


**< Technology Enabled
Fraud; Trend and Control >**





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



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

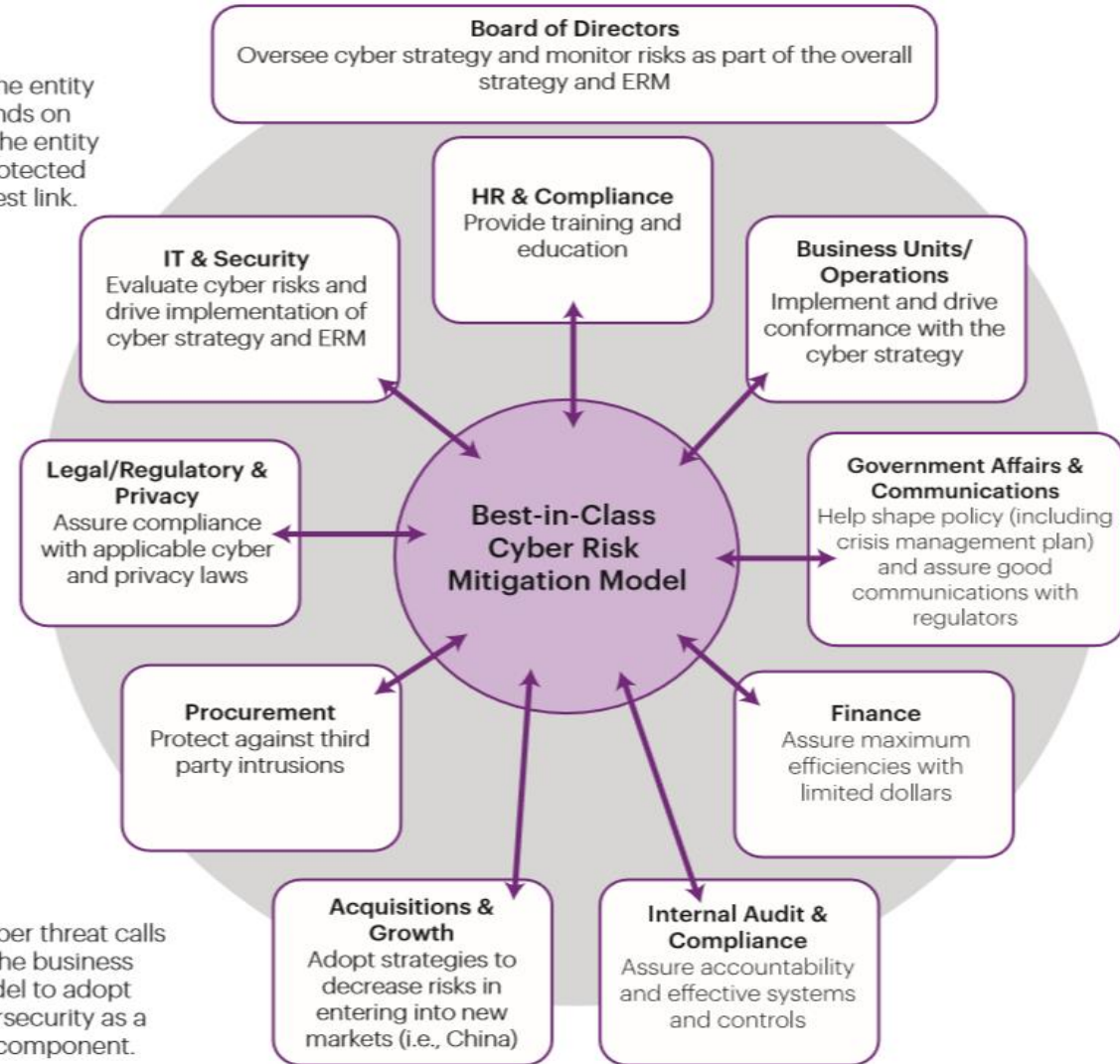
Problems commonly faced are:

- 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.

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



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

CYBER SECURITY vs CYBER RESILIENCE



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?

