CERT) to deal with cybersecurity incidents and threats.
4. Use of security technologies like firewalls and antivirus.
5. Cybersecurity awareness trainings for staff, students and stakeholders.



Universities need to implement a Computer Emergency Response Team (CERT) to deal with cybersecurity incidents and threats.



**Equipping and empowering young people with the skills necessary to detect and contain cyber threats is a very important task in this information age.**

## **Daniel Kihia,**

*Tech Educator, Nova Pioneers Girls*

Cyber insecurity is a serious international threat that needs to be addressed.

Serianu has made this possible by having Cyber Immersion training programs that are aimed at mentoring and helping students to learn and practice ethical hacking skills which later help them to be safe and secure

online. Nova Pioneers Girls students were privileged to attend the training sessions and they learnt quite a lot. They expressed interest in the program and some are considering it as a viable career path.



“

Programs that are aimed at mentoring and helping students to learn and practice ethical hacking skills.



# EXPERIENCE WHEN IT COMES TO CYBERSECURITY OR TECHNOLOGY?

Currently I am involved in mentoring fellow students who look up to me even as I am mentored by industry professionals. My growth in the cybersecurity field would have been stunted if not for mentorship.



## Lorena Munene

*Student, Multimedia University of Kenya*

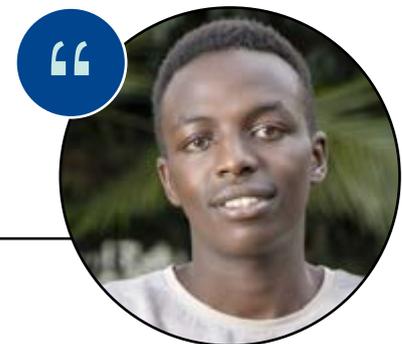


Initially, I thought cybersecurity was just about hacking WIFI passwords but I was very wrong. I have learnt that cybersecurity is a broad discipline ranging from computer security to disaster discovery. How did I learn? My curiosity and willingness to learn new skills has been helpful during this journey. I have done various online security courses including the Certified Ethical Course (CEH), attended security meetups and boot camps. I actively engaged myself in spaces where I get to interact with like-minded individuals.

