KPMG

Building An effective incident response capability

NATIONAL CYBER SECURITY WEEK

OCTOBER 2017

Contents

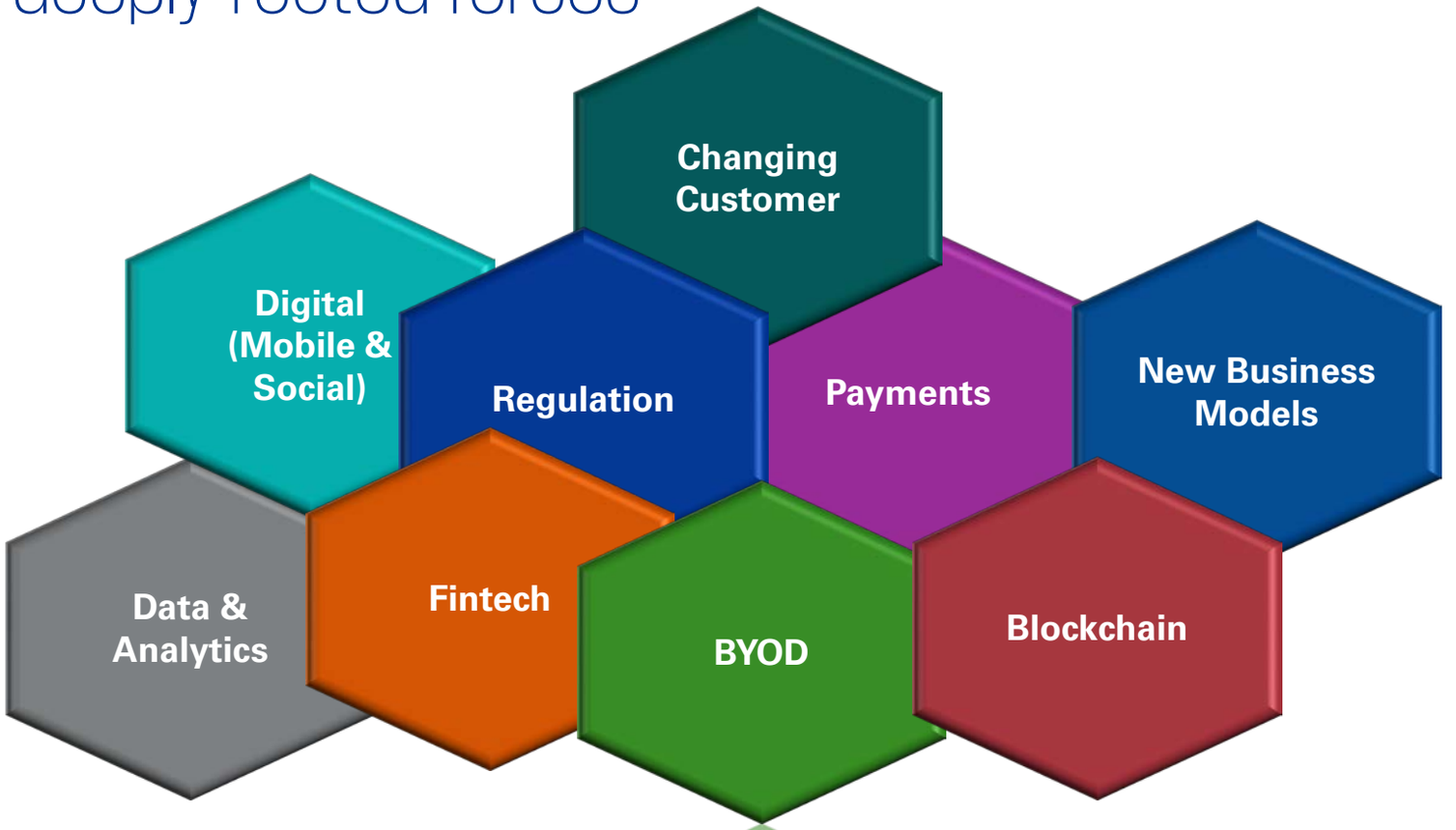
KPMG

SECTION ONE

INTRODUCTION

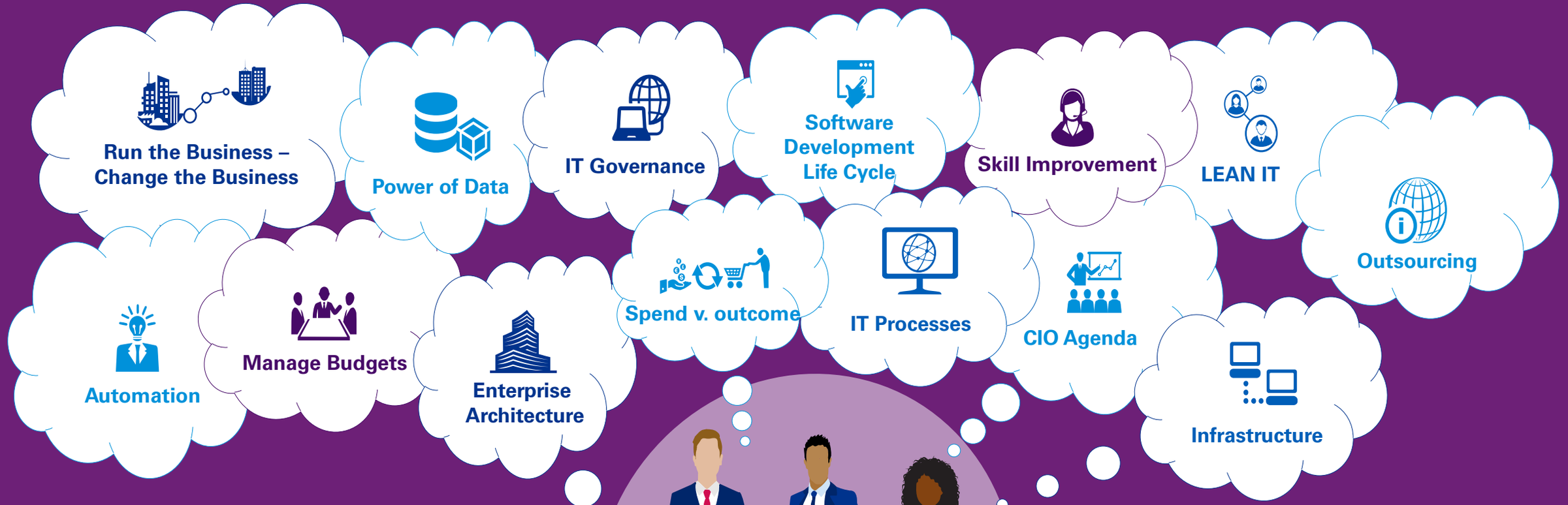
Introduction

The world in which we live and work is changing rapidly, driven by a number of deeply-rooted forces



Introduction

What is on the mind of a C-Level executive?



SECURITY & RESILIENCE

Introduction

Data Breaches

EQUIFAX

July 2017, 145 million users compromised

- Social Security Nos
- Birth dates
- Driver license Nos
- Credit card details

YAHOO!

2013-2014, 3 Billion User Accounts compromised

- Real names
- Email addresses
- Birth dates
- Security questions and answers

Target

December 2013, 110 million customers compromised

- Credit card details

ebay

May 2014, 145 million users compromised

- Names
- Addresses
- Encrypted passwords

SONY

April 2011, 77 million PSN user accounts compromised

- Names
- Passwords
- emails
- credit card numbers

May 2017, 150 countries affected

What is happening in Ghana ?

Over 80%

of reported fraud cases in Ghana are electronic

$250,000

lost weekly to cyber crime in the banking industry

$13,000,000

lost yearly to cyber crime in the banking industry

Source: B&FT 8/08/2016, e-Crime Bureau

KPMG

Introduction

Threat Landscape

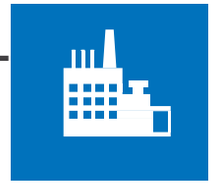
The Enemy

THE INSIDER

Intentional or unintentional

Motivation: Grudge, financial gain

Business impact: Reputational damage, financial loss, regulatory censure.



COMPETITORS

Competition or rivalry

Motivation: competitive advantage

Business impact: competitive disadvantage, reputational damage, information loss

ORGANISED CRIME

Global, difficult to trace and prosecute

Motivation: financial advantage, potentially opportunistic

Business impact: reputational damage, theft of information

HACKERS OR HACKTIVISTS

Attention or popular causes

Motivation: dynamic and unpredictable, potentially issue motivated

Business Impact: reputational damage, operational disruption information

STATE SPONSORED

Espionage and sabotage

Motivation: political and economic advantage

Business Impact: theft of information, operational disruption, financial loss

KPMG

SECTION TWO

WHY CYBER INCIDENT RESPONSE

Incidents and their impact

Intellectual property theft by employee – company unaware of data leaked or lost

Malware / Virus on network – confidential information leaked

Deletion of logs and other critical information from network

Denial of Service attack

