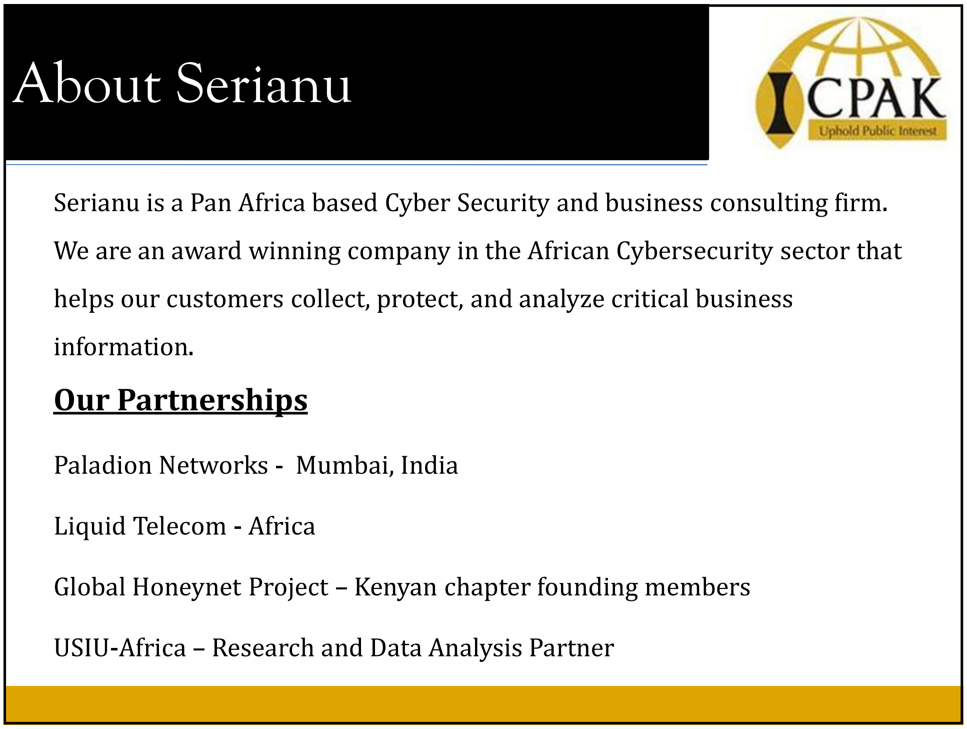
Contemporary Corporate Governance Issues from an Audit Perspective: Emerging Risks – Technology Risks, Fraud, Corruption, Artificial Intelligence and Cyber Crime

William Makatiani, Managing Director Serianu Limited.



About Serianu

Serianu is a Pan Africa based Cyber Security and business consulting firm. We are an award winning company in the African Cybersecurity sector that helps our customers collect, protect, and analyze critical business information.

Our Partnerships

Paladion Networks - Mumbai, India

Liquid Telecom - Africa

Global Honeynet Project – Kenyan chapter founding members

USIU-Africa – Research and Data Analysis Partner

24/7 Security Command Centre

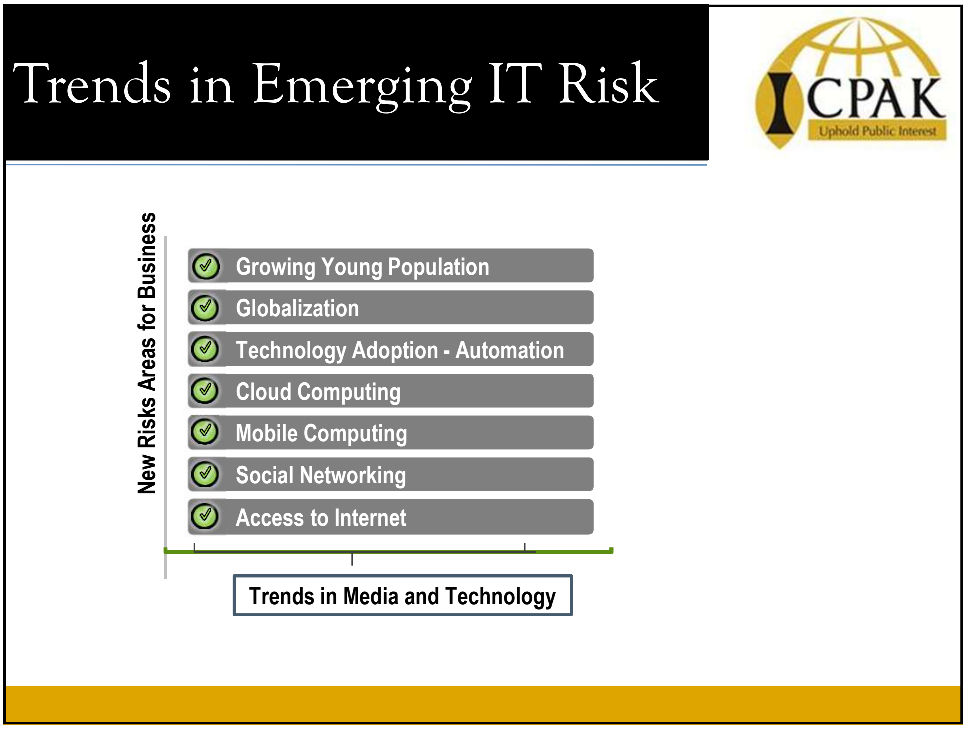
ICPAK
Uphold Public Interest

Africa Cyber Immersion Centre

ICPAK
Uphold Public Interest

Technical Cyber Immersion trainings are delivered at the **Africa Cyber Immersion Centre (ACIC)** in Nairobi, Kenya. ACIC emulates the environments and operations of enterprises using state-of-the-art technologies.

We simulate cyber-attacks in order to test an organisation's inherent vulnerabilities, defense and response capabilities. This facility also replicates an organisation's operating environment and uses the latest range of cyber threats, including an extensive library of viruses and malware, to simulate attacks.

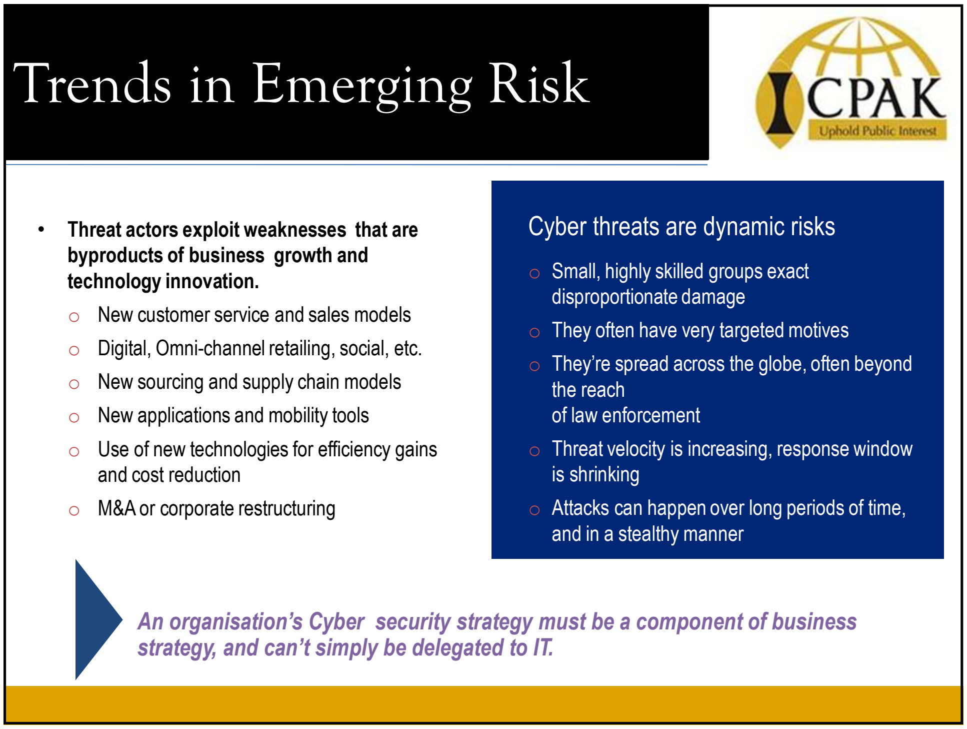


Trends in Emerging IT Risk

New Risks Areas for Business

- ✓ Growing Young Population
- ✓ Globalization
- ✓ Technology Adoption - Automation
- ✓ Cloud Computing
- ✓ Mobile Computing
- ✓ Social Networking
- ✓ Access to Internet

