Technology and Vulnerability to Cyber Attacks: Mitigation Measures

Presentation by:

Raymond Bett
CEO, Salaam Technology Limited

Thursday, 24th October 2019

Presentation agenda

- The changing Landscape
- Traditional Crime Vs Cybercrime
- Common attack types & Vectors
- Types of Cybercriminals
- Mobile Payments
- Social Media
- Cloud Computing
- Consumerization of IT and Internet of Things
- Cybercrime Challenges and Impact
- Mitigation Measures

Raymond Bett

- Founder and CEO of Salaam Technology Limited.
- Over 10 years Information Assurance, cybersecurity, Forensics, ICT Audit
- Holder of BSC in Electrical and Information Engineering, Cybersecurity Fundamentals CSX, CISA, CISM, CRISC, CEH, CPA Certifications
- President of the ISACA Kenya Chapter, Member of ICPAK and EC-Council.
- Previously worked for Safaricom Limited and PricewaterhouseCoopers (PwC)

Salaam

Headlines

Cyber Threat	Jan-Mar 19	Apr-Jun 19
Malware	8,883,862	21,137,458
DDOS/Botnet	1,133,893	2,353,460
Web Application Attacks	1,222,237	3,084,687
System vulnerabilities	13,319	28,597
Totals	11,253,311	26,604,202

08 Sep 2019

Kenyan(s) hack into London company's systems and import excavators worth sh. 43m.

04:45 A+ A- Print Email

Latest Kenya Power postpaid billing scandal linked to cybercrime

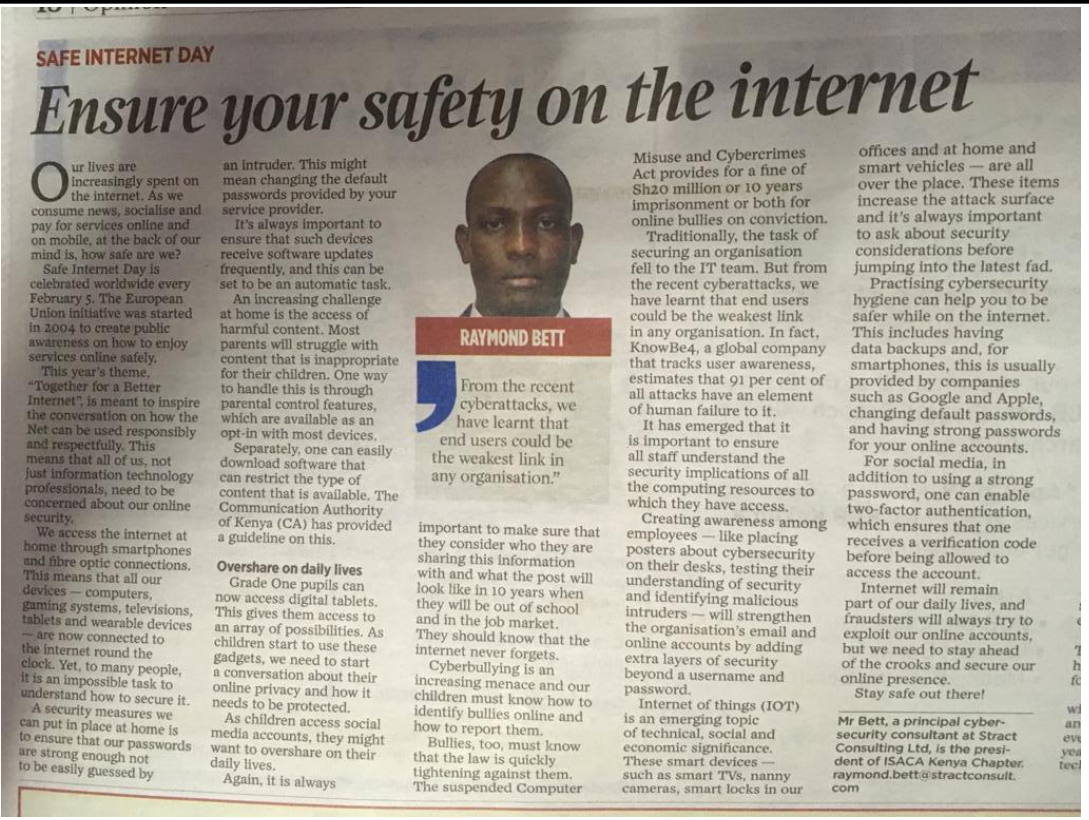
By Citizen Reporter For Citizen Digital

Published on: June 29, 2019 08:21 (EAT)

The Changing Landscape

Mobile Devices

The changing landscape



SAFE INTERNET DAY

Ensure your safety on the internet

Our lives are increasingly spent on the internet. As we consume news, socialise and pay for services online and on mobile, at the back of our mind is, how safe are we?

