Cyber Security Readiness Presentation

Ethiopia Roadshow

KPMG Advisory Services Limited

May 2022

Agenda

- Survey Results – Ethiopia Roadshow
- Setting the Context – Cyber Security Awareness & Training
- Cyber Maturity Assessment Overview
- Data Privacy
- Value Proposition

KPMG

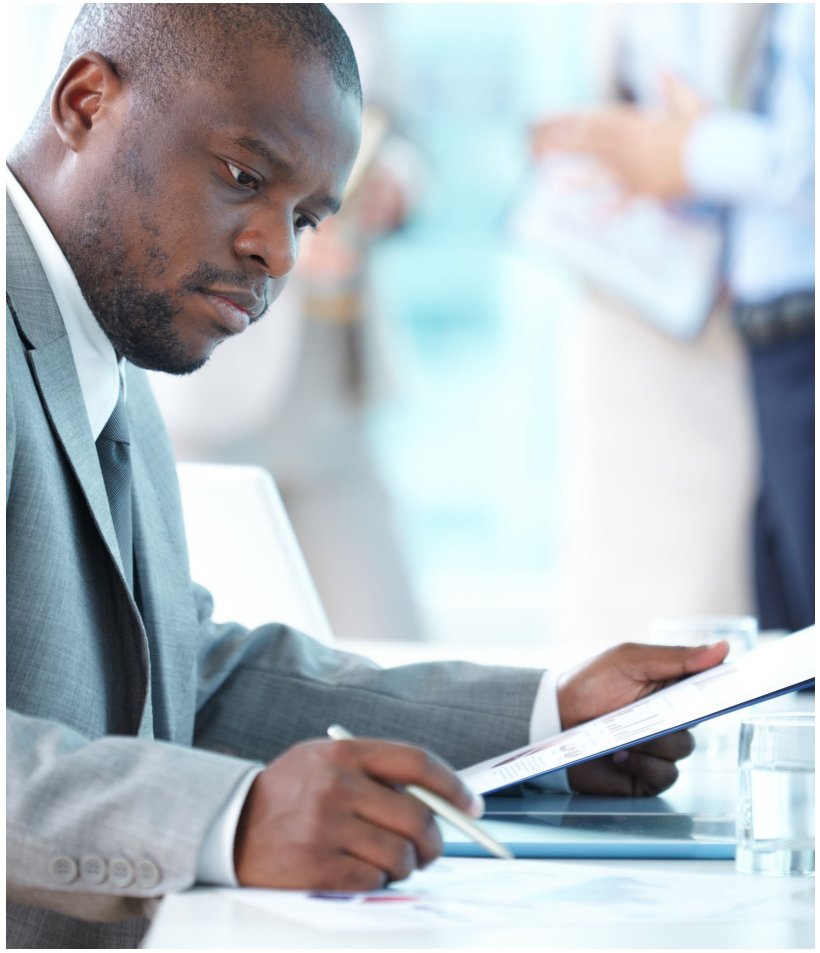
Survey Results - Ethiopia Roadshow

East Africa CEOs see cyber security as a major threat to the growth of their organization ranking it second out of twelve risks...

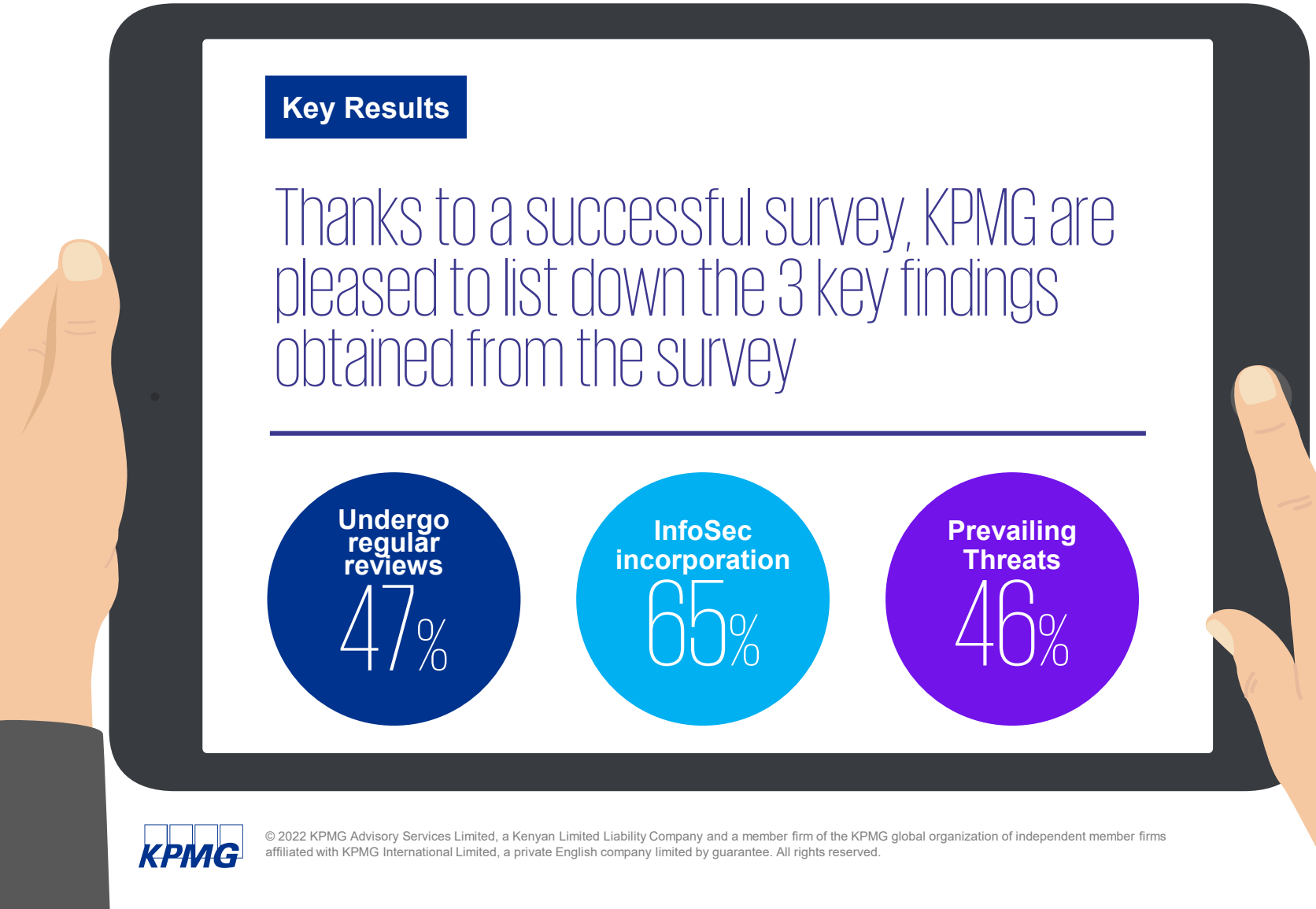
79% Say protecting their partner ecosystem and supply chain is just as important as building their own organization's cyber defenses.

