< Cyber Resilience
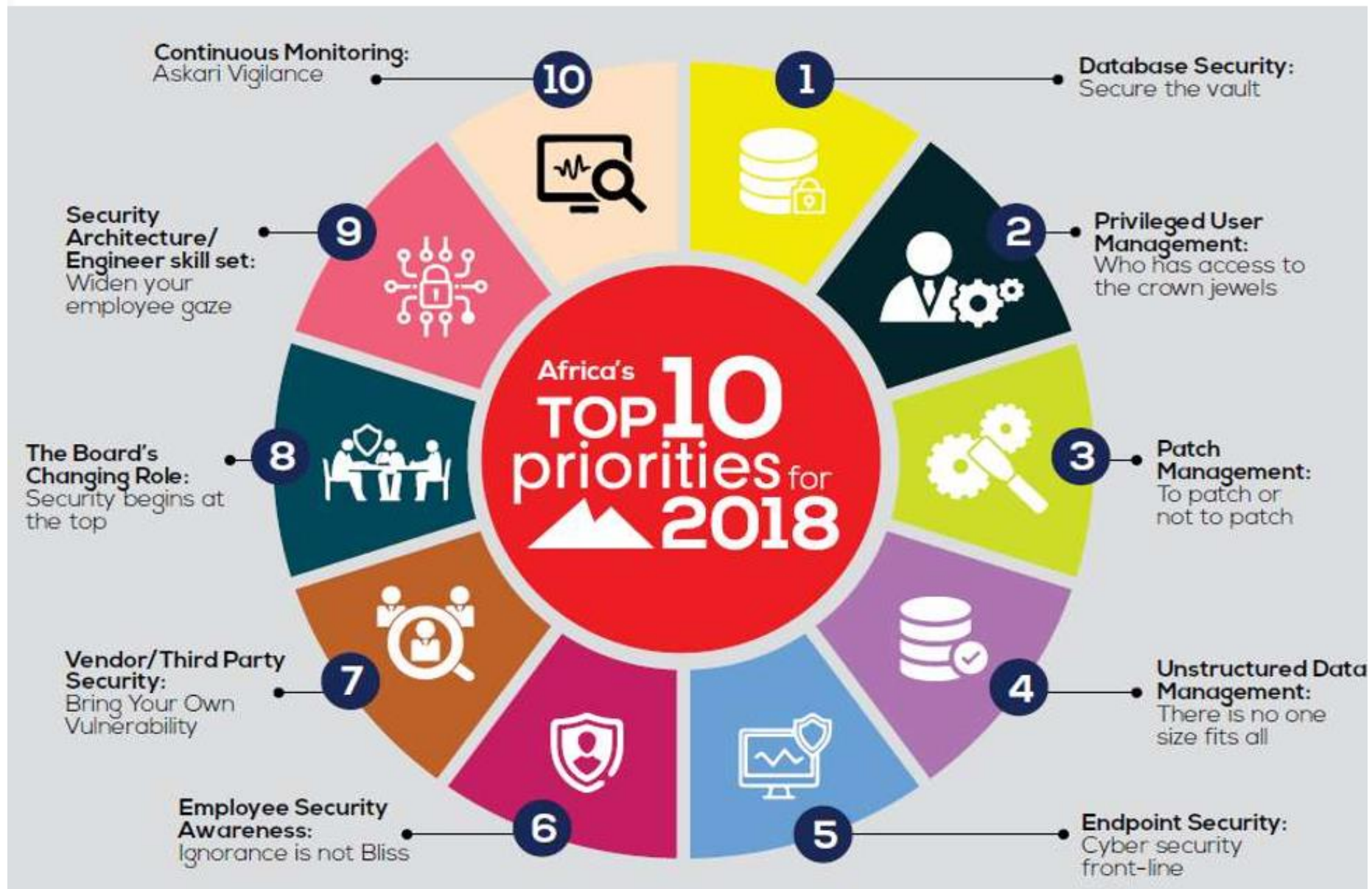
—

Building a Comprehensive Cybersecurity Plan >

Question is not
'**if**'
but
'**When**'
You Get HACKED

Who Am I

- Dr. Bright Gameli Mawudor,PhD

- Head of Cyber Security Services, Internet Solutions
  Kenya

- Founder of Africahackon

- www.is.co.ke & www.brightgameli.com

Top 10 Cyber Security Priorities for 2018

Continuous Monitoring:
Askari Vigilance

Security Architecture/ Engineer skill set:
Widen your employee gaze

The Board's Changing Role:
Security begins at the top

Vendor/Third Party Security:
Bring Your Own Vulnerability

Employee Security Awareness:
Ignorance is not Bliss

Database Security:
Secure the vault

Privileged User Management:
Who has access to the crown jewels

Patch Management:
To patch or not to patch

Unstructured Data Management:
There is no one size fits all

Endpoint Security:
Cyber security front-line

Africa's **TOP 10 priorities** for **2018**

Common Security Problems to Organizations

Hackers have all the time in the world to lay foundations for crippling attacks, which means you have no time in becoming less vulnerable
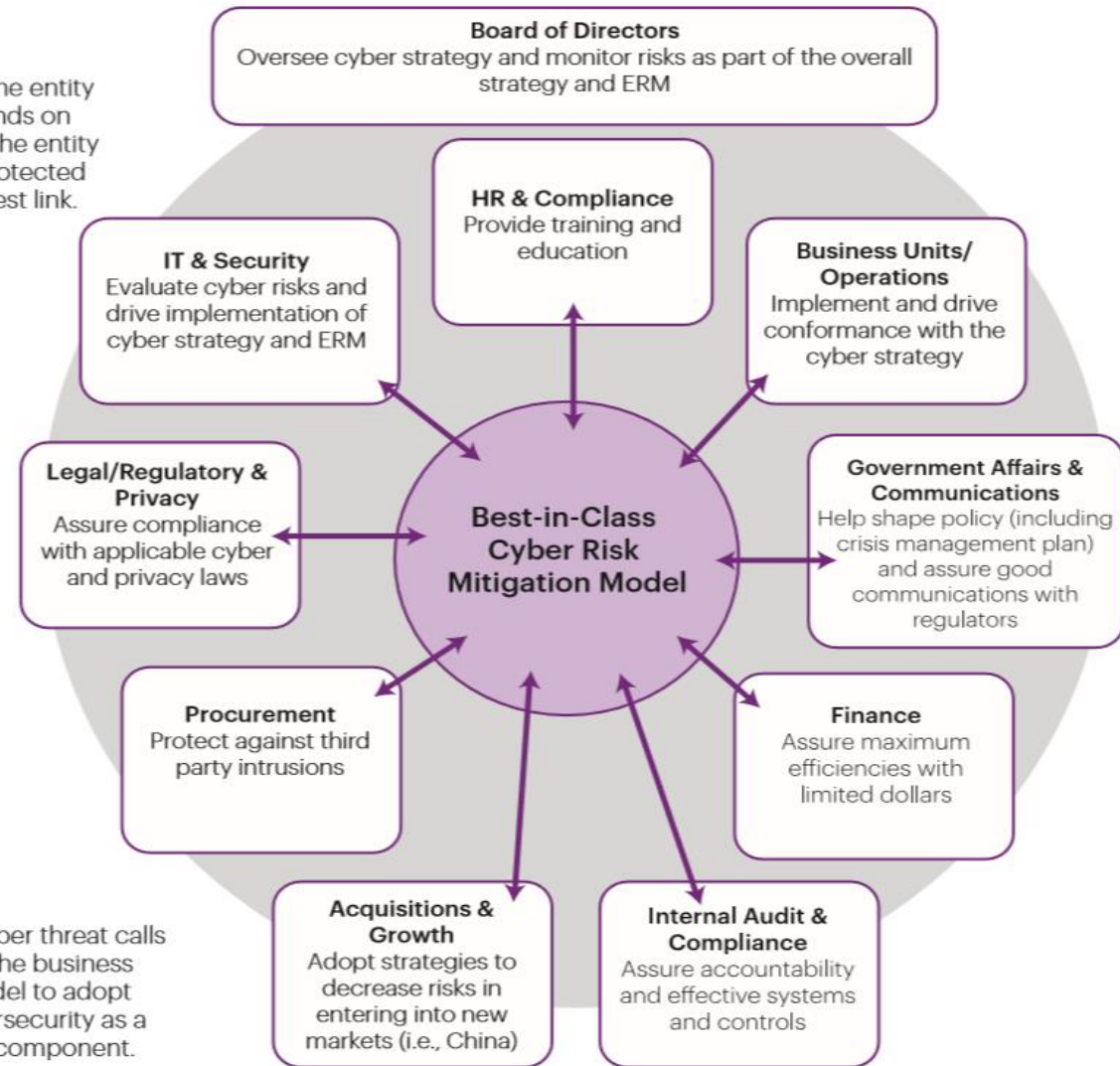
Problems commonly faced are:
- Insider Threats
- External Threats
- Policy and Strategy alignment
- Actualizing timely mitigation processes
- Email phishing and social engineering
- Physical attacks
- Implementation of robust controls during an incident