Trends in Media and Technology



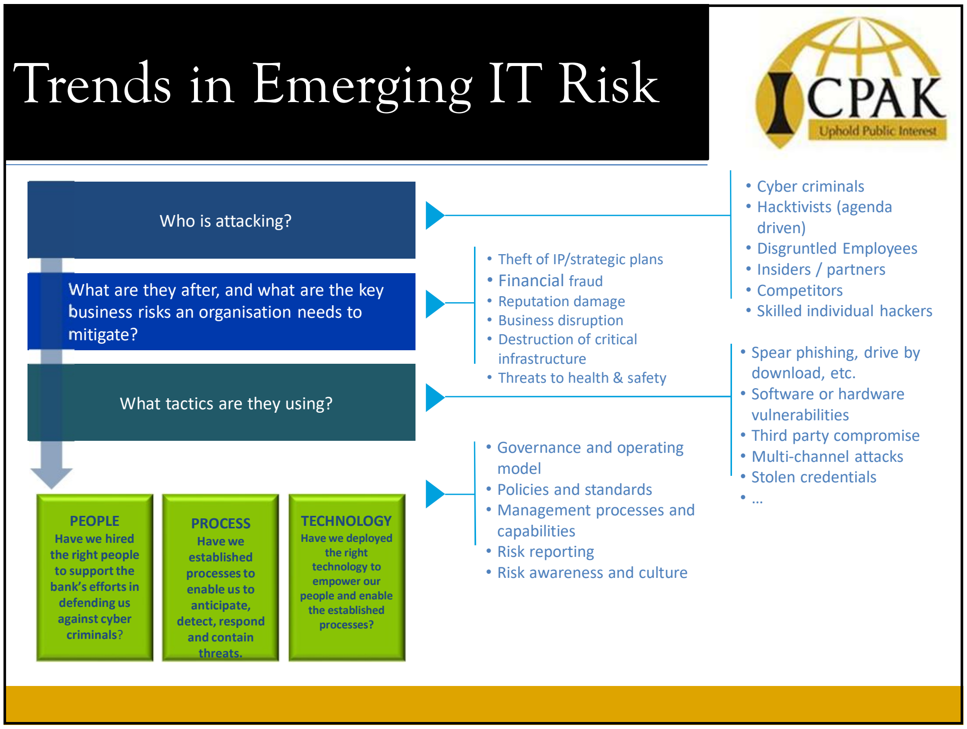
Trends in Emerging Risk

- **Threat actors exploit weaknesses that are byproducts of business growth and technology innovation.**
  - ○ New customer service and sales models
  - ○ Digital, Omni-channel retailing, social, etc.
  - ○ New sourcing and supply chain models
  - ○ New applications and mobility tools
  - ○ Use of new technologies for efficiency gains and cost reduction
  - ○ M&A or corporate restructuring

Cyber threats are dynamic risks

- ○ Small, highly skilled groups exact disproportionate damage
- ○ They often have very targeted motives
- ○ They're spread across the globe, often beyond the reach of law enforcement
- ○ Threat velocity is increasing, response window is shrinking
- ○ Attacks can happen over long periods of time, and in a stealthy manner

An organisation's Cyber security strategy must be a component of business strategy, and can't simply be delegated to IT.



Trends in Emerging IT Risk

ICPAK Uphold Public Interest

Who is attacking?

- Cyber criminals
- Hacktivists (agenda driven)
- Disgruntled Employees
- Insiders / partners
- Competitors
- Skilled individual hackers

What are they after, and what are the key business risks an organisation needs to mitigate?

- Theft of IP/strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety

What tactics are they using?

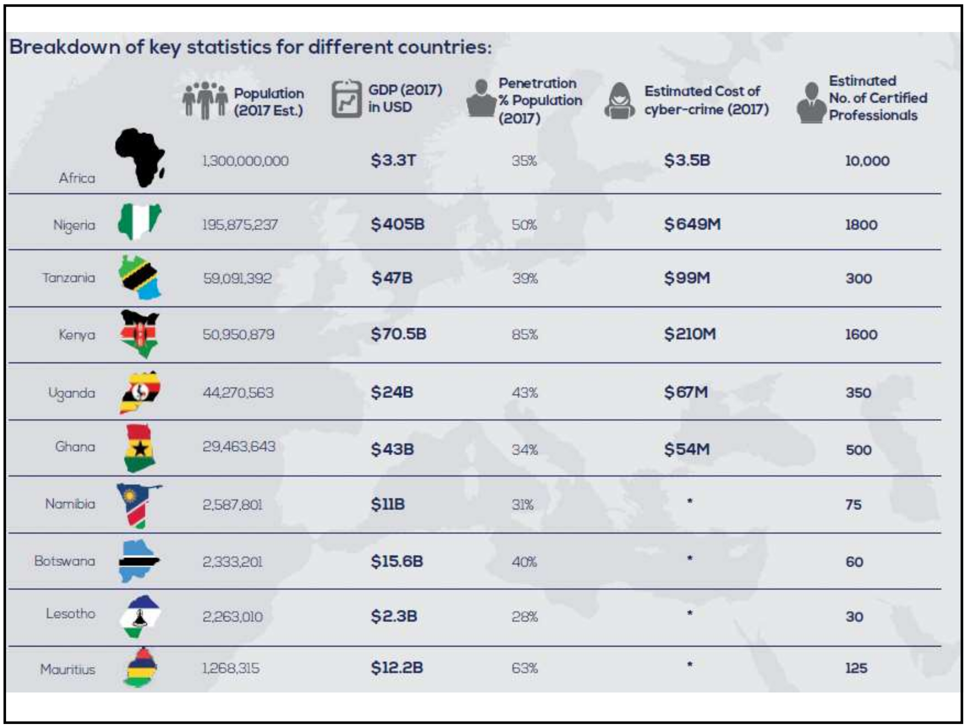
- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Stolen credentials
- …

PEOPLE Have we hired the right people to support the bank's efforts in defending us against cyber criminals?

PROCESS Have we established processes to enable us to anticipate, detect, respond and contain threats.