Safe Internet Day is celebrated worldwide every February 5. The European Union initiative was started in 2004 to create public awareness on how to enjoy services online safely.

This year's theme, "Together for a Better Internet", is meant to inspire the conversation on how the Net can be used responsibly and respectfully. This means that all of us, not just information technology professionals, need to be concerned about our online security.

We access the internet at home through smartphones and fibre optic connections. This means that all our devices — computers, gaming systems, televisions, tablets and wearable devices — are now connected to the internet round the clock. Yet, to many people, it is an impossible task to understand how to secure it.

A security measures we can put in place at home is to ensure that our passwords are strong enough not to be easily guessed by an intruder. This might mean changing the default passwords provided by your service provider.

It's always important to ensure that such devices receive software updates frequently, and this can be set to be an automatic task.

An increasing challenge at home is the access of harmful content. Most parents will struggle with content that is inappropriate for their children. One way to handle this is through parental control features, which are available as an opt-in with most devices.

Separately, one can easily download software that can restrict the type of content that is available. The Communication Authority of Kenya (CA) has provided a guideline on this.

Overshare on daily lives

Grade One pupils can now access digital tablets. This gives them access to an array of possibilities. As children start to use these gadgets, we need to start a conversation about their online privacy and how it needs to be protected.

As children access social media accounts, they might want to overshare on their daily lives.

Again, it is always important to make sure that they consider who they are sharing this information with and what the post will look like in 10 years when they will be out of school and in the job market. They should know that the internet never forgets.

Cyberbullying is an increasing menace and our children must know how to identify bullies online and how to report them.

Bullies, too, must know that the law is quickly tightening against them. The suspended Computer Misuse and Cybercrimes Act provides for a fine of Sh20 million or 10 years imprisonment or both for online bullies on conviction.

Traditionally, the task of securing an organisation fell to the IT team. But from the recent cyberattacks, we have learnt that end users could be the weakest link in any organisation. In fact, KnowBe4, a global company that tracks user awareness, estimates that 91 per cent of all attacks have an element of human failure to it.

It has emerged that it is important to ensure all staff understand the security implications of all the computing resources to which they have access.

Creating awareness among employees — like placing posters about cybersecurity on their desks, testing their understanding of security and identifying malicious intruders — will strengthen the organisation's email and online accounts by adding extra layers of security beyond a username and password.

Internet of things (IOT) is an emerging topic of technical, social and economic significance. These smart devices — such as smart TVs, nanny cameras, smart locks in our offices and at home and smart vehicles — are all over the place. These items increase the attack surface and it's always important to ask about security considerations before jumping into the latest fad.

Practising cybersecurity hygiene can help you to be safer while on the internet. This includes having data backups and, for smartphones, this is usually provided by companies such as Google and Apple, changing default passwords, and having strong passwords for your online accounts.

For social media, in addition to using a strong password, one can enable two-factor authentication, which ensures that one receives a verification code before being allowed to access the account.

Internet will remain part of our daily lives, and fraudsters will always try to exploit our online accounts, but we need to stay ahead of the crooks and secure our online presence.

Stay safe out there!

RAYMOND BETT

"From the recent cyberattacks, we have learnt that end users could be the weakest link in any organisation."