75% Say a strong cyber strategy is critical to engender trust with their key stakeholders.

70% Say that they are well prepared for future cyber-attacks.



Key Findings – Digital Transformation & Cyber Security Readiness Survey



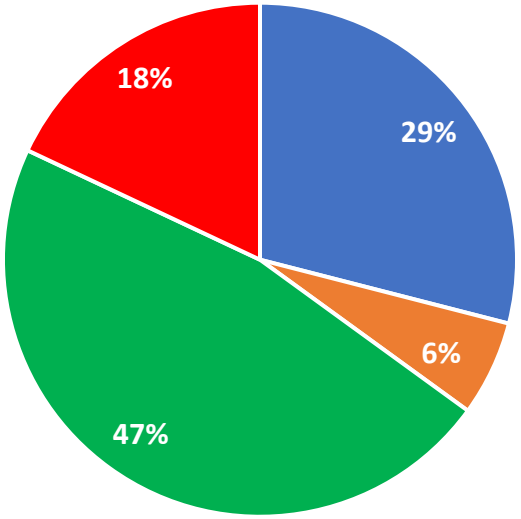
47% noted that their strategic Cyber Security Outlook is subject to regular reviews.

65% noted that Information Security is incorporated into IT security and reports to the CIO or equivalent

46% noted that Ransomware, Business Email Compromise and Data Leakage have been the prevailing threats

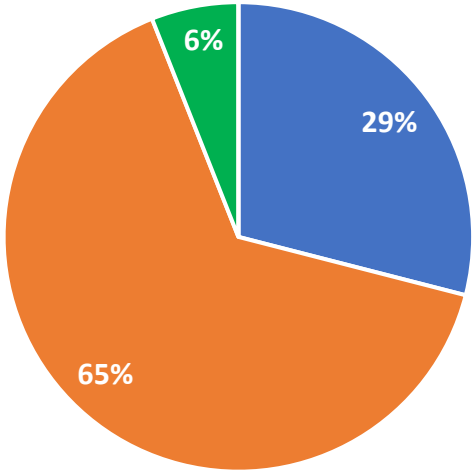
Survey Responses - Summary

How would you describe your strategic Cyber Security outlook?



- Efforts are ad-hoc and responsive in nature
- We have a strategy, but it has not been refreshed recently
- We have a strategy that is subject to regular review
- Our strategy is linked to our specific threat profile with measurable KPIs

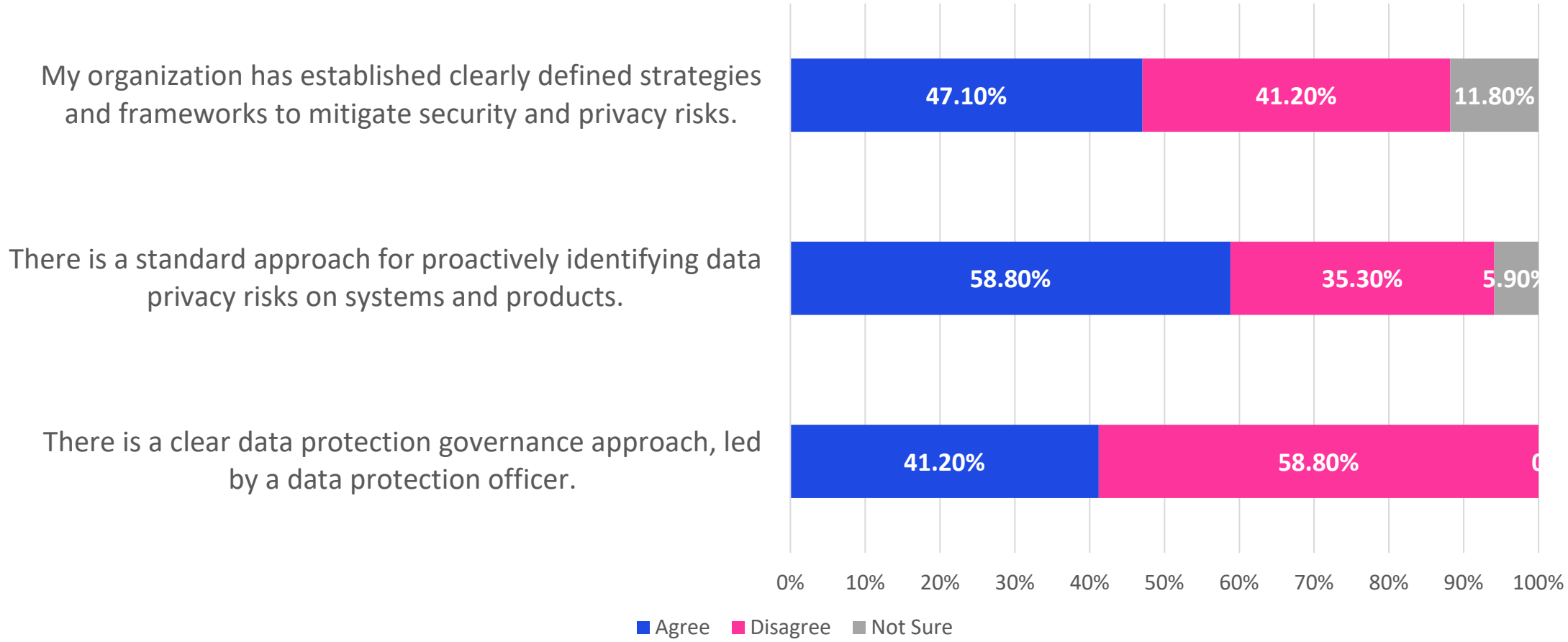
What is your organization's approach to implementing independent information security oversight?