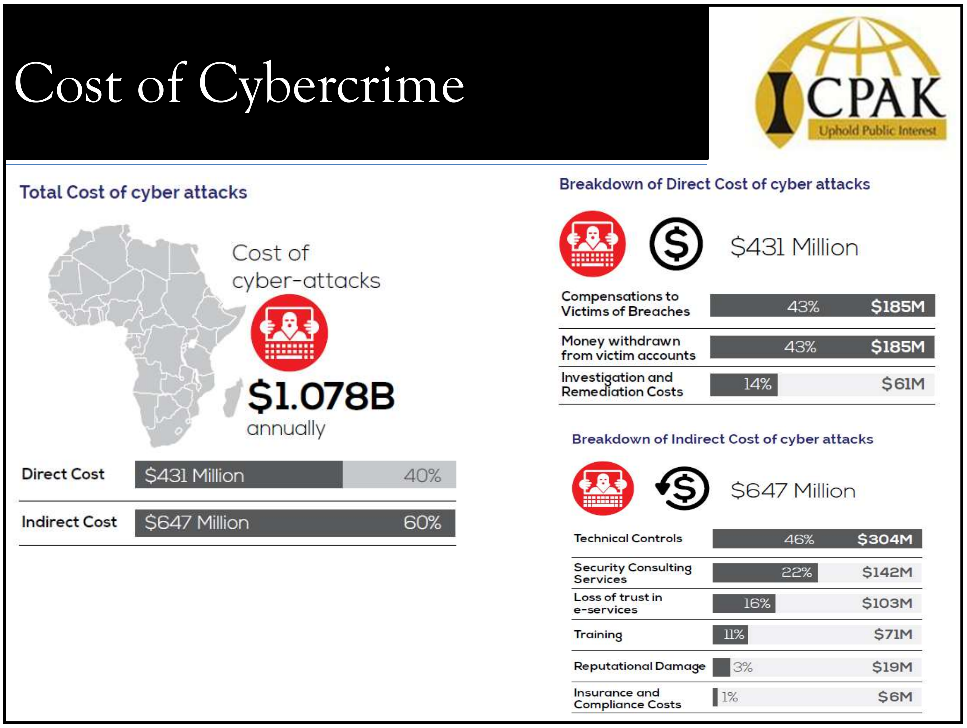
TECHNOLOGY Have we deployed the right technology to empower our people and enable the established processes?

- Governance and operating model
- Policies and standards
- Management processes and capabilities
- Risk reporting
- Risk awareness and culture



Breakdown of key statistics for different countries:

	Population (2017 Est.)	GDP (2017) in USD	Penetration % Population (2017)	Estimated Cost of cyber-crime (2017)	Estimated No. of Certified Professionals
Africa	1,300,000,000	$3.3T	35%	$3.5B	10,000
Nigeria	195,875,237	$405B	50%	$649M	1800
Tanzania	59,091,392	$47B	39%	$99M	300
Kenya	50,950,879	$70.5B	85%	$210M	1600
Uganda	44,270,563	$24B	43%	$67M	350
Ghana	29,463,643	$43B	34%	$54M	500
Namibia	2,587,801	$11B	31%	*	75
Botswana	2,333,201	$15.6B	40%	*	60
Lesotho	2,263,010	$2.3B	28%	*	30
Mauritius	1,268,315	$12.2B	63%	*	125



Cost of Cybercrime

ICPAK
Uphold Public Interest

Total Cost of cyber attacks

Cost of cyber-attacks

$1.078B
annually

Direct Cost	$431 Million	40%
Indirect Cost	$647 Million	60%

Breakdown of Direct Cost of cyber attacks

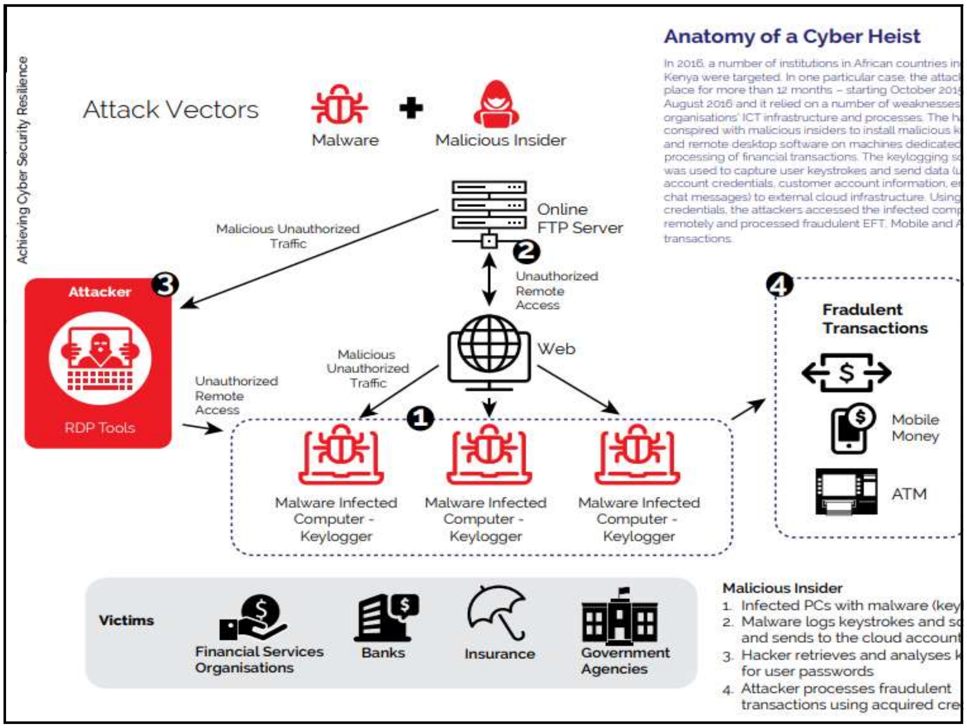
$431 Million

Compensations to Victims of Breaches	43%	$185M
Money withdrawn from victim accounts	43%	$185M
Investigation and Remediation Costs	14%	$61M

Breakdown of Indirect Cost of cyber attacks

$647 Million

Technical Controls	46%	$304M
Security Consulting Services	22%	$142M
Loss of trust in e-services	16%	$103M
Training	11%	$71M
Reputational Damage	3%	$19M
Insurance and Compliance Costs	1%	$6M



Achieving Cyber Security Resilience

Anatomy of a Cyber Heist

In 2016, a number of institutions in African countries in
Kenya were targeted. In one particular case, the attack
place for more than 12 months – starting October 2015
August 2016 and it relied on a number of weaknesses
organisations' ICT infrastructure and processes. The h
conspired with malicious insiders to install malicious k
and remote desktop software on machines dedicated
processing of financial transactions. The keylogging so
was used to capture user keystrokes and send data (u
account credentials, customer account information, e
chat messages) to external cloud infrastructure. Using
credentials, the attackers accessed the infected comp
remotely and processed fraudulent EFT, Mobile and A
transactions.

Attack Vectors
Malware
Malicious Insider
Online FTP Server
Malicious Unauthorized Traffic
2
Unauthorized Remote Access
Attacker
3
RDP Tools
Web
Malicious Unauthorized Traffic
Unauthorized Remote Access
1
Malware Infected Computer - Keylogger
Malware Infected Computer - Keylogger
Malware Infected Computer - Keylogger
4
Fradulent Transactions
Mobile Money
ATM
Victims
Financial Services Organisations
Banks
Insurance
Government Agencies

Malicious Insider

1. Infected PCs with malware (key
2. Malware logs keystrokes and sc
   and sends to the cloud account
3. Hacker retrieves and analyses k
   for user passwords
4. Attacker processes fraudulent
   transactions using acquired cre

Cybercrime

What's changed?