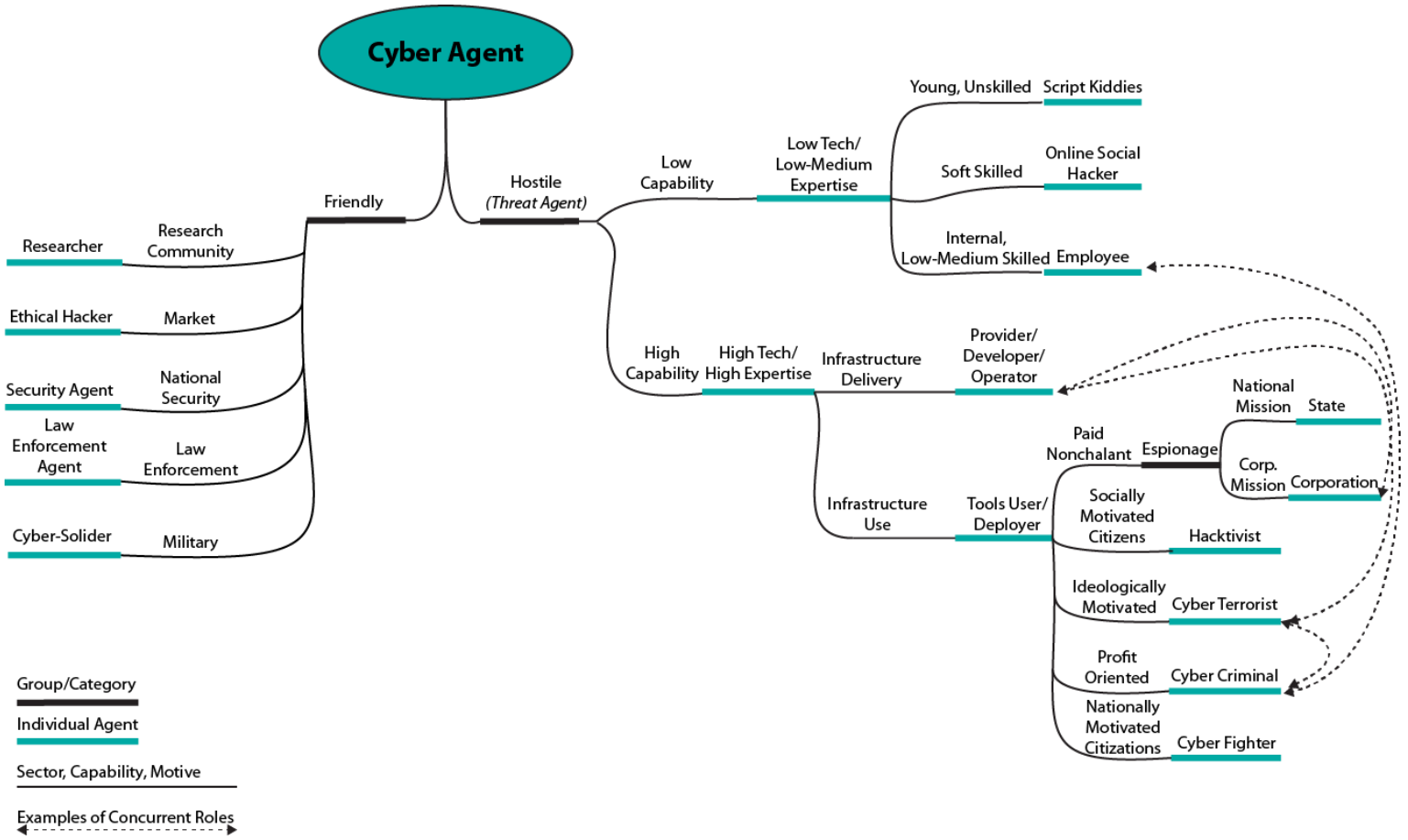
Mr Bett, a principal cyber-security consultant at Stract Consulting Ltd, is the president of ISACA Kenya Chapter. raymond.bett@stractconsult.com

- Incomplete implementation of systems
- Unlicensed systems
- Insecure connectivity with third parties for mobile, ATM, Agency banking
- Fraud committed by insiders or through collusion between insiders and professional cybercriminals
- Inadequate disaster recovery mechanism
- Inadequate awareness of users on cybercrime
- Increasing spotlight from regulators, CBK, SASRA, IRA, CMA
- New Laws

Traditional Crime Vs Cybercrime

Burglary	Hacking
Deceptive Callers	Phishing
Extortion	Ransomware
Impersonation	Identity Theft
Stalking	Cyberbullying/Trolling

Types of Cybercriminals



Source: ENISA Threat Landscape

Types of Cybercriminals

Types of Cybercriminals

- Young and blessed with merely basic hacking skills,
- Curious, keen to learn, and impress peers
- Might not understand the consequences or illegality of their actions.

Script Kiddie

Types of Cybercriminals

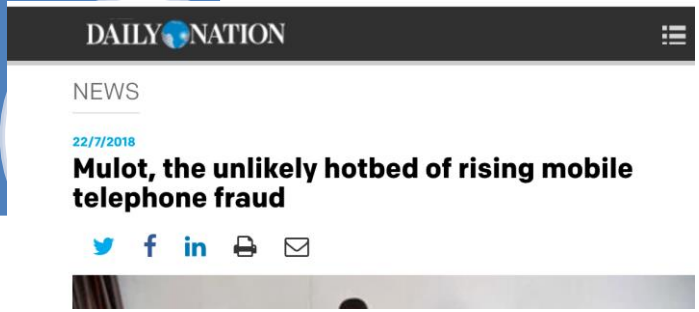
- A burning cause and takes political, religious or social cause on to the Internet. The Activist targets adversaries with data theft, reputational damage and the defacement of web sites and social media accounts E.g. WikiLeaks, local bloggers

Hacktivist

Types of Cybercriminals

- They work at what looks like a legitimate ‘8 to 5’ job – but it’s anything other than law abiding. The Professional has built a career out of committing or supporting cyber crime. They target customers of financial institution through social engineering.