- We have no formal information security function and IT security efforts are fully managed out of IT with little to no independent oversight.
- Information Security is incorporated into IT security and reports to the CIO or equivalent. Risk management and/or Internal audit provides independent oversight.
- We have a fully independent Cyber and Information security function reporting directly to the organizational leadership. Risk management and Internal audit provides independent oversight.
- Other

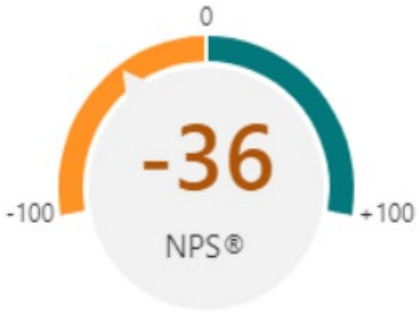
Survey Responses - Summary

What is your organization's approach to implementing independent information security oversight?



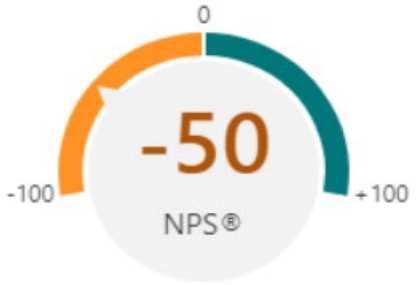
Survey Responses - Summary

How confident are you in the effectiveness of your organization's Cyber Security awareness training?



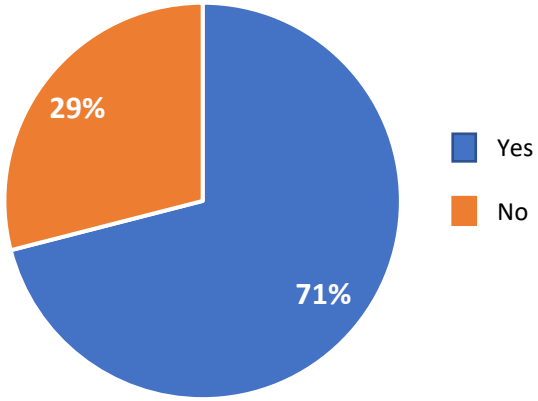
Promoters	21%
Passives	21%
Detractors	58%

How confident are you that the Cyber Security incident response team (CIRT) is equipped to effectively deal with a major incident?



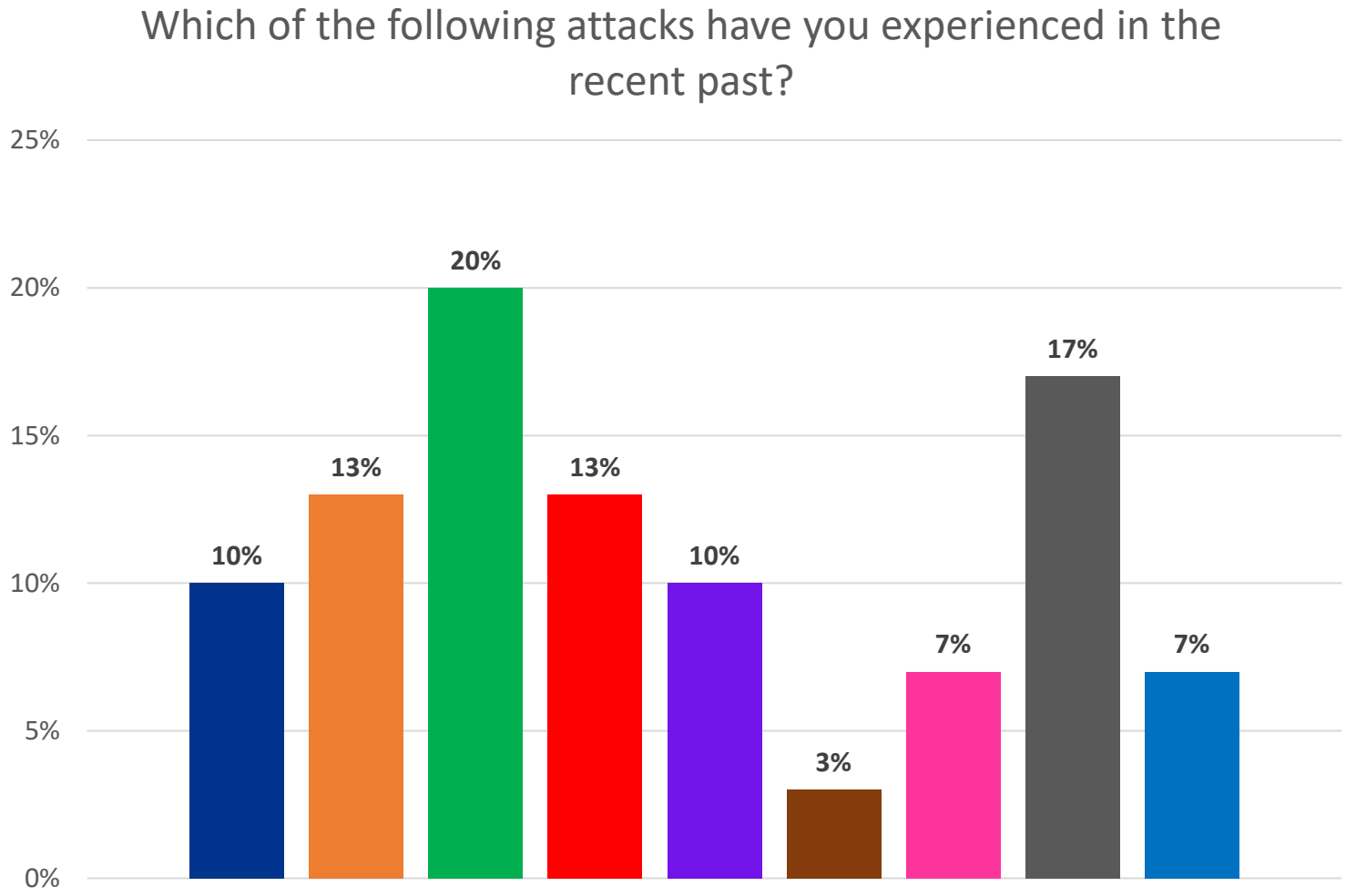
Promoters	7%
Passives	36%
Detractors	57%

Is your organization planning on recruiting Cyber Security resources in the next 12 months?