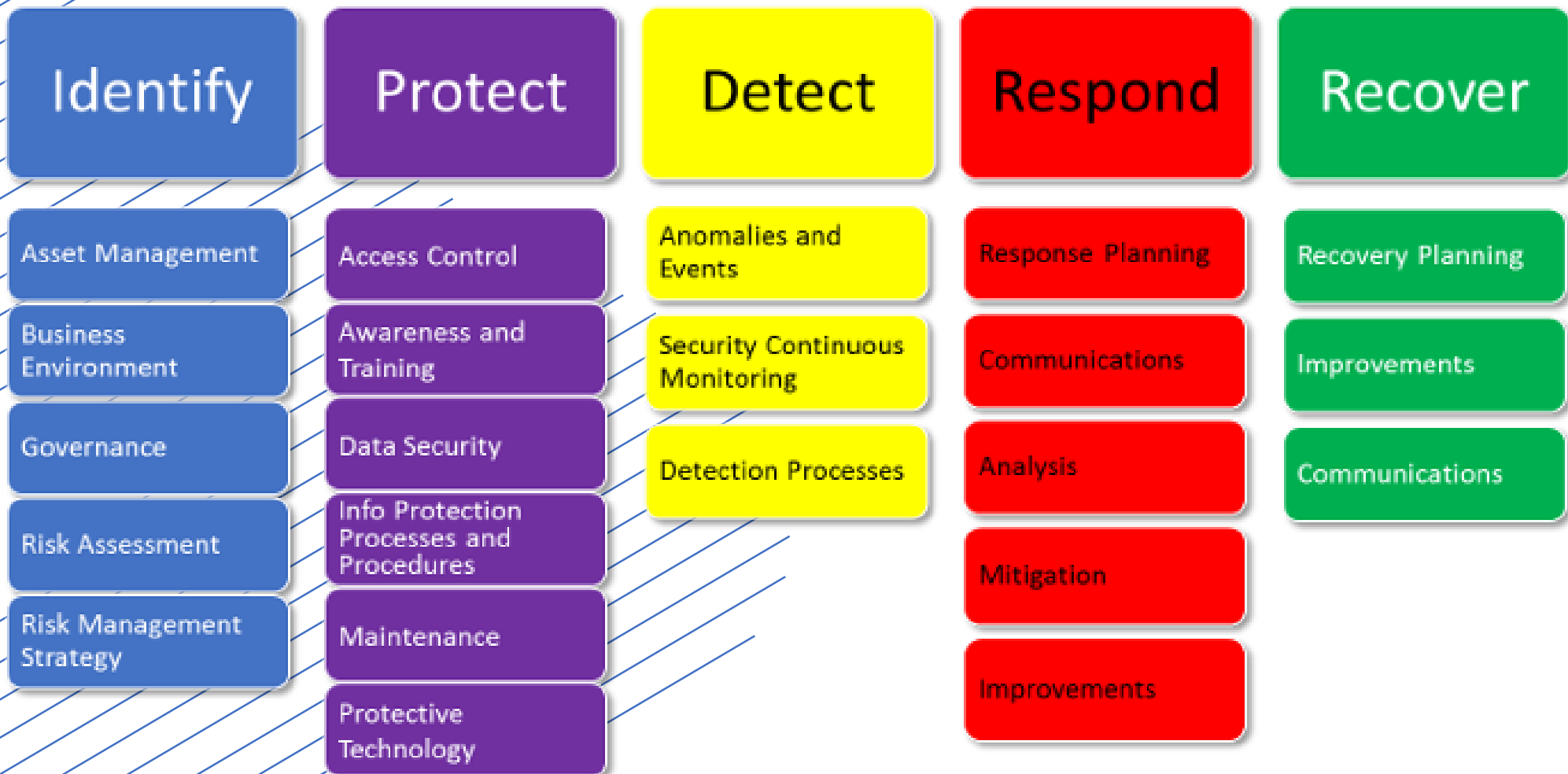


Could gaps or weaknesses in your IT controls and security be contributing factors?