Professional


DAILY NATION

NEWS

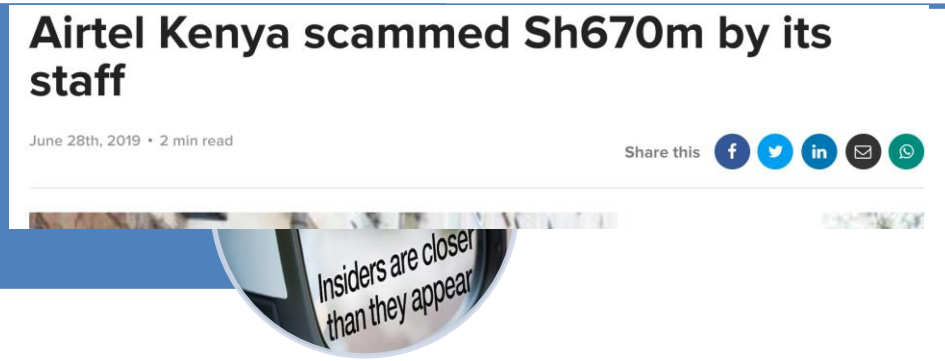
22/7/2018

Mulot, the unlikely hotbed of rising mobile telephone fraud

Types of Cybercriminals

- These attackers are considered to be the highest risk.
- Could be current employees, former employees, employees of related organizations.
- The threat comes in because they know how the company operates, which are the weak points and so on.

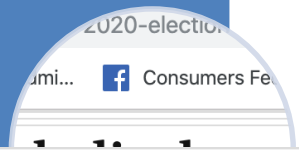
Insiders



Types of Cybercriminals

- Responsible for highly targeted attacks carried out by extremely organized state-sponsored groups.
- Their technical skills are deep and they have access to vast computing resources.

Nation State Actor



Facebook discloses operations by Russi and Iran to meddle in 2020 election

Ubiquity of Mobile

Growth of Mobile Payments

- M-PESA 26.9M, Airtel Money 3.7M, Equitel 1.8M Subscribers

Growth of APIs

- Instantaneous connection between Mobile payments and traditional banking platforms.
- Bigger role played by intermediaries “FinTech's”

Mobile Payment Risks

- Money Laundering/Terrorist financing
- Fraud to Customers/Agents
- Insider fraud
- Cyber-attacks
- Service Availability

Mobile Payment controls

- System Controls
  - User Access rights, SoD, Multi Factor Authentication, Customer limits enforcement, Cyber-security and network protection
- Operational Controls
  - KYC validation, Training of partners/customers, Reversals process, Whistleblowing channels, Revenue reconciliations

Mobile Payment controls

Continuous reviews

- Reconciliation of e-money to cash money
- Vulnerability/Penetration tests
- User access monitoring
- Transaction/logs monitoring
- Business Continuity testing
- Independent audits

Social Media

Benefits of Social Media are:

- Increasing brand recognition
- Increasing sales
- Immediately connecting with customers
- Exploring new advertising channels
- Monitoring competition
- Researching prospective employees

Social Media Risks

- Data Privacy Concerns
- Negative brand image
- Data loss
- Distribution of malware
- Imposter accounts

Social Media Controls

- Social Media Policy
- Social Media Training and Awareness
- Social Media Alignment With Business Processes
- Social Media Brand Protection
- Social Media Monitoring
- Social Media Branding Enforcement
- Access Management of Social Media Data

Cloud Computing

Cloud computing has the advantage of lower IT costs, less complex infrastructure, better flexibility and increased operating efficiencies but its challenges are:

- Data privacy in the cloud: inability of the cloud provider to enforce data privacy guidelines
- Data might be shared with other companies
- Data stored in different jurisdiction with different set of laws and regulations
- Cloud service availability

Cloud Computing

To manage risk in the cloud the following should be addressed:

- Contractual agreements:
- Access controls
- Certification and third-party audits:
- Compliance requirements
- Availability, reliability, and resilience
- Back-up and recovery
- Decommissioning

Consumerization of IT

Consumerization of IT is the reorientation of technologies and services designed around the individual end user. Examples include:

- Smart devices such as smartphones and tablets
- Bring Your Own Device (BYOD) strategies
- New, freely available applications and services

Consumerization of IT

PROS

- Shifts costs to user
- Worker satisfaction
- More frequent hardware upgrades
- Cutting-edge technology with the latest features and capabilities