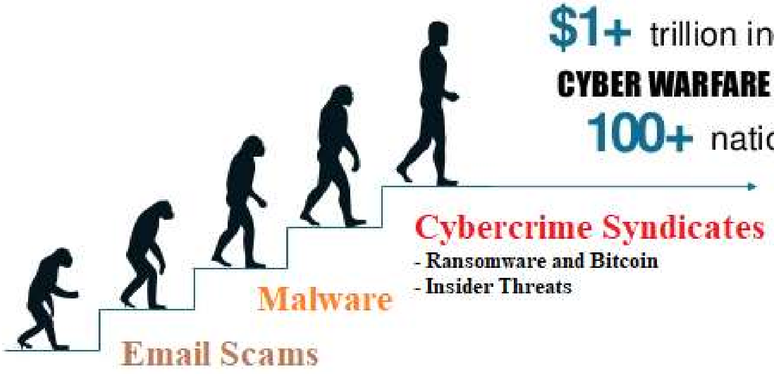
THE EVOLUTION OF THE **ADVERSARY**

CYBERCRIME NOW

$1+ trillion industry

CYBER WARFARE

100+ nations



Email Scams

Malware

Cybercrime Syndicates

- Ransomware and Bitcoin
- Insider Threats

Social Media

❑ Social networking has morphed old ways of communicating into a new electronic format. Conversations that used to be private now happen openly online in front of hundreds, or thousands, of other people.

❑ However, social media is now being weaponized across the world

Social Media

#AllEyesOnISIS announced the 2014 invasion of northern Iraq.

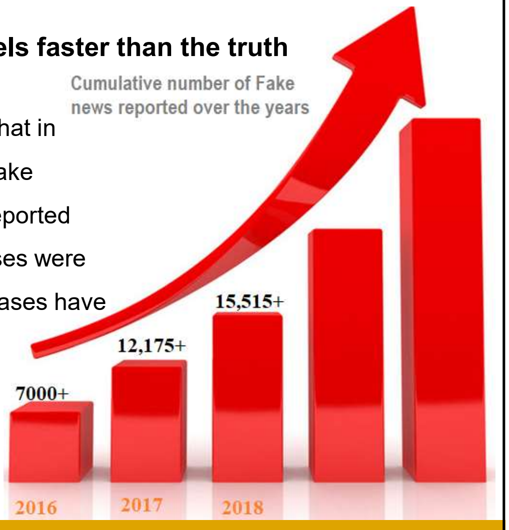
Social media has empowered ISIS in the following areas

- **Recruiting**: helping the group draw at least 30,000 foreign fighters, from some 100 countries, to the battlefields of Syria and Iraq.
- **Seeding of new franchises:** Mainly in places ranging from Libya and Afghanistan to Nigeria and Bangladesh.

Social Media

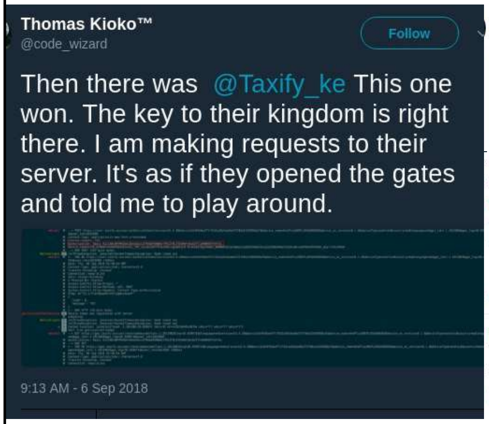
Fake news on social media travels faster than the truth

The Tanzania Police Force indicated that in 2015/2016 more than **7,000** cases of fake accounts and false information were reported while in December, a total of **5,175** cases were reported. Since January 2018, **3,340** cases have been reported to police stations.



Social Media

ICPAK Uphold Public Interest

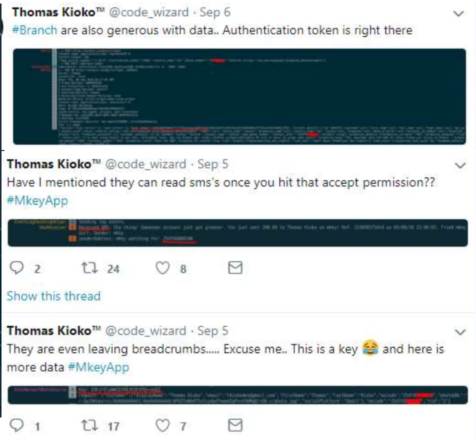


Thomas Kioko™
@code_wizard

Follow

Then there was @Taxify_ke This one won. The key to their kingdom is right there. I am making requests to their server. It's as if they opened the gates and told me to play around.

9:13 AM - 6 Sep 2018



Thomas Kioko™ @code_wizard · Sep 6
#Branch are also generous with data.. Authentication token is right there

Thomas Kioko™ @code_wizard · Sep 5
Have I mentioned they can read sms's once you hit that accept permission?? #MkeyApp

2 24 8

Show this thread

Thomas Kioko™ @code_wizard · Sep 5
They are even leaving breadcrumbs..... Excuse me.. This is a key 😂 and here is more data #MkeyApp

1 17 7

Social Media

ICPAK Uphold Public Interest

Auditors role in Social Media – Social Media Assurance

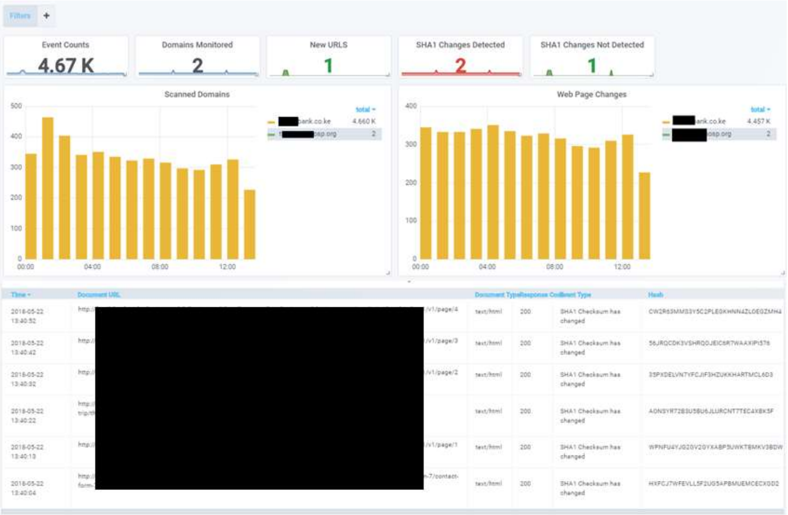
- The objective of the social media audit/assurance review is to provide management with an independent assessment relating to the effectiveness of controls over the enterprise's social media policies and processes.