## Mercy Chebet

*Student, Multimedia University of Kenya*

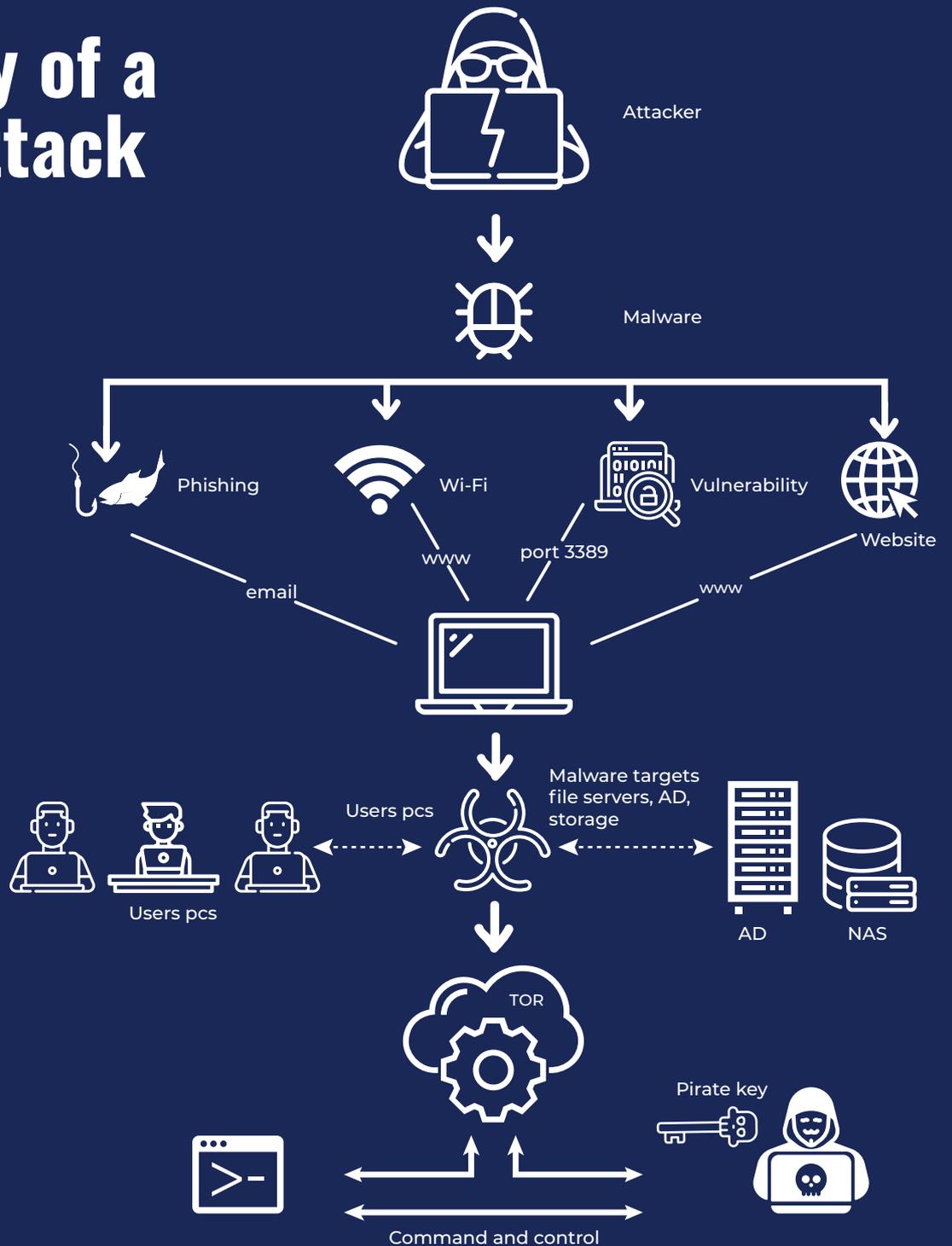
Since Serianu launched the Cyber Immersion Club at Alliance High School, I have learnt a lot. The curiosity made learning and interaction easy and interesting. Apart from that, I also served as the vice president of the ICT Club. At first I thought cybersecurity was all about hacking, but later I learnt that it entails so much more. In today's world, cybersecurity is very important because of the many security threats and cyber-attacks.