System hack

Phishing attack

Employee

Customer

Business

Importance of Incident Response

"There are two types of organisations. Those that have been hacked and those that will be hacked."

Robert S. Mueller III, FBI Director

Limits any potential damage to organizational reputation

Reduce recovery time and cost from any breach

Demonstrable evidence of duty of care and compliance with legal obligations

Key component of a business continuity program

Increase investor confidence

Why Cyber Incident Response

Five common cyber incident response mistakes

KPMG

SECTION THREE

HOW TO RESPOND TO INCIDENTS

Incident Response

Incidence response plan

An incident response plan is to ensure that there is a documented and fully understood mechanism for responding to an incident that has the potential to cause disruption to the organization, regardless of its cause.

Key steps in designing an incidence response plan include

- **Identify the organization's key processes and recovery requirements**
- **Establish teams for emergency response and crisis management**
- **Develop an incident response process**
- **Obtain management buy in and approval of the incident management process**
- **Publish and train all staff**

Incident Response

Ready to manage a cyber incident?

Paper testing

- Test incident response plan

Tabletop exercises

- Executive and/or operational team
- Discussion around roles and responses to a specific incident

Cyber incident simulation

- Simulation of a real world incident
- Simulation will be followed by a debrief
- Recommendation on improvement steps

Incident Response

Cyber incident response framework

	Phase 1 Preparation	Phase 2 Identification	Phase 3 Containment	Phase 4 Eradication	Phase 5 Recovery	Phase 6 Wrap-up
Objectives	Get familiar with the process and technology	Determine the scope and parties involved	Minimise the effect on IT resource	Eliminate compromise artifacts	Restore system to normal operations	Post incident activities
Activities	• Incident Response team assembly • Incident reports	• Gather critical information	• Isolate the threat • Disconnect from production environment • Remove illegitimate access • Update firewall policy	• Controls creation • Security baselines • Configuration reviews • Patching	• Restore back-up • Test, monitor and validate systems	• Incident reporting • Provide awareness and training on lessons learned

Thank You

Andrew Akoto
Partner

KPMG,
Marlin House,
13 Yiyiwa Drive
Abelenkpe - Accra
Ghana

M: +233208174629
Email:
aakoto@kpmg.com