Stop assuming – start anticipating

From Cyber Security to Cyber Resilience

—

Markus Limbach

The dramatic evolution of today's cyber-threat landscape

Every 11 seconds a company falls victim to a ransomware attack[(a)]

This sums up to >80 during the course of this presentation

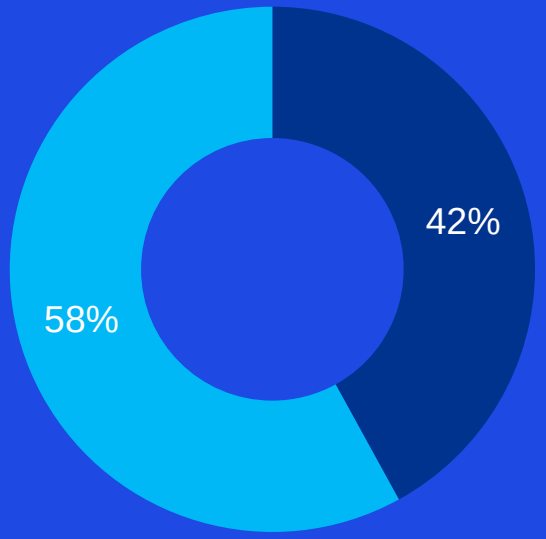
Source: (a) According to estimates from Cybersecurity Ventures for 2021

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Cybersecurity teams are struggling to keep up

- Cyber teams are under pressure to keep up with evolving threats
- Lack of key skills is the top issue
- Over half are behind schedule