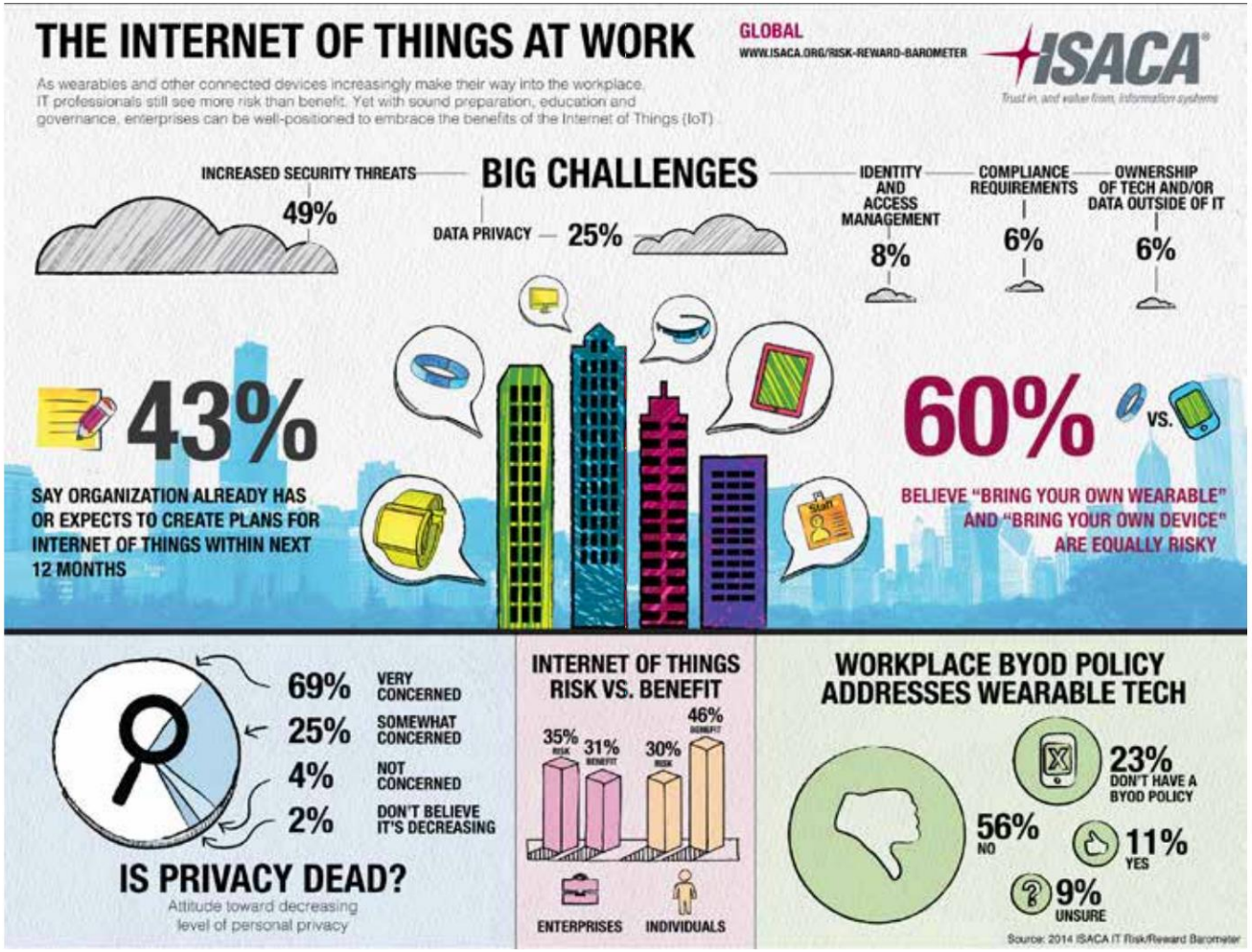
CONS

- IT loss of control
- Security risk
- Acceptable Use Policy difficult to enforce
- Unclear compliance and ownership of data

Internet of Things

IoT is a world where virtually everything is imbued with one or more tiny computers or smart sensors, all transmitting a flow of data onto the Internet.

Internet of Things



Internet of Things

The risks to IoT are:

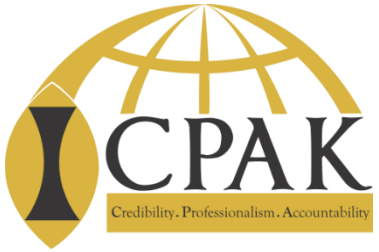
- Insufficient testing and updating
- Brute-forcing and the issue of default passwords
- IoT malware and ransomware
- Data security and privacy concerns (mobile, web, cloud)
- Home Invasions
- Insecure communication
- Device updates and Device management

Internet of Things

Controls expected on IoT are:

- Identify information
- Prioritize the devices
- Evaluate data loss risk
- Evaluate IoT access risk
- Perform IoT incident response planning
- Formulate a big data strategy to manage the vast amount of IoT data generated
- Devise policies for privacy of sensor data
- Protect IoT devices

Mitigation of cyber attacks



- Organizational risk assessment
- Cybersecurity framework, strategy and policies
- Investment in human resources and tools
- Cybersecurity incident management
- Cyber security awareness and training
- Regular and independent compliance audits

Organizational risk assessment

Asset vulnerabilities are identified and documented.