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

NIST Cyber Security Framework



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 flashlight app on your phone can give a hacker indefinite access to your phone such as call records, SMS, make calls on your behalf 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. >

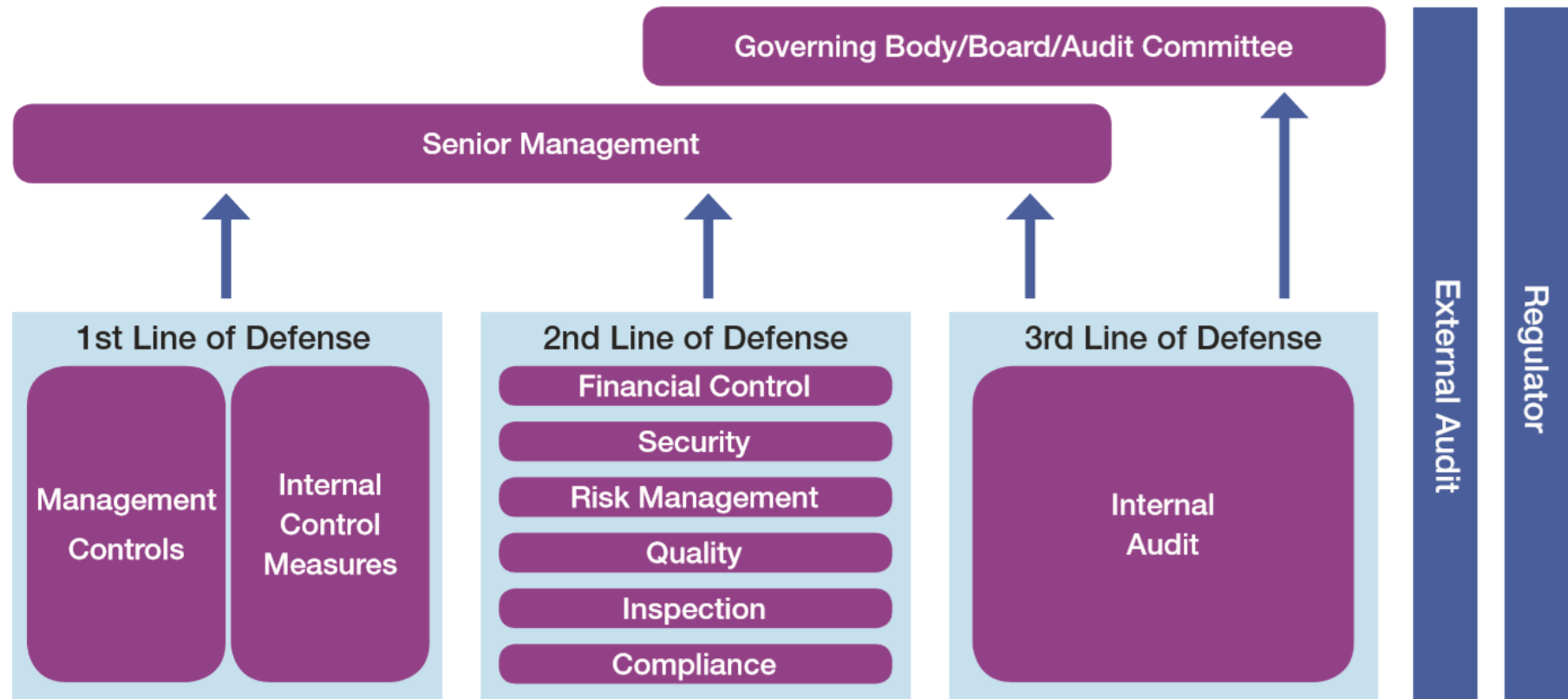
DID YOU KNOW THAT

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