Social Media

Auditors role in Social Media – Social Media Assurance

- Review of Profile information (name and URL)
- Review of changes and postings done
- Web defacement Monitoring

Social Media



Time	Document URL	Document Type	Response Code	Content Type	Hash
2018-05-22 13:40:52	http:/[redacted]/v1/page/4	text/html	200	SHA1 Checksum has changed	CW2R63MMS3Y5C2PLEGKHNN4ZL0EGZMH4
2018-05-22 13:40:42	http:/[redacted]/v1/page/3	text/html	200	SHA1 Checksum has changed	56JRQCDK3VSHRQOJEIC6R7WAAXIPI576
2018-05-22 13:40:32	http:/[redacted]/v1/page/2	text/html	200	SHA1 Checksum has changed	35PXDELVNTYFCJIF3HZUKKHARTMCL6D3
2018-05-22 13:40:22	http:/ trip/t[redacted]	text/html	200	SHA1 Checksum has changed	AONSYR72B3U5BU6JLURCNT7TECAXBK5F
2018-05-22 13:40:13	http:/[redacted]/v1/page/1	text/html	200	SHA1 Checksum has changed	WPNFU4YJG2GV2GYXABP5UWKTBMKV3BDW
2018-05-22 13:40:04	http:/ form-[redacted]n-7/contact-	text/html	200	SHA1 Checksum has changed	HXFCJ7WFEVLL5F2UG5APBMUEMCECXGD2

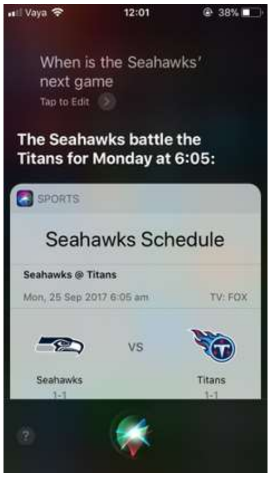
Artificial Intelligence

Artificial Intelligence is revolutionizing the way enterprises are doing business.

- Augment existing abilities and make us better at what we do.
- Give us better vision, better understanding, of the enterprise data collected

Artificial Intelligence

SIRI


Vaya 12:01 38%

When is the Seahawks' next game

Tap to Edit

The Seahawks battle the Titans for Monday at 6:05:

SPORTS

Seahawks Schedule

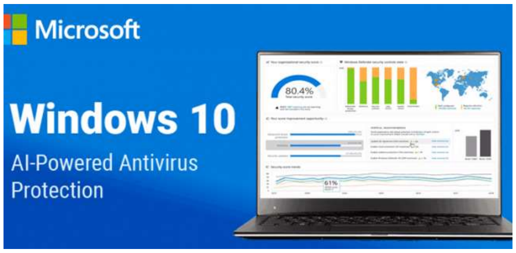
Seahawks @ Titans

Mon, 25 Sep 2017 6:05 am TV: FOX

Seahawks VS Titans

1-1 1-1

Alexa's skills



Cloud and IoT

❑ Cloud computing has become the de facto platform on which enterprises are fueling digital transformations and modernizing IT portfolios.

Outlook

Gmail

Cloud and IoT

Smart Farms in Africa

These farms use big data and the Internet of Things to provide insights into current and predicted water and soil moisture levels to farmers and water service providers.

Smart Meters

Records consumption of electric energy and communicates the information to the electricity supplier for monitoring and billing

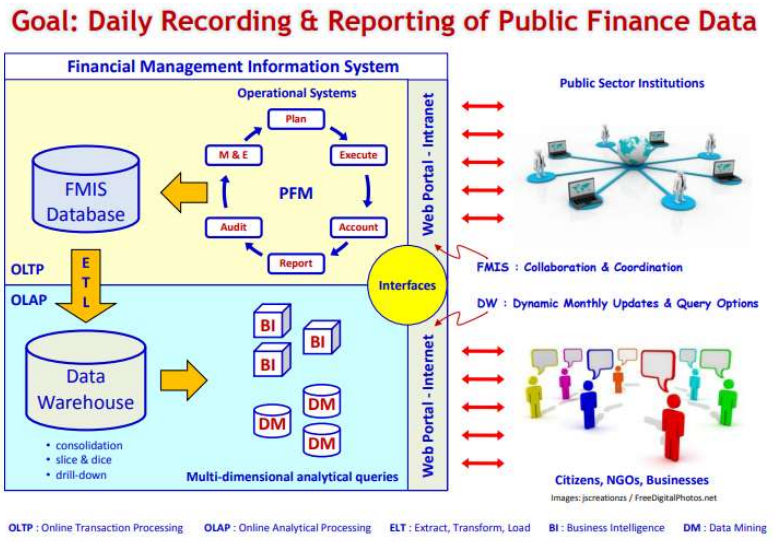
Wearable activity tracking devices like those made by Fitbit were one of the hottest gifts this past holiday season

Analytics

Key Areas are

1. **Identification of Threats**
2. **Correlation of multiple data sources - T**he biggest problem for analysts is how to manage the volume, velocity, and complexity of data generated by the myriad of IT and security tools in an organization.
3. **Behavioral Analysis**

Analytics -IFMIS

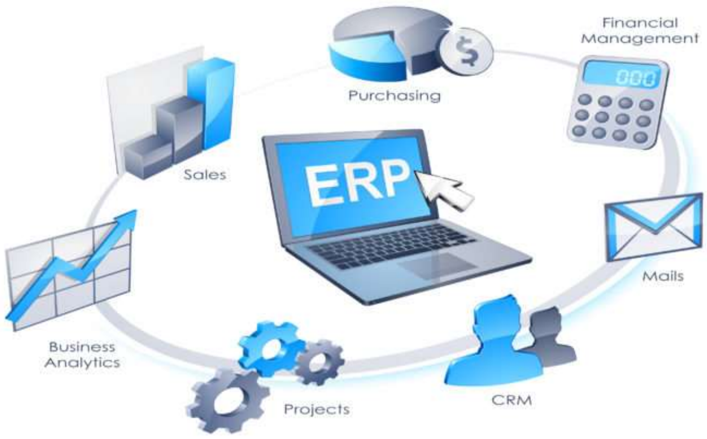

Goal: Daily Recording & Reporting of Public Finance Data

Financial Management Information System
Operational Systems
Plan
Execute
Account
Report
Audit
M & E
PFM
FMIS Database
OLTP
E T L
OLAP
Data Warehouse
• consolidation
• slice & dice
• drill-down
BI
BI
BI
DM
DM
DM
Multi-dimensional analytical queries
Interfaces
Web Portal - Intranet
Web Portal - Internet
Public Sector Institutions
FMIS : Collaboration & Coordination
DW : Dynamic Monthly Updates & Query Options
Citizens, NGOs, Businesses

Images: jscreationzs / FreeDigitalPhotos.net

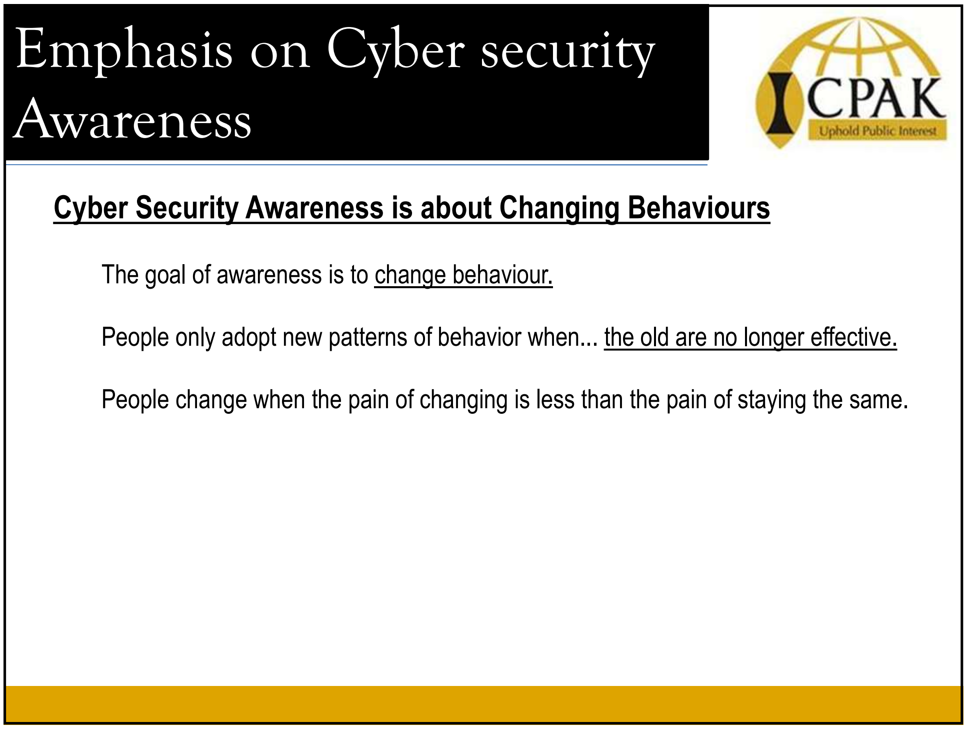
OLTP : Online Transaction Processing OLAP : Online Analytical Processing ELT : Extract, Transform, Load BI : Business Intelligence DM : Data Mining