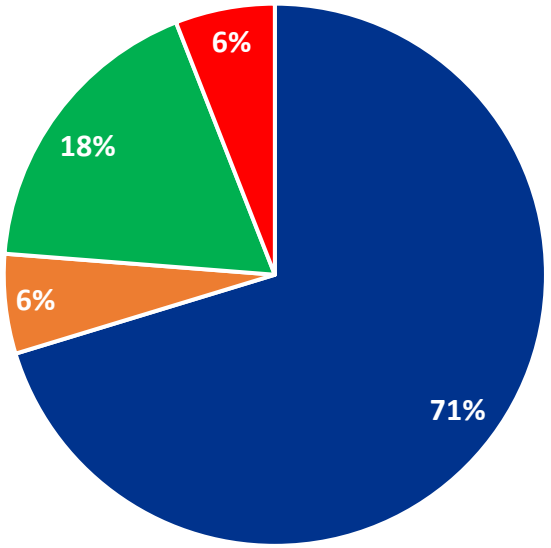
Survey Responses - Summary

- Denial of Service (10%)
- Data Leakage (13%)
- Ransomware (20%)
- Business Email Compromise (13%)
- Insider Threat (10%)
- Supply Chain Attack (3%)
- Cannot disclose for confidentiality reasons (7%)
- None (17%)
- Other (7%)



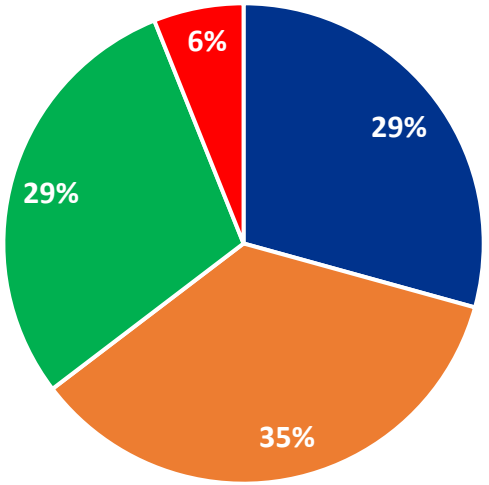
Survey Responses - Summary

How long did the recovery effort take?



- A few days at most
- Less than a week
- Less than two weeks
- More than two weeks

How confident are you about the Cyber Security controls implemented by your organization to detect and mitigate the threat of a cyber incident?



- Not confident
- Partially Confident
- Very Confident
- Cannot measure

KPMG

Setting the Context - Cyber Security Awareness & Training

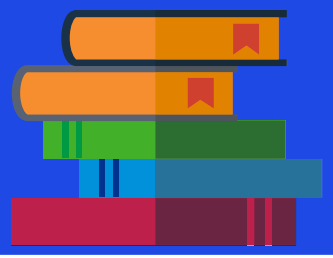
Awareness: Its Importance

43%

of employees are **not aware** of implications in **clicking a suspicious link**

55%

of employees are **not convinced** of risks associated with connecting their laptop to a **public Wi-Fi network**



50%

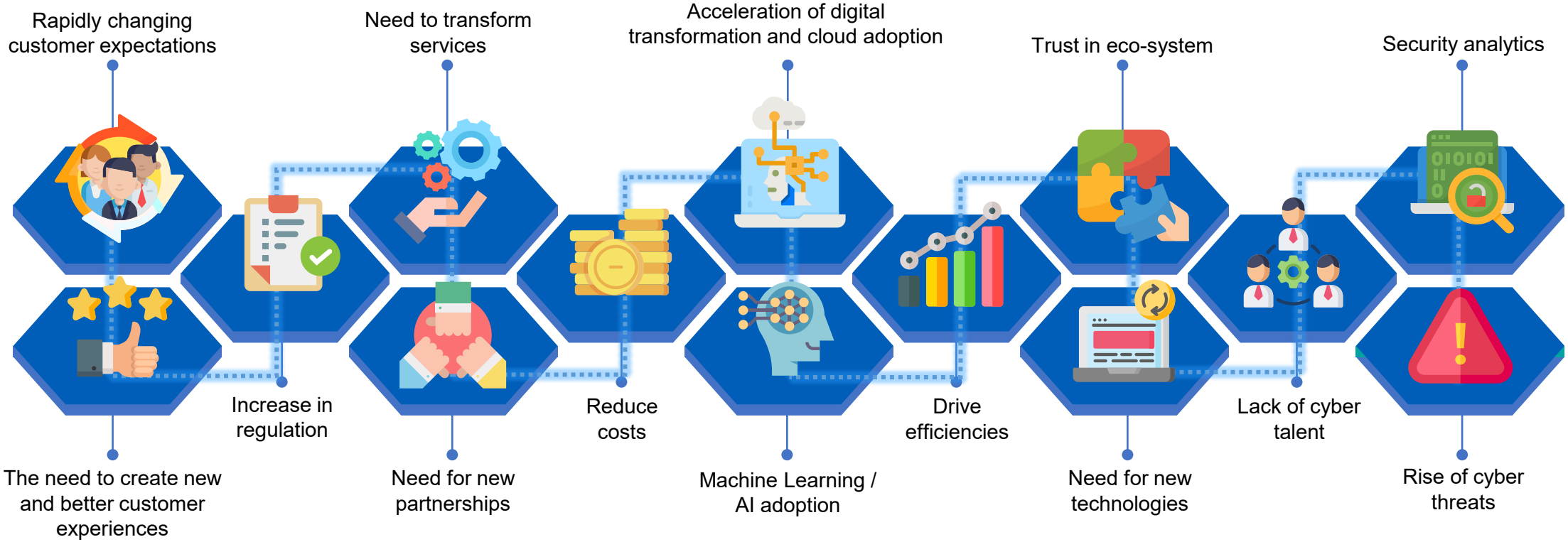
of employees consider that **using personal emails for work doesn't pose a risk** to their organization

28%

of employees admitted a lack of confidence in **identifying a phishing email**

Source: https://www.bsigroup.com/globalassets/localfiles/en-ie/our-services/mediapro/2020_state_of_privacy security_awareness_report_mediapro.pdf