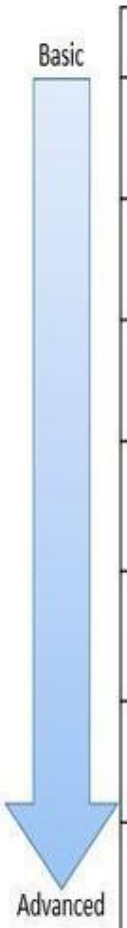
Threats, both internal and external, are identified and documented.

Potential business impacts and likelihoods are identified.

Threats, vulnerabilities, likelihoods and impacts are used to determine risk.

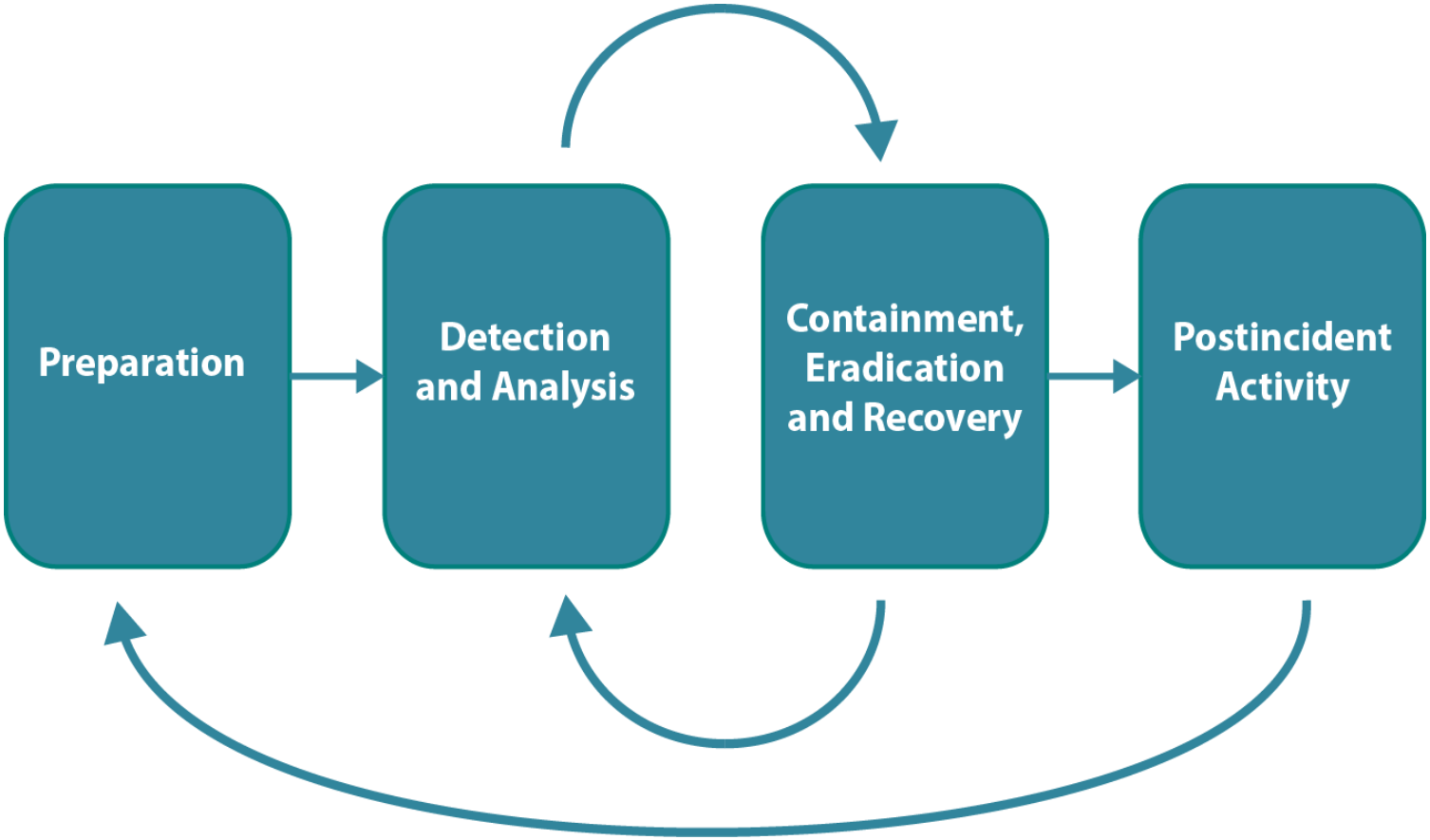
Risk responses are identified and prioritized.