## Kevin Kattam

*Student Alumni, Alliance Boys High School*

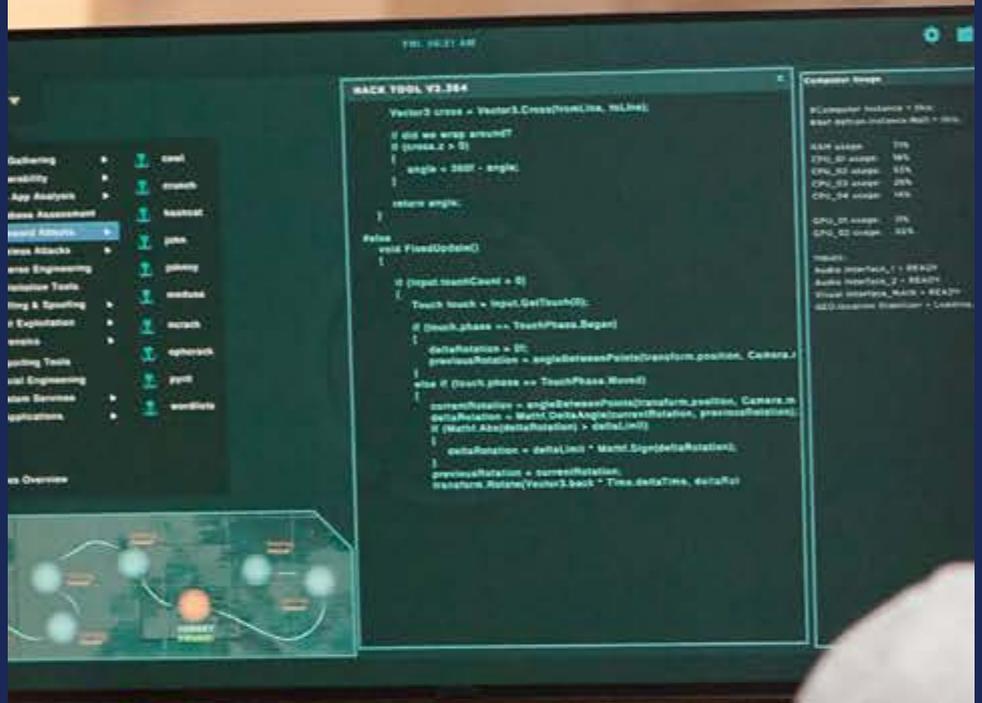
# Anatomy of a cyber attack



Initial

Gaining access

Maintaining & encryption



# 07

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



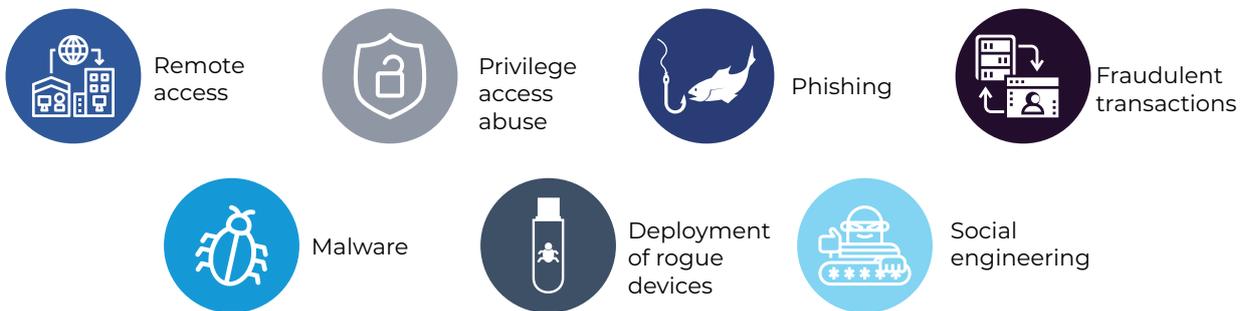
# 7. 2021 PRIORITIES

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:** Kenya

**Name of Bill/Law/Act:** Data Protection Bill

**Year drafted/Enacted:** 2019

**Status:** Enacted to law

### **Summary:**

#### **What sections are covered?**

- Establishment of the Office of the Data Protection Commissioner
- Registration of Data Controllers and Data Processors
- Data Protection
- Storage of Data
- Transfer of Personal Data Outside Kenya
- Enforcement

#### **Who authored it?**

Kenya's president Uhuru Kenyatta approved legislation

#### **Key issues addressed**

- Consent
- Data Protection Officer
- Email Marketing
- Encryption
- Fines / Penalties
- Personal Data
- Privacy by Design
- Privacy Impact Assessment
- Processing
- Records of Processing Activities
- Right of Access
- Right to be Forgotten
- Right to be Informed

8.1. SECTION ADDRESSED	Details
8.2. DEFINITION OF PERSONAL DATA	Sensitive personal data is defined as data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.
8.2.1. Section 2 of the Act	The Data Protection Act, 2019 (the "Act") came into force on 25th November, 2019 and is now the primary statute on data protection in Kenya. It gives effect to Article 31 c) and d) of the Constitution of Kenya, 2010 (right to privacy).
8.3. DEFINITION OF SENSITIVE PERSONAL DATA	Sensitive personal data is defined as data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.
8.4. PART II OF THE ACT	The Act established the Office of the Data Protection Commissioner (DPC) whose mandate includes overseeing the implementation and enforcement of the provisions of the Act. The DPC is also tasked with the maintenance of the register of data controllers and processors, receiving and investigation of complaints under the Act and carrying out inspections of public and private entities to evaluate the processing of personal data.
8.5. SECTION 18 OF THE ACT	Data processors and data controllers are required to be registered with the DPC. The DPC, however, has discretion to prescribe the thresholds for mandatory registration based on: <ul style="list-style-type: none"> <li>■ The nature of industry;</li> <li>■ The volumes of data processed; and</li> <li>■ Whether sensitive personal data is being processed.</li> </ul>
8.6. SECTION 24 OF THE ACT	<p>The Act makes provisions for the designation of Data Protection Officers (DPOs) but this obligation is not mandatory.</p> <p>DPOs can be members of staff and may perform other roles in addition to their roles. A group of entities can share a DPO and the contact details of the DPO must be published on the organisation's website and communicated to the DPC.</p> <p>DPOs have the following roles:</p> <ul style="list-style-type: none"> <li>■ Advising the data controller or data processor and their employees on data processing requirements provided under the Act or any other written law;</li> <li>■ Ensuring compliance with the Act;</li> <li>■ Facilitating capacity building of staff involved in data processing operations;</li> <li>■ Providing advice on data protection impact assessment; and</li> <li>■ Co-operating with the DPC and any other authority on matters relating to data protection.</li> </ul>
8.7. SECTION 25 OF THE ACT	<p>The processing of personal data must comply with the principles prescribed in this part. It must be:</p> <ul style="list-style-type: none"> <li>■ Processed in accordance with the right to privacy of the data subject;</li> <li>■ Processed lawfully, fairly and in a transparent manner in relation to any data subject;</li> <li>■ Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;</li> <li>■ Adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;</li> <li>■ Collected only where a valid explanation is provided whenever information relating to family or private affairs is required</li> <li>■ Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;</li> <li>■ Kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and</li> <li>■ Not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.</li> </ul>