Cyber is a Golden Thread

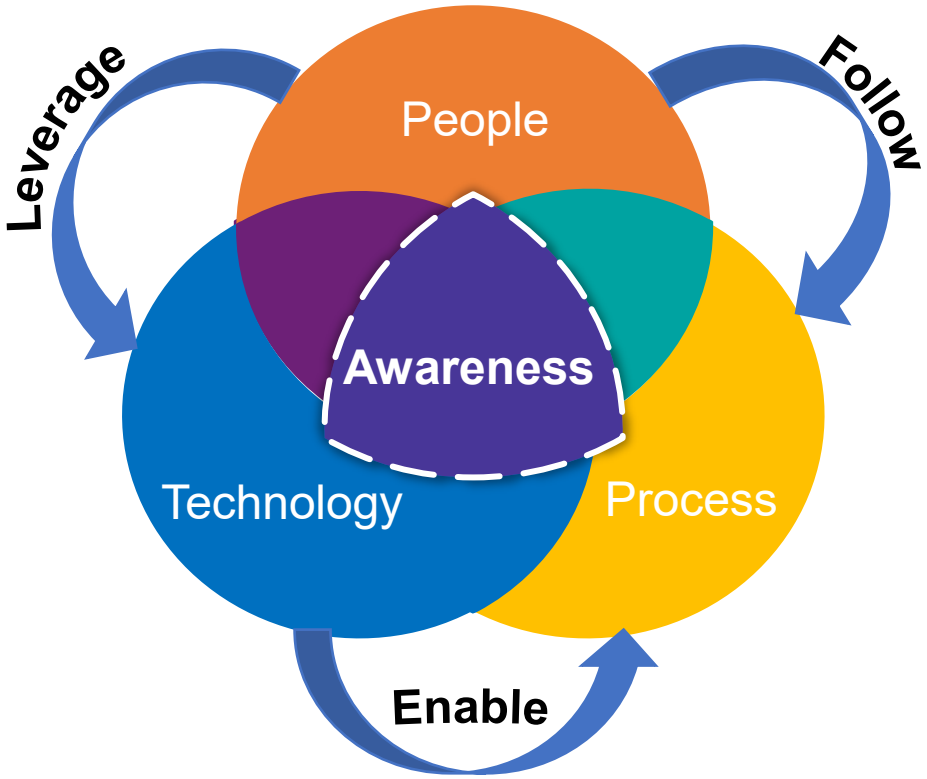


Business drivers and outcomes

Technology drivers and outcomes

Cyber drivers and outcomes

Awareness: Its Importance



Case Study: SolarWinds Breach

Solar winds recent massive cybersecurity breach affected multiple organizations in USA and the world at large.

Reports claim that it could have all begun with an old school password blunder **by an intern** !

Root cause:

Weak password : solarwinds123

Password was **shared on an internal account of publicly accessible repository** for several years

KPMG

Cyber Maturity Assessment Overview

Assessment Overview - KPMG Cyber Maturity Assessment

The CMA is a **KPMG proprietary methodology** based on leading information security frameworks, such as:

A. Information Assurance Maturity Model (**IAMM**)

B. American National Standards Institute (**ANSI**) Financial Management of Cyber Risk

C. Industry frameworks such as **ISO 27001** and **NIST** (including Cyber security framework, 800-53, etc.)

Benefits of our web based CMA platform

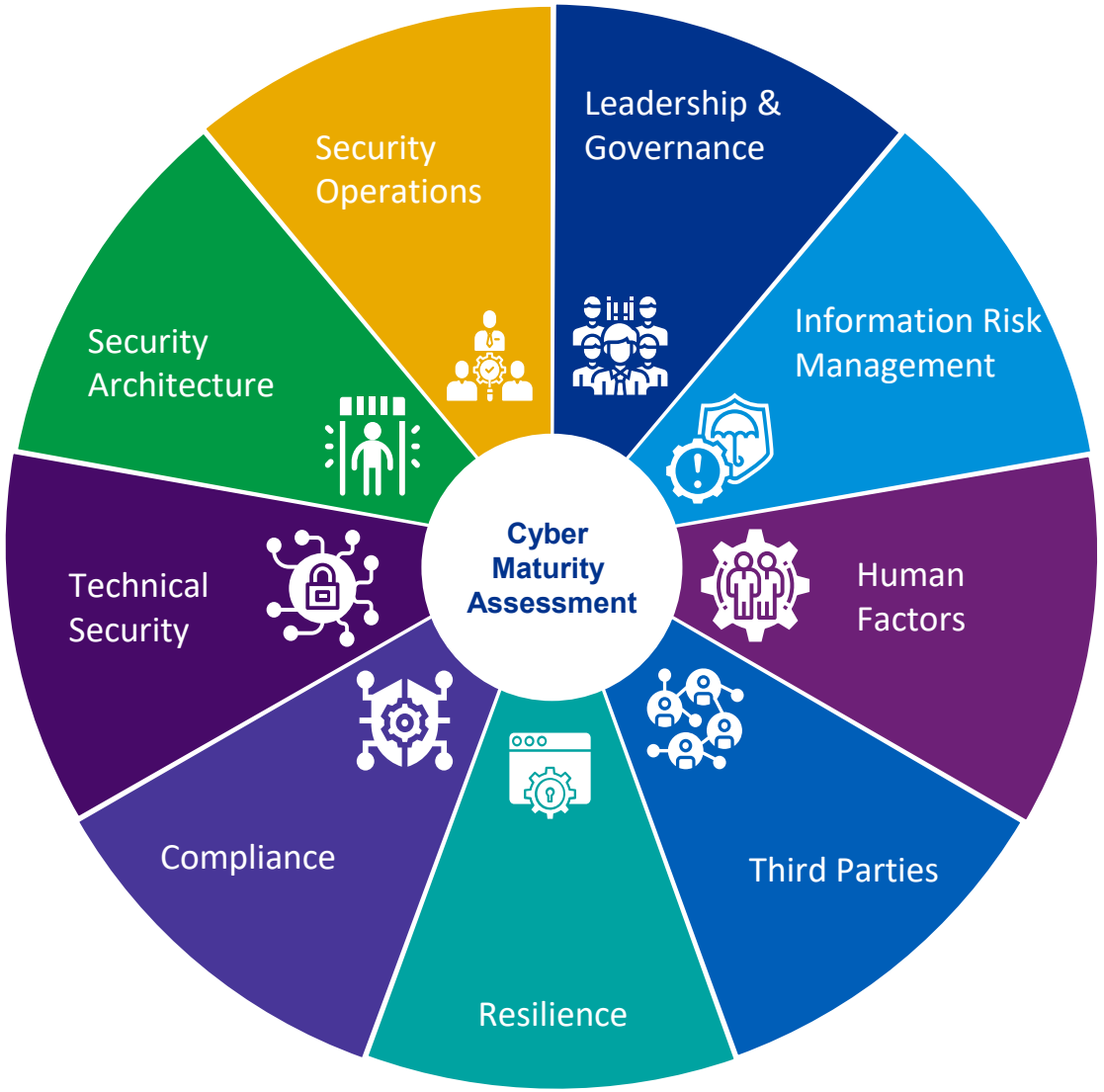
Efficient assessment delivery by easy web access and option for delegation of questions.