Cyber Security Responsibility is for ALL

Success of the entity now depends on cyber – and the entity is only as protected as its weakest link.

Board of Directors
Oversee cyber strategy and monitor risks as part of the overall strategy and ERM

HR & Compliance
Provide training and education

IT & Security
Evaluate cyber risks and drive implementation of cyber strategy and ERM

Business Units/ Operations
Implement and drive conformance with the cyber strategy

Legal/Regulatory & Privacy
Assure compliance with applicable cyber and privacy laws

Best-in-Class Cyber Risk Mitigation Model

Government Affairs & Communications
Help shape policy (including crisis management plan) and assure good communications with regulators

Procurement
Protect against third party intrusions

Finance
Assure maximum efficiencies with limited dollars

The cyber threat calls for the business model to adopt cybersecurity as a key component.

Acquisitions & Growth
Adopt strategies to decrease risks in entering into new markets (i.e., China)

Internal Audit & Compliance
Assure accountability and effective systems and controls

These critical components all need to collaborate and be a part of the cybersecurity strategy.

6

CYBER SECURITY vs CYBER RESILIENCE

Identify · Protect · Detect · Respond · Recover

SECURITY FRAMEWORK

Questions to Ask

How would a cyber attack affect your reputation and brand?

How will your organization address the key risk areas of security, resilience and data leakage?

What is your organization's exposure to cyber attack shocks?
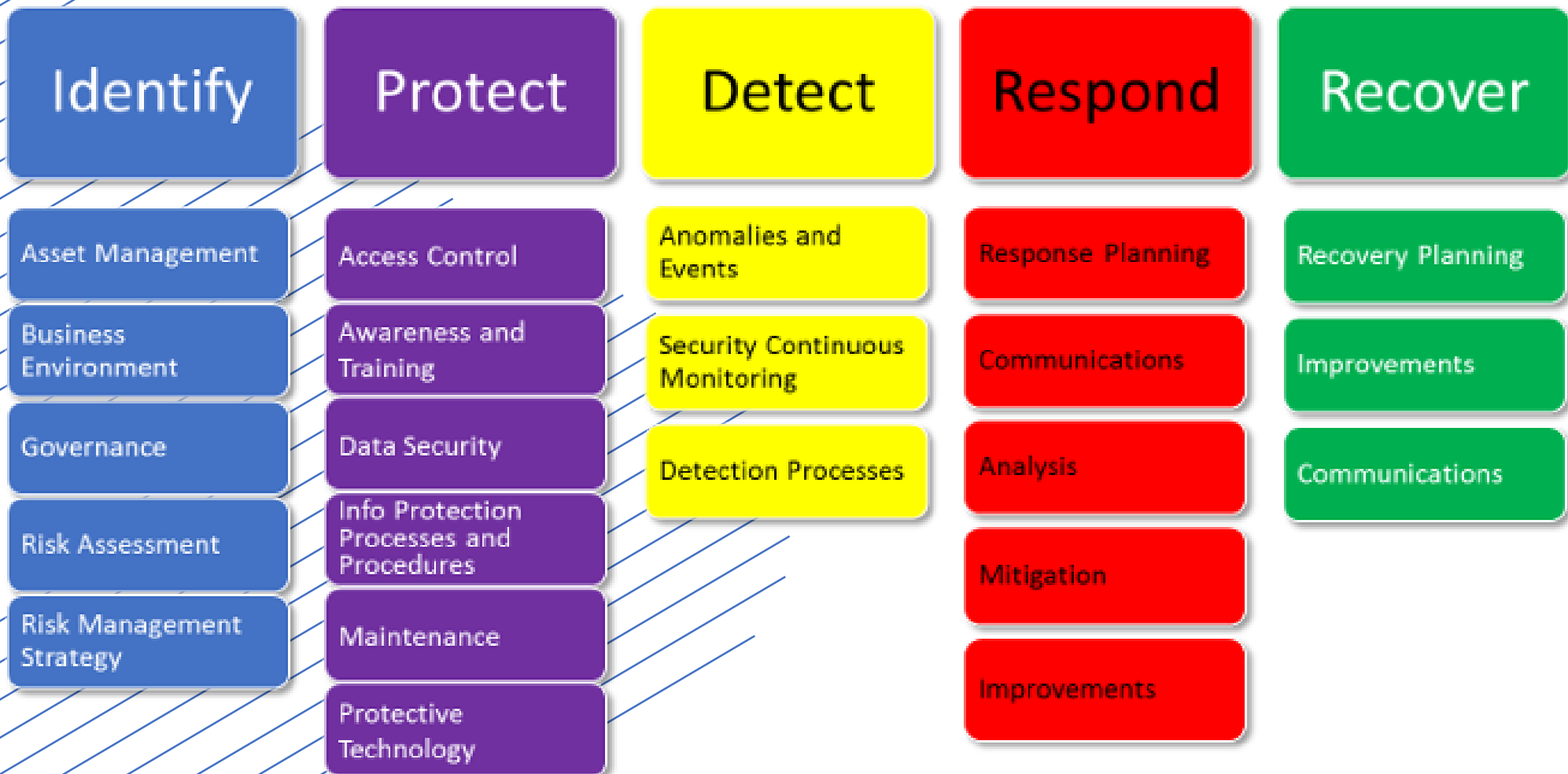How responsive is your IT organization?