8.1. SECTION ADDRESSED	Details
8.8. SECTION 30 OF THE ACT	<p>The Act recommends personal data to be collected and processed lawfully. The lawful reasons for processing include:</p> <ul style="list-style-type: none"> <li>■ Consent of the data subject; or</li> <li>■ The processing is necessary: <ul style="list-style-type: none"> <li>• for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;</li> <li>• for compliance with any legal obligation to which the controller is subject;</li> <li>• in order to protect the vital interests of the data subject or another natural person;</li> <li>• for the performance of a task carried out in the public interest or in the exercise of <ul style="list-style-type: none"> <li>• official authority vested in the controller;</li> <li>• the performance of any task carried out by a public authority;</li> </ul> </li> <li>• for the exercise, by any person in the public interest, of any other functions of a public nature;</li> <li>• for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or</li> <li>• for the purpose of historical, statistical, journalistic, literature and art or scientific research.</li> </ul> </li> </ul>
	It is an offence to process personal data without a lawful reason.
8.9. PART VI OF THE ACT	<p>The transfer of personal data outside Kenya 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.</p> <p>The consent of the data subject is required for the transfer of sensitive personal data out of Kenya.</p>
8.10. SECTIONS 41 AND 42 OF THE ACT	Data controllers and processors are required to implement the appropriate organisational and technical measures to implement data protection principles in an effective manner.
8.11. BREACH NOTIFICATION	Data controllers have an obligation to notify the DPC of any breaches within 72 hours of becoming aware of a breach. On the other hand, data processors are required to inform data controllers of any breach within 48 hours of becoming aware of such a breach.
8.12. SECTION 43 OF THE ACT	The data controller must notify the data subject of such breach without undue delay.
8.13. MANDATORY BREACH NOTIFICATION	Yes. Please see above analysis under "Breach Notification"
8.14. SECTION 62 OF THE ACT	<p>In instances where the DPC is satisfied that any person has violated the provisions of the Act, he has the power to issue penalty notices for up to a maximum of Kenya Shillings Five Million (approximately USD 50,000) or 1% of an undertaking's annual turnover the preceding year, whichever is lower.</p> <p>In addition, any act which constitutes an offence under the Act where a penalty is not provided attracts a fine of up to Kenya Shillings Three Million (approx. USD 30,000) or imprisonment for up to 10 years or both a fine and imprisonment.</p>

8.1. SECTION ADDRESSED	Details
8.15. SECTION 37 OF THE ACT	<p>The use of personal data for commercial purposes is prohibited unless the person undertaking this processing:-</p> <ul style="list-style-type: none"> <li>■ Has sought and obtained express consent from a data subject; or</li> <li>■ 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.</li> </ul> <p>The Cabinet Secretary in charge of information, communication and technology may, in consultation with the DPC, develop guidelines on the commercial use of personal data.</p>
8.16. ONLINE PRIVACY	Kenyan law does not regulate on-line privacy. However, this may be prescribed in the regulations or future amendments to the Act.

## Fines

Crime	Fine	Other consequences
A person has violated the provisions of the act.	<p>In instances where the DPC is satisfied that any person has violated the provisions of the Act, he has the power to issue penalty notices for up to a maximum of Kenya Shillings Five Million (approximately USD 50,000) or 1% of an undertaking's annual turnover the preceding year, whichever is lower.</p> <p>In addition, any act which constitutes an offence under the Act where a penalty is not provided attracts a fine of up to Kenya Shillings Three Million (approx. USD 30,000) or imprisonment for up to 10 years or both a fine and imprisonment.</p>	

## Establishment of the Office of the Data Protection Commissioner

The act sets up the workplace of a Data Protection Commissioner.