Flexible adaption of controls and question catalogue to individually match your needs.

Usable web interface with interactive charts and export functionality.

Secure storage of data by using strong encryption and data center locations only within EU.

Cyber Maturity Assessment Dimensions



Cyber Security Assessment Report - Illustrative

Risk Diagram

144/144
Risks shown

Impact \ Probability					
	2	0	0	0	0
	12	2	0	2	4
	37	10	8	5	6
	35	8	7	3	1
	1	0	1	0	0

Critical
Very High
High
Medium
Low

Criticality	Risk Title	Impact	Probability	Actions
High	There is a high risk of inactivity in case of a disruptive or emergency event.	Extreme	Unlikely	
High	There is a high risk of people's health and safety being affected through the effects of the disruptive or emergency event.	Extreme	Unlikely	
High	There is a high risk of vendors misusing classified information.	Critical	Likely	
Medium	There is a medium risk of insufficient accountability for security management.	Critical	Unlikely	
Very High	There is a very high risk of insufficient action taken to ensure continuity of operations in case of a disruptive or emergency event.	Critical	Almost Certain	
Very High	There is a very high risk of classified information being disclosed to unauthorised parties.	Critical	Certain	

KPMG

Data Privacy

Data Privacy in Banking and Insurance Sector

Due to the perceived value of this data, the banking industry is one of the primary targets not only for the attackers but is under radar of regulators for maintain data privacy standards.

Privacy Exposure with Digital Initiatives

- With increasingly dependency on the cloud to store information and conduct financial transactions online with apps, bots etc. data privacy concerns continue to grow

Information Flexibility

- High flow of information exchange can make it difficult to maintain data privacy and security standards where compliance responsibility doesn't go away with outsourcing.

Proliferation of social media

- Social media provides challenges in maintaining data privacy due to lack of privacy centric standardized social media operations

Data Flow Management

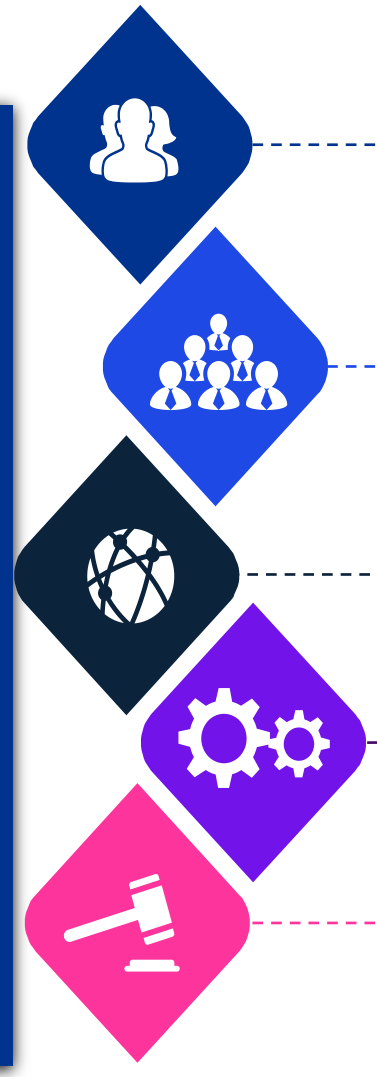
- No automatic labelling of inactive customers make it difficult to adhere to data privacy principles in practice

Customer centric Vs Privacy centric

- Use of front offices for sales promotion, cross selling, upselling and customer service pose privacy concerns

Why is Data Privacy important?

Privacy is defined as the rights of individuals and obligations of organizations with respect to the collection, use, retention, disclosure, and disposal of personal information



- **Shift to Customer Privacy centric approach in Banking Sector**
- **Data Privacy Regulations with extra territorial scope**
- **Customer trust**
- **Digital initiatives and threat landscape**
- **Third party data sharing**

Top 5 Data Breaches of all time...

Yahoo data breach (2013)
Records affected: 3 billion
Damages: $350 million loss

Target data breach (2013)
Records affected: 60 million
Damages: $18.5 million multistate settlement

Facebook data breach (2019)
Records affected: 540 million
Damages: leaked account information

First American Financial Corporation data breach (2019)
Records affected: 885 million
Damages: Charges from the New York State

LinkedIn data breach (2012)
Records affected: 165 million
Damages: $1.25 million to breached victims

Source: https://www.secureworld.io/industry-news/top-10-data-breaches-of-all-time

Data Privacy Principles

LAWFUL,FAIR,TRANSPARENT

Organizations shall process customer data in accordance with the law and inform customers how they process their personal data to the extent necessary to ensure that processing is fair

PURPOSE LIMITATION

Organizations shall process personal data only for the purposes where it would be useful (and allowed by law) to administer business and provide products, service and other opportunities to customers

DATA MINIMIZATION

Organizations shall collect customer data that is adequate, relevant and limited to what is necessary in relation to the set-out purpose

ACCURACY

Organizations shall establish procedures to ensure that customer's financial information is accurate, current and complete in accordance with commercial standards. Banks shall respond to requests to correct inaccurate information in a timely manner

STORAGE LIMITATION

Organizations shall keep customer data in a form which permits identification of customers for no longer than is necessary for the purpose for which the data is processed

SECURITY

Organizations shall maintain appropriate security standards and procedures regarding unauthorized access to customer information. Security measures must commensurate with the sensitivity of the information and the level of risk associated with the processing of it

ACCOUNTABILITY

Organizations should assign roles and responsibilities (e.g., DPO) to oversee adherence to the principles and demonstrate compliance with applicable regulations

KPMG has identified

Eight key cyber security considerations for 2022

Expanding the strategic security conversation

Change the conversation from cost and speed to effective security to help deliver enhanced business value and user experience.

Achieving the x-factor: Critical talent and skillsets

Transform the posture of CISOs and their teams from cyber security enforcers to influencers.

Adapting security for the cloud

Enhance cloud security through automation — from deployment and monitoring to remediation.

Placing identity at the heart of zero trust

Put IAM and zero trust to work in today's hyperconnected workplace.

Exploiting security automation

Use smart deployment of security automation to help realize business value.

Protecting the privacy frontier

Move to a multidisciplinary approach to privacy risk management that embeds privacy and security by design.