Analytics - ERP



Why Cybercrime

- We don’t know ourselves
- We don’t know our enemies
- We don’t learn from (others/our) mistakes
- Hackers are getting smarter?
- Users are more vulnerable?



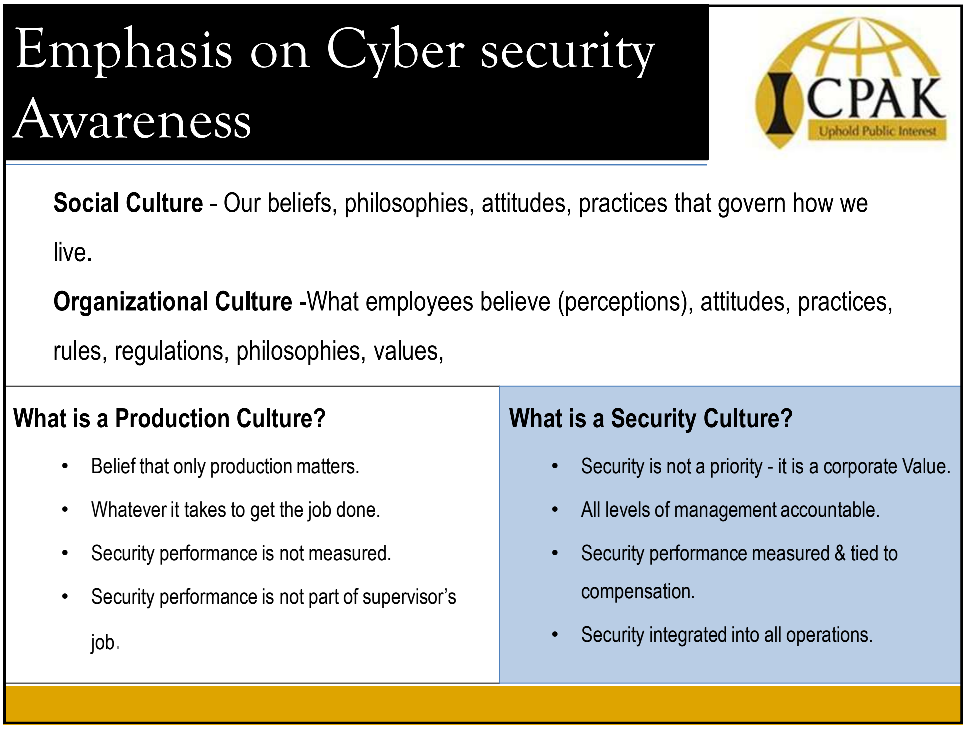
Emphasis on Cyber security Awareness

Cyber Security Awareness is about Changing Behaviours

The goal of awareness is to change behaviour.

People only adopt new patterns of behavior when... the old are no longer effective.

People change when the pain of changing is less than the pain of staying the same.



Emphasis on Cyber security Awareness

Social Culture - Our beliefs, philosophies, attitudes, practices that govern how we live.

Organizational Culture -What employees believe (perceptions), attitudes, practices, rules, regulations, philosophies, values,

What is a Production Culture?

- Belief that only production matters.
- Whatever it takes to get the job done.
- Security performance is not measured.
- Security performance is not part of supervisor's job.

What is a Security Culture?

- Security is not a priority - it is a corporate Value.
- All levels of management accountable.
- Security performance measured & tied to compensation.
- Security integrated into all operations.

Emphasis on Cyber security Awareness

- ❑ Board members focus on OVERSIGHT role alone.
- ❑ Board-level capabilities for strategic thinking and governance in this area **fail to keep pace** with both the technological risks and the solutions that new innovations provide.

- ❑ Board members take a **PROACTIVE OVERSIGHT** role.
- ❑ Being proactive and resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and proactively mitigating risks.

The Executive Committee

Regulatory Requirements for Senior Management

1. Implement the board approved cybersecurity strategy, policy and framework.
2. Understand cyber organizational scope as well as identify cyber threats, critical business processes and assets.
3. Continuously improve collection, analysis, and reporting of cybercrime information.
4. Ensure timely and regular reporting to the board on the cyber risk status of the institution.
5. Provide regular reports of the institution’s cybersecurity posture to the board.

Internal Audit

Regulatory Requirements for Internal Audit

1. Continuously review and report on cyber risks and controls of the ICT systems within the institutions and other related third-party connections.
2. Assess both the design and effectiveness of the cybersecurity framework implemented.
3. Conduct regular independent threat and vulnerability assessment tests.
4. Report to the board the findings of the assessments.
5. Conduct comprehensive penetration tests.

The Audit Committee

CORE CYBER SECURITY FUNCTIONS: KEY QUESTIONS

ANTICIPATE

What are our risks and how do we mitigate them?

DETECT

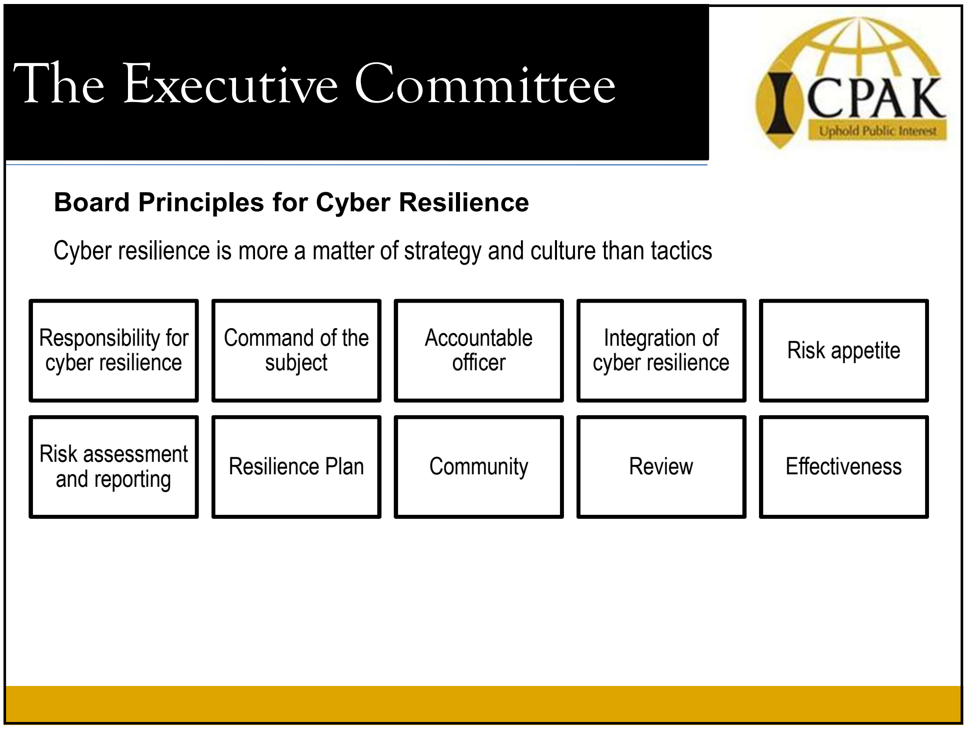
Should these risks materialize, are we able to detect them?