Cybersecurity Investment



Security Aspect	Initial	Developing	Defined	Managed	Optimised
Patch Management and Anti-Virus	Inconsistent, Automatic updates, No reporting	Some automation & reporting	Documented & consistently applied	Measured and Reported. Enforced by end-point management tools	Continuous improvement and innovation
Firewalls & Network Segmentation	Simple firewall at internet boundary, ad hoc use of desktop firewalls	Dedicated firewall appliance and/or DMZ	Multiple firewalls and network segmentation	Centralised firewall configuration mgmt.	Continuous improvement and innovation
Identity & Access Management	Ad hoc with no process	Domain users & computers, some access restrictions / structure	Documented repeatable change control processes and JML processes	Analysis, visualisation and reporting tools	Continuous improvement and innovation
Asset and Configuration Management	None	Register of assets and deployment documentation	Asset discovery and reporting	Configuration Change Management and License Management tools deployed	Continuous improvement and innovation
Information Classification and Protection	None	Ad hoc file / disk encryption, inconsistent visual labelling	Structured & unstructured data classification, defined meta-data / templates	Discovery, Data Loss Prevention / Rights Mgmt.	Continuous improvement and innovation
Monitor, Alert and Incident Response	None	Some logging, inconsistent monitoring	Basic SIEM deployed Embryonic continuity plans	SIEM tools integrated with most areas. Regular reviews, response and recovery tests	Continuous improvement and innovation
Risk Management and Governance	None	Ad hoc risk assessments, developing security policies	Regular risk assessments and mitigation planning, ad hoc awareness training	Regular policy reviews. Training and compliance tracking	Continuous improvement and innovation

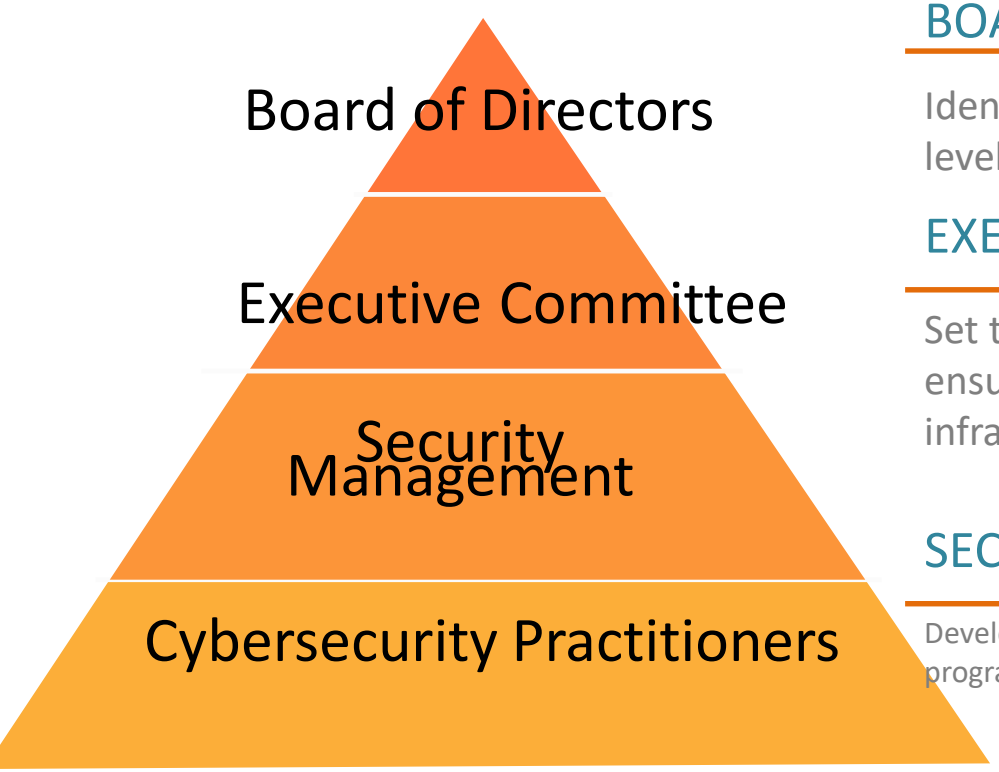
Incident Response Phases



Training and Awareness

- All users are informed and trained.
- Privileged users understand roles and responsibilities.
- Third-party stakeholders (e.g., suppliers) understand roles and responsibilities.
- Senior executives understand roles and responsibilities.
- Physical and information security personnel understand roles and responsibilities.