Securing beyond the boundaries

Transform supply chain security approaches — from manual and time consuming to automated and collaborative.

Reframing the cyber resilience conversation

Broaden the ability to sustain operations, recover rapidly and mitigate the consequences when a cyberattack occurs.

Q&A session / Open discussion

Annexures

KPMG in East Africa

Your Vision, our Proven Capabilities. Our integrated team of cyber security specialists providing unique insights throughout the Cyber Transformation project implementations, combining knowledge, analytical tools and intelligent feeds to help fuel smarter, faster decisions.

Real results achieved by integrated specialists.

KPMG's deep telecommunication sector knowledge

Established relationships with key decision makers

We help you identify key risks, unique selling points, potential synergies and deal breakers early in the process

We have the capabilities to provide an end-to-end service offering

We will hold your hand through every step of your transaction journey

Our experienced transformation team takes a practical approach to helping you maximize value

We employ tested methodologies to maximize value to you

As a strategy and transformation Advisor we support your strategy, with the right partners, in line with your long term visions

Our values

Excellence
We never stop learning and improving.

Courage
We think and act boldly.

For Better
We do what matters.

Together
We respect each other and draw strength from our differences.

Integrity
We do what's right.

Quantum of Our Privacy Experience

COLLABORATION WITH THE GLOBAL TEAMS

UK
USA
BELGIUM
ITALY
MALDIVES
SRI LANKA
UAE
MALAYSIA
INDONESIA

INDIA PRIVACY SKILLS

- 70+ Member Privacy Team
- 50+ OneTrust Certified Resources
- 40+ IAPP Members
- 25+ IAPP Certified Resources
- 20+ DSCI Certified Resources

GEORAPHICAL COVERAGE

EU, US, APAC, EMEA, LATAM, ANZ

GEOGRAPHIES COVERED IN OUR ASSESSMENTS

SELECT INDUSTRY CREDENTIALS

GOVERNMENT
IT / ITeS
BFSI
TELECOM
OIL & GAS
LOGISTICS
MEDIA
AVIATION
AUTO

SELECT PRIVACY REGULATIONS

GDPR, PDPA – MALAYSIA & SINGAPORE, CHINA, IRR, HIPAA, CCPA, PDPB, US REGULATIONS, DIFC,ANZ

DATA INVENTORIZATION

800+

RECORDS OF PROCESSING ACTIVITIES PREPARED

APPLICATION ASSESSMENTS

1200+

DATA FLOW DIAGRAMS

900+

DATA FLOW MAPS CREATED

PRIVACY IMPACT ASSESSMENTS

1100+

PRIVACY RISK / IMPACT ASSESSMENTS PERFORMED

PRIVACY TOOLS

KPMG K - WASP

OneTrust Privacy

PrivacyAI

Let's have a look at our Global Cyber Presence

KPMG Cyber practice assists organisations in transforming their security, privacy, and continuity controls while maintaining the confidentiality, integrity, and availability of critical business functions. Our approach to cybersecurity is aligned with client business priorities and compliance needs.

KPMG Business Units

- Audit
- Tax
- Advisory

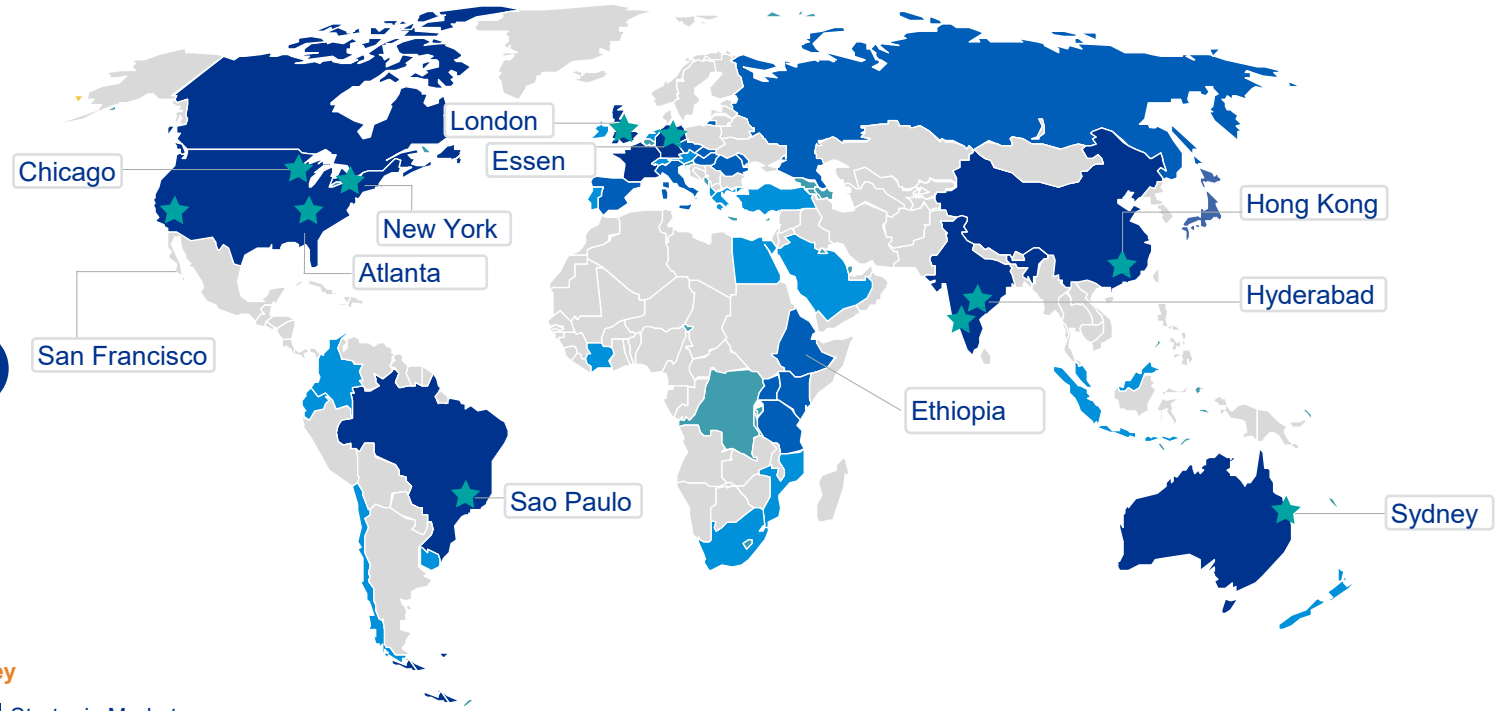
40,000+

Our Corner of KPMG

- Deal Advisory
- Management Consulting (MC)
- Risk Consulting (RC)