RESPOND

What would we do if we were hacked today?

CONTAIN

What strategies do we have in place to ensure damage issues don't reoccur?

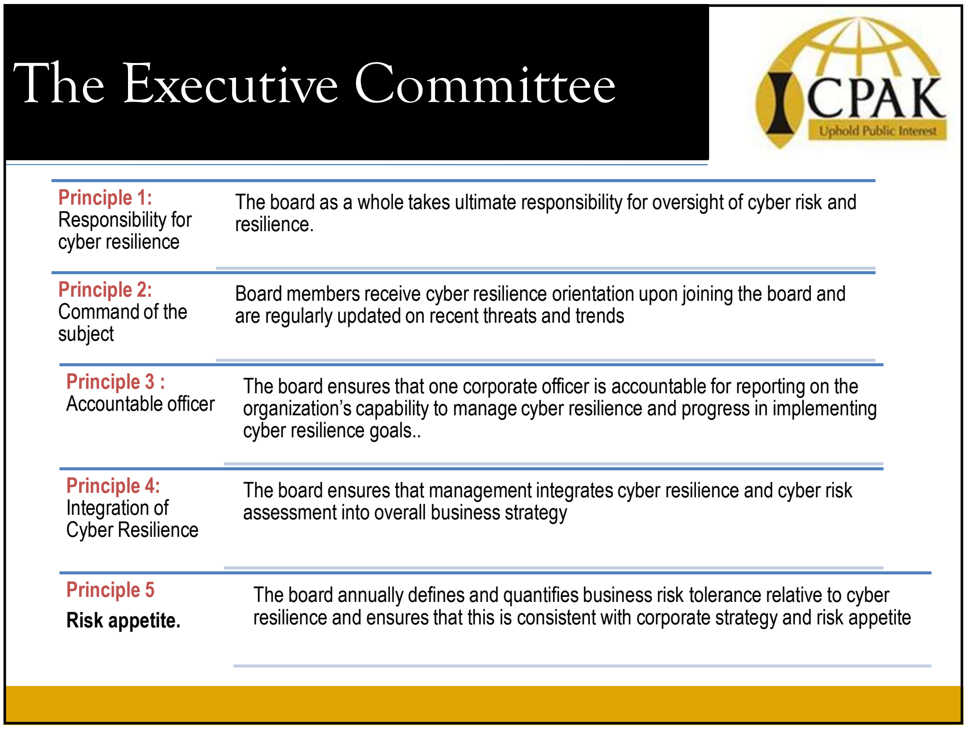


The Executive Committee

Board Principles for Cyber Resilience

Cyber resilience is more a matter of strategy and culture than tactics

Responsibility for cyber resilience	Command of the subject	Accountable officer	Integration of cyber resilience	Risk appetite
Risk assessment and reporting	Resilience Plan	Community	Review	Effectiveness



The Executive Committee

Principle 1: Responsibility for cyber resilience	The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience.
Principle 2: Command of the subject	Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends
Principle 3 : Accountable officer	The board ensures that one corporate officer is accountable for reporting on the organization’s capability to manage cyber resilience and progress in implementing cyber resilience goals..
Principle 4: Integration of Cyber Resilience	The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy
Principle 5 **Risk appetite.**	The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite

The Executive Committee

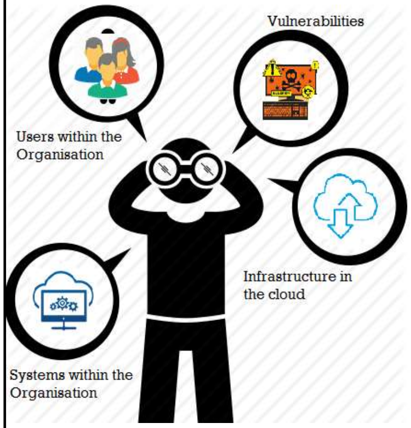
Principle 6 **Risk assessment and reporting.**	The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings
Principle 7 **Resilience plans.**	The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans.
Principle 8 **Community.**	The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.
Principle 9 **Review.**	The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.
Principle 10: **Effectiveness.**	The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement

The Cyber Risk reporting problem?

Many organisations are struggling to confirm their cyber security posture :

1. Are we spending an appropriate amount on securing our business and infrastructure?
2. Is the investment going to the more critical areas of risk, and is it having the desired effect?
3. Perhaps most critically, we lack a clear means to answer the deceptively difficult question “How secure are we?”

Cyber security Resilience and Visibility Statement


Vulnerabilities
Users within the Organisation
Infrastructure in the cloud
Systems within the Organisation

'the cyber security balance sheet'

Reports the level of visibility that management have into cyber security posture of the organisation

It is based on the cyber security resources, investments and details of a company security posture on a specific day.

This is a snapshot of what the company looked like at a certain time in history.

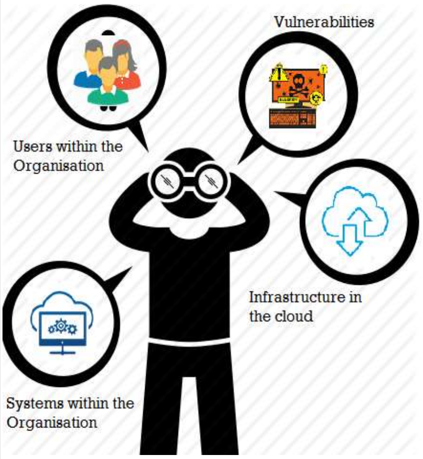
Cyber security Resilience and Visibility Statement

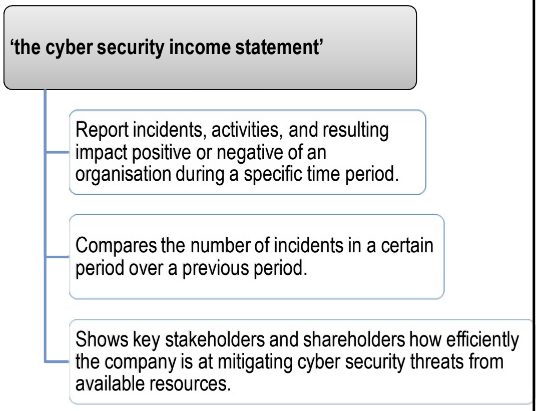
The Cyber Security Resilience and Visibility Statement