The Commissioner's office is commanded with directing the execution of the Act together with setting up and keeping up a register of data controllers and data processors; discovering and investigating any complaints on encroachments of the rights under the Act; doing examinations with the end goal of assessing the preparing of personal information; forcing authoritative fines for disappointments to agree to the Act, among different functions.

## Registration of Data Controllers and Data Processors

All data controllers and data processors are required to be enrolled with the Commissioner. The Commissioner is required to recommend compulsory enrollment and is to think about the nature of the industry; the amount of data information being handled.

## Data Protection

Each data controller or processor is required to guarantee that every personal data is handled legally, reasonably and in a straightforward way comparable to any data act. The Act applies to data controllers and processors set up or inhabitant in or outside Kenya as long as they process data situated in Kenya.

The data subjects reserve the right to be informed on the use of their own information; to question the handling of all or some portion of their own information; to delete deluding information, and to eradicate bogus or misdirecting information about them.

## Storage of Data

There are no recommended spans for the storage of individual data. Data controllers and processors are required to apply a sensibility test in evaluating storage lengths.

# REFERENCES

Cisomag. (2019, July 8). Cyber-attacks on Kenyan organisations rise to 11.2 million. Retrieved February 14, 2020, from <https://www.cisomag.com/cyber-attacks-on-kenyan-organisations-rise-to-11-2-million/>

Janzen, G., Janzen, G., Nourse, S., Nourse, S., & Mawudor, B. G. (n.d.). Top trends to repel cyberattacks in Kenya. Retrieved February 14, 2020, from <https://www.is.co.ke/blog/articles/top-trends-to-repel-cyberattacks-in-kenya/>

Cybersecurity Threat landscape in Kenya 2019 and the remedy. (n.d.). Retrieved February 14, 2020, from <https://www.mtn.co.ke/insights/cybersecurity-threat-landscape-in-kenya-and-the-remedy-2/>

Emerging trends in the financial industry: <https://www.linkedin.com/pulse/emerging-trends-financial-industry-its-impact-software-nelson-kamau/>

Enisa, Handbook on Security of Personal Data Processing: <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>

Arinifu Company Profile. (n.d.). Retrieved February 14, 2020, from <https://arinifu.com/company-profile/>

Vulnerability Information. (n.d.). Retrieved February 14, 2020, from [https://talosintelligence.com/reputation\\_center/lookup?search=Kenya#ip-addresses](https://talosintelligence.com/reputation_center/lookup?search=Kenya#ip-addresses)

Kenyan government official websites hacked and defaced. (2019, June 3). Retrieved February 14, 2020, from <https://nairobinews.nation.co.ke/news/kenyan-government-websites-hacked>

<http://www.ikm.co.ke/news/articles/2019/WHY-KENYAN-FIRMS-RISK-PAYING-BILLIONS-OF-SHILLINGS-IN-FINES-FOR-BREACH-OF-EUROPEAN-DATA-LAW.html>

<https://www.aig.co.ke/commercial/products/financial-lines/cyber-edge-insurance>

<https://ke.britam.com/insure/business/protect-your-business/cyber-insurance>

[http://www.projecthoneypot.org/list\\_of\\_ips.php?by=13&ctry=KE](http://www.projecthoneypot.org/list_of_ips.php?by=13&ctry=KE)

[http://www.projecthoneypot.org/list\\_of\\_ips.php?by=16&ctry=KE](http://www.projecthoneypot.org/list_of_ips.php?by=16&ctry=KE)

<https://www.dlapiperdataprotection.com/index.html?t=law&c=KE>

<https://censys.io/>

<https://www.shodan.io/>

<https://zone-h.org/?hz=2>

<https://postamate.com/interpol-names-juja-a-global-cyber-crime-hotspot/>

<https://www.pulselive.co.ke/news/dci-reveals-list-of-130-wanted-for-electronic-fraud-by-hacking-into-banks/rlnx5hp>



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



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](mailto:info@serianu.com)



**WEBSITE**

<https://www.serianu.com>