Mitigation - Governance



BOARD OF DIRECTORS

Identify key assets and verify that protection levels and priorities are appropriate

EXECUTIVE COMMITTEE

Set the tone for cybersecurity management and ensure that necessary functions, resources and infrastructure are available and properly utilized

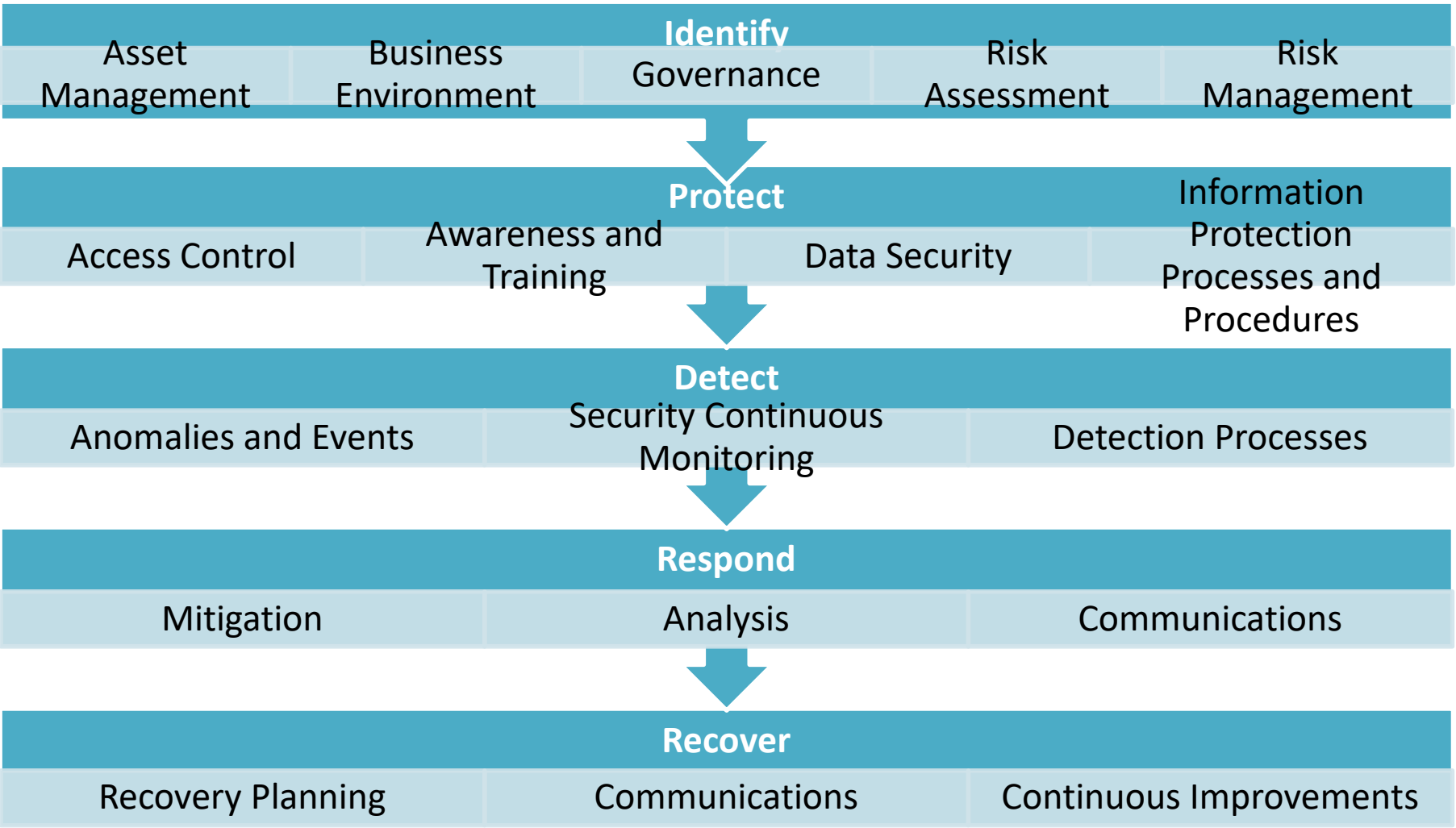
SECURITY MANAGEMENT

Develop security and risk mitigation strategies, implement security programs and manage incidents and remediation

CYBERSECURITY PRACTITIONERS

Design, implement and manage processes and technical controls and respond to events and incidents

Cyber Resilience



Questions?

Raymond Bett

+254 720 983 411

raymond.bett@salaam.ke

www.salaam.ke