Visibility as at March 30, 2018

Control Devices	Year	Existence	Completeness	Timeliness	Reporting	Visibility Score
Asset Management						
Hardware and Software (Databases, Servers, Laptops, Routers)	2018	80%	80%	60%	60%	70%
	2017	70%	70%	60%	50%	63%
User Management						
1) Employees 2) Vendors 3) System Accounts	2018	60%	50%	40%	30%	45%
	2017	30%	30%	25%	25%	28%
Breach Scenarios						
1) Insider Threats 2) External Threats	2018	70%	66%	70%	70%	69%
	2017	40%	40%	33%	40%	38%
Monitoring and Analysis						
1) Logging 2) Static Metric Analysis 3) Threshold Analysis 4) Profiling 5) Correlation	2018	80%	78%	71%	78%	77%
	2017	68%	63%	63%	40%	59%

Cyber security Resilience and Visibility Statement

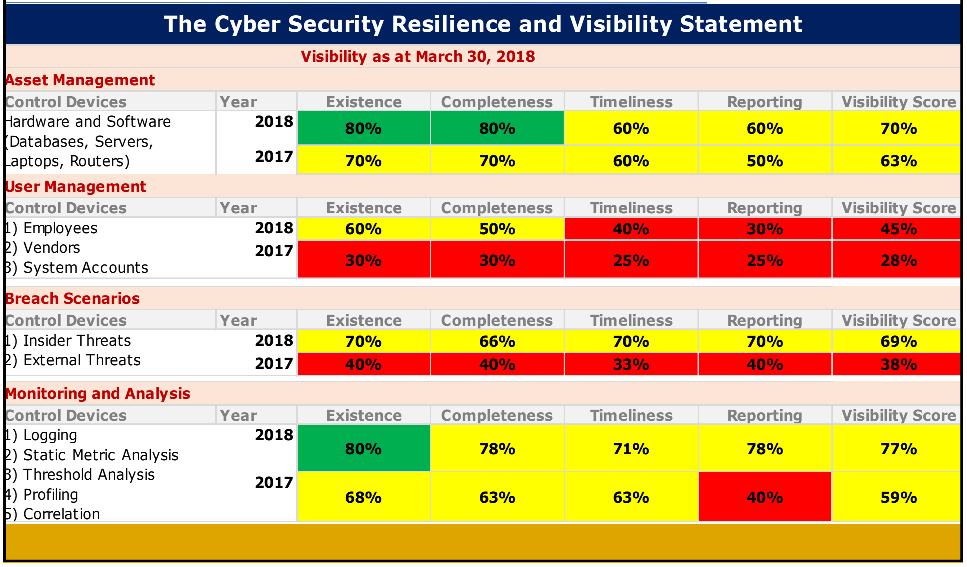

Users within the Organisation
Vulnerabilities
Infrastructure in the cloud
Systems within the Organisation



‘the cyber security income statement’

- Report incidents, activities, and resulting impact positive or negative of an organisation during a specific time period.
- Compares the number of incidents in a certain period over a previous period.
- Shows key stakeholders and shareholders how efficiently the company is at mitigating cyber security threats from available resources.

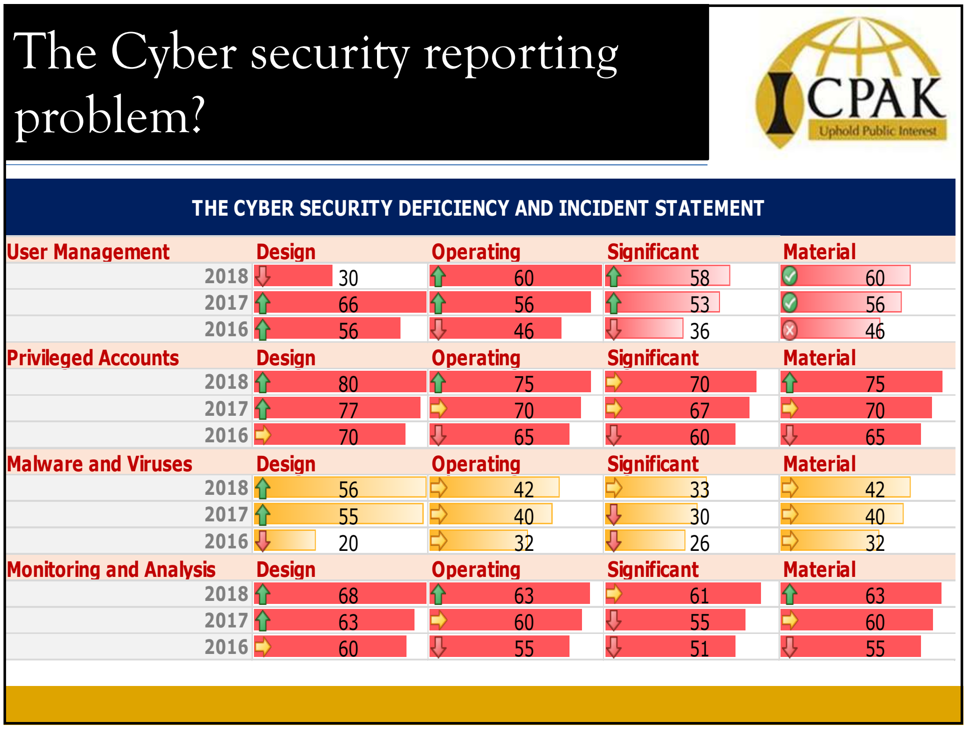
The Cyber security reporting problem?



The Cyber Security Resilience and Visibility Statement

Visibility as at March 30, 2018

Control Devices	Year	Existence	Completeness	Timeliness	Reporting	Visibility Score
Asset Management						
Hardware and Software (Databases, Servers, Laptops, Routers)	**2018**	**80%**	**80%**	**60%**	**60%**	**70%**
	2017	**70%**	**70%**	**60%**	**50%**	**63%**
User Management						
1) Employees 2) Vendors 3) System Accounts	**2018**	**60%**	**50%**	**40%**	**30%**	**45%**
	2017	**30%**	**30%**	**25%**	**25%**	**28%**
Breach Scenarios						
1) Insider Threats 2) External Threats	**2018**	**70%**	**66%**	**70%**	**70%**	**69%**
	2017	**40%**	**40%**	**33%**	**40%**	**38%**
Monitoring and Analysis						
1) Logging 2) Static Metric Analysis 3) Threshold Analysis 4) Profiling 5) Correlation	**2018**	**80%**	**78%**	**71%**	**78%**	**77%**
	2017	**68%**	**63%**	**63%**	**40%**	**59%**



The Cyber security reporting problem?

ICPAK Uphold Public Interest

THE CYBER SECURITY DEFICIENCY AND INCIDENT STATEMENT

User Management	Design	Operating	Significant	Material
2018	↓ 30	↑ 60	↑ 58	✓ 60
2017	↑ 66	↑ 56	↑ 53	✓ 56
2016	↑ 56	↓ 46	↓ 36	✗ 46
Privileged Accounts	**Design**	**Operating**	**Significant**	**Material**
2018	↑ 80	↑ 75	⇨ 70	↑ 75
2017	↑ 77	⇨ 70	⇨ 67	⇨ 70
2016	⇨ 70	↓ 65	↓ 60	↓ 65
Malware and Viruses	**Design**	**Operating**	**Significant**	**Material**
2018	↑ 56	⇨ 42	⇨ 33	⇨ 42
2017	↑ 55	⇨ 40	↓ 30	⇨ 40
2016	↓ 20	⇨ 32	↓ 26	⇨ 32
Monitoring and Analysis	**Design**	**Operating**	**Significant**	**Material**
2018	↑ 68	↑ 63	⇨ 61	↑ 63
2017	↑ 63	⇨ 60	↓ 55	⇨ 60
2016	⇨ 60	↓ 55	↓ 51	↓ 55