Could gaps or weaknesses in your IT controls and security be contributing factors?

Is your organization covered against data leakage, loss and rogue employees?

Cyber Security Benchmarking & Maturity Framework

IS.

Cybersecurity Risk Management

- Risk Management
- People & Culture
- Infrastructure Management
- Access & Data Management
- Third Party Management

Cybersecurity Vulnerability Management

- Vulnerability Management
- Patch Management
- External Dependency Monitoring

Cybersecurity Incident Management

- Event Detection
- Response and Mitigation
- Threat Intelligence

Cyberthreat Management

- Cyber risk Remediation
- Information Sharing
- Metrics and Reporting
- Continuous Improvement

3 ON 3 ELEMENTS OF SOLUTION FOCUS

PEOPLE

PROCESSES   =

CONTROLS

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

DEMO

DID YOU KNOW THAT

Opening a Website is good enough to tell a hacker how much battery level your laptop has and a malware can be forced to you to download and take over your computer.

DID YOU KNOW THAT

< Opening a malicious document can make a hacker activate your camera and even listen to your Mic without you noticing. >

DID YOU KNOW THAT

Staying on a wireless network can make a hacker grab your passwords on the fly, make changes to websites you visit and even force you to play music that you don't want at the highest volume possible.

DID YOU KNOW THAT

Opening a simple malicious app on your phone can give a hacker indefinite access to your phone such as call records, SMS, force apps to open and even download your pics, videos as well as your WhatsApp database.

DID YOU KNOW THAT

< Plugging a phone to charge on a laptop or inserting a flash disk can enable you to get fully hacked in less than 5 seconds. >

DID YOU KNOW THAT

< A single mobile application reverse engineering can lead to a corporate network breached. **>**

EVERYDAY BEST PRACTICES

- NEVER disclose passwords

- Limit IT information disclosed

- Allow System and Antivirus Updates to run

- Escort guests in sensitive areas

- Question people you don't know

- Talk to employees about security

- Centralize reporting of suspicious behaviour

- [Operational Security Guideline](#)