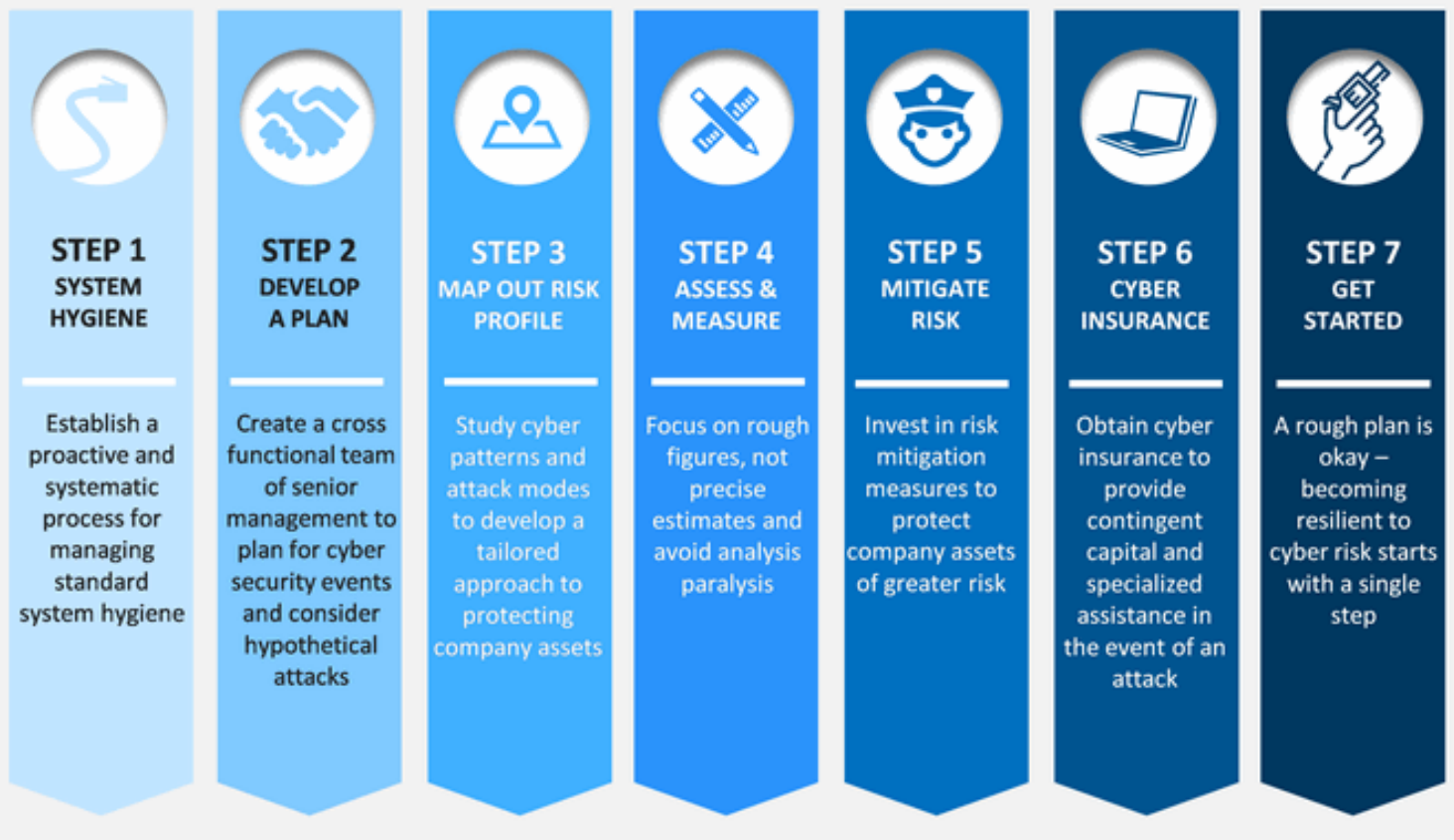
BEST PRACTICES

- NEVER disclose passwords
- Limit IT information disclosed
- Limit information in auto-reply emails
- Escort guests in sensitive areas
- Question people you don't know
- Talk to employees about security
- Centralize reporting of suspicious behaviour
- [Operational Security Guideline](#)

Organizational Structure



How to Achieve Resilience in 7 Steps



IS.