18,000+

- KPMG Cyber



Key

- Strategic Markets
- High-Growth Markets
- Investment Markets
- Key City

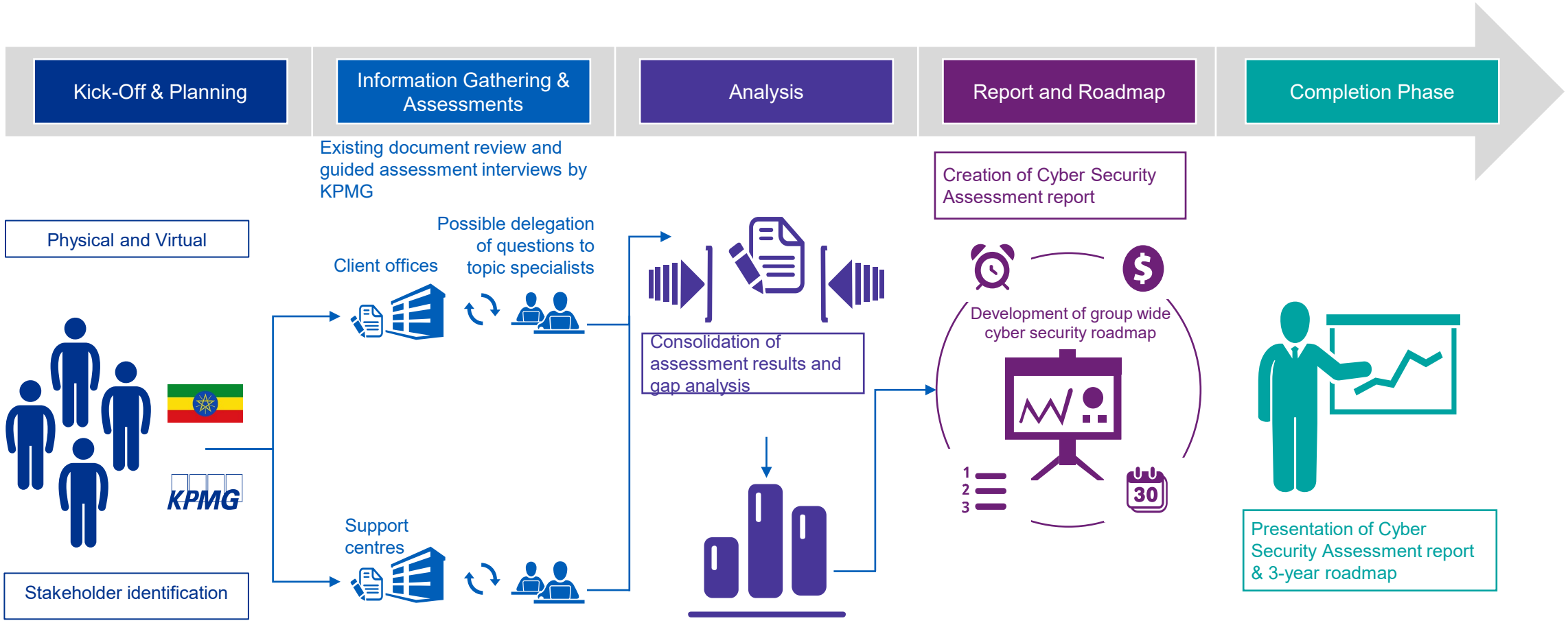
- A global network of 18000+ risk management professionals
- A global network consisting of 3000+ cyber security professionals
- Member firms located in key markets around the world that can be leveraged where needed

Our service offerings

	Strategy and governance	Transformation	Cyber defense	Cyber response
	Nancy Mosa	*Anthony Muiyuro*	*Anthony Muiyuro*	*Samuel Keter*
Core services	— Cyber maturity assessment (CMA) — Compliance assessment — Cyber security strategy — Information governance and privacy — Third-party security risk management — Business resilience	— Enterprise identity and access management (IAM) — Consumer identity and access management (CIAM) — Privileged access management — Cyber GRC — Technology integration — Security architecture — Cyber program delivery	— Technical security assessments — Security operations and monitoring — Patch and vulnerability management — Application security — Insider threat	— Compromise assessment and simulations — Incident response readiness and planning — Digital investigations and remediation — Threat intelligence — Red Teaming
	Cloud security – *consumer adoption* | *service providers*			
	Secure automation			
	Secure DevOps			
	Operational technology resiliency and transformation			
	Cyber managed services			

Executing the Cyber Maturity Assessment

The five phased Cyber Maturity Assessment approach follows a logical sequencing to help ensure that we validate findings through the process and seek feedback on an iterative basis. In addition to alignment, this engages stakeholders throughout the process.

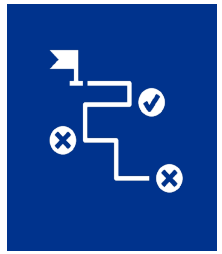


Deliverables – Assessment Report and Roadmap

Cyber Security Assessment Report

The identification of policy, process, personnel, and technical vulnerabilities with asset and critical details based on the assessment.

The identification of existing and proposed safeguards, and an assessment of their adequacy.



An analysis of the consequences/impact of potential threats, and an evaluation of the likelihood of occurrence

Benchmarking of the organization's security posture against similar industry (international organizations, or equivalent)/best practices/maturity scale

Roadmap - Detailed and achievable recommendations report based on issues identified in assessment

Contact us:

Brian DeSouza
Partner, Risk Consulting
KPMG Advisory Services Limited
M: +254 709 576 132
E: briandesouza@kpmg.co.ke

David Leahy
Partner, Risk Consulting
KPMG Advisory Services Limited
M: +254 709 576 833
E: davidleahy@kpmg.co.ke

Nancy Mosa
Partner, Risk Consulting
KPMG Advisory Services Limited
M: +254 709 576 133
E: nmosa@kpmg.co.ke

Bernard Amukah
Partner, Risk Consulting
KPMG Advisory Services Limited
M: +254 709 576 250
E: bamukah@kpmg.co.ke

Abiy Fesseha
Director, Risk Consulting
KPMG Advisory Services Limited
M: +254 202 806 000
E: abiyfesseha@kpmg.co.ke

kpmg.com/socialmedia

Download on the App Store

kpmg.com/app