Building A Strategy RoadMap

GAP ANALYSIS

Vulnerability Assessment, Penetrations Testing, Business Impact Analysis

RISK PROFILE

Know what to prioritize according to the Risks Identified

BUDGET PLANNING

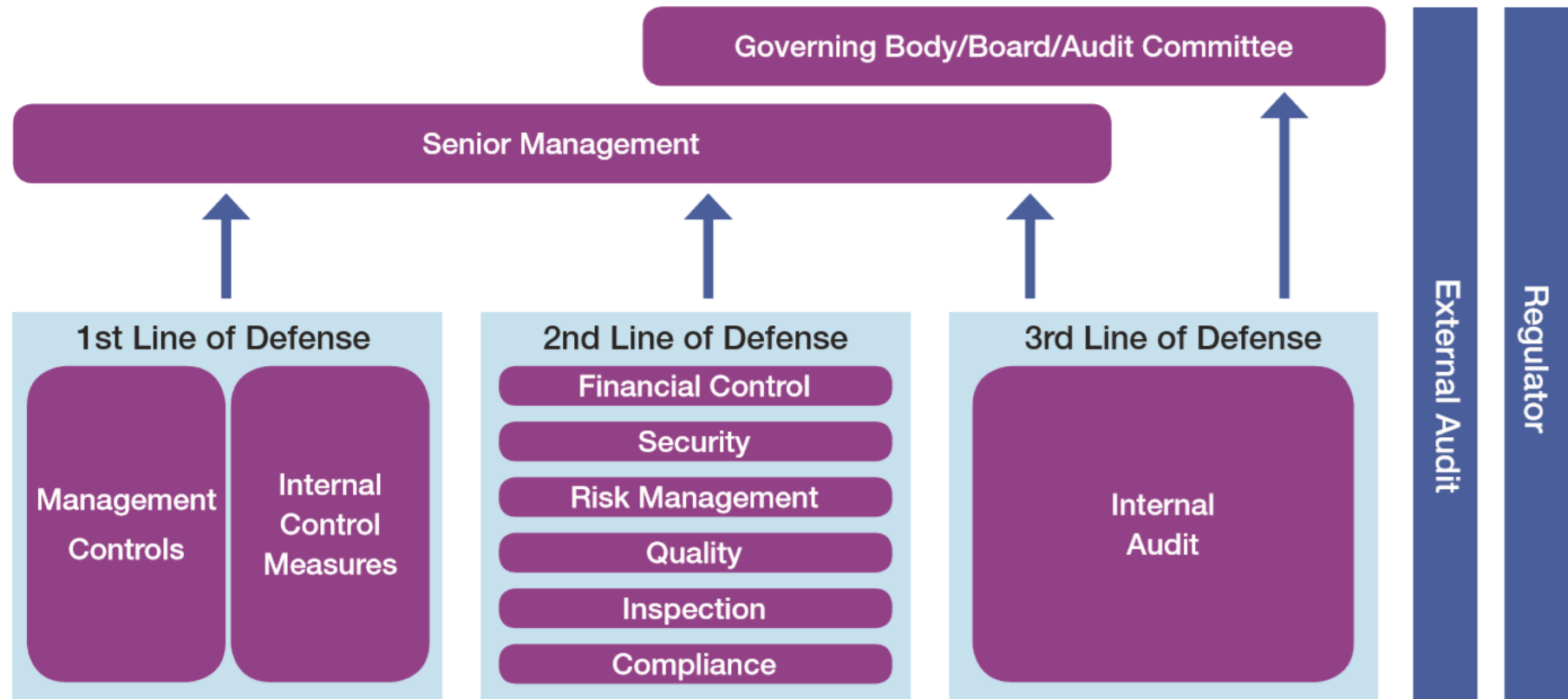Spread out the Cyber Security budget according to the priority above
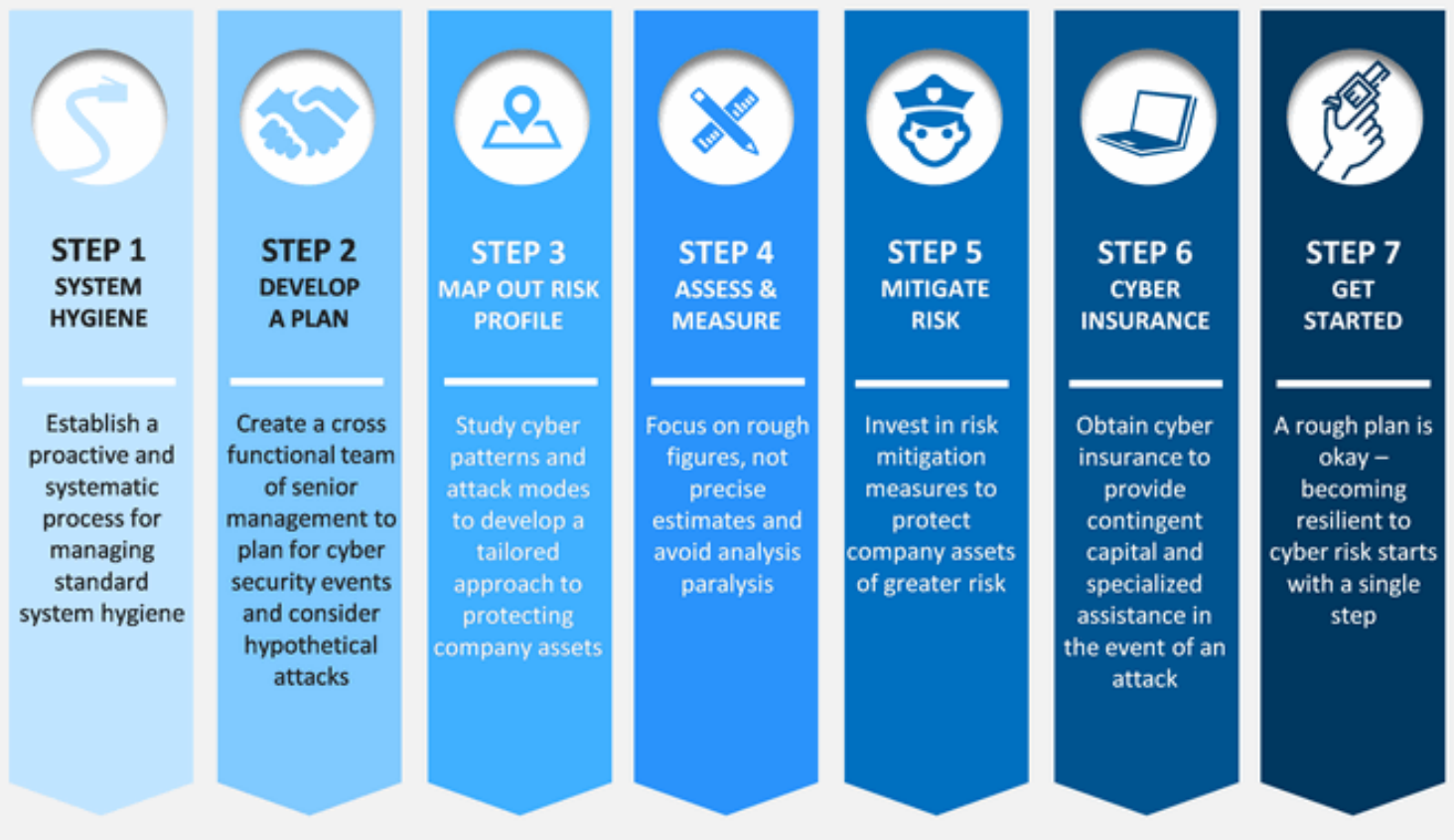
START SOMEWHERE

Start Implementation someday
Outsourced Managed Services
Board Level Involvement

How to Achieve Resilience in 7 Steps

STEP 1
SYSTEM HYGIENE

Establish a proactive and systematic process for managing standard system hygiene

STEP 2
DEVELOP A PLAN

Create a cross functional team of senior management to plan for cyber security events and consider hypothetical attacks

STEP 3
MAP OUT RISK PROFILE

Study cyber patterns and attack modes to develop a tailored approach to protecting company assets

STEP 4
ASSESS & MEASURE

Focus on rough figures, not precise estimates and avoid analysis paralysis

STEP 5
MITIGATE RISK

Invest in risk mitigation measures to protect company assets of greater risk

STEP 6
CYBER INSURANCE

Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack

STEP 7
GET STARTED

A rough plan is okay – becoming resilient to cyber risk starts with a single step

IS.

Thank you

Contacts
bright.gameli@is.co.ke
www.brightzeed.com
www.is.co.ke
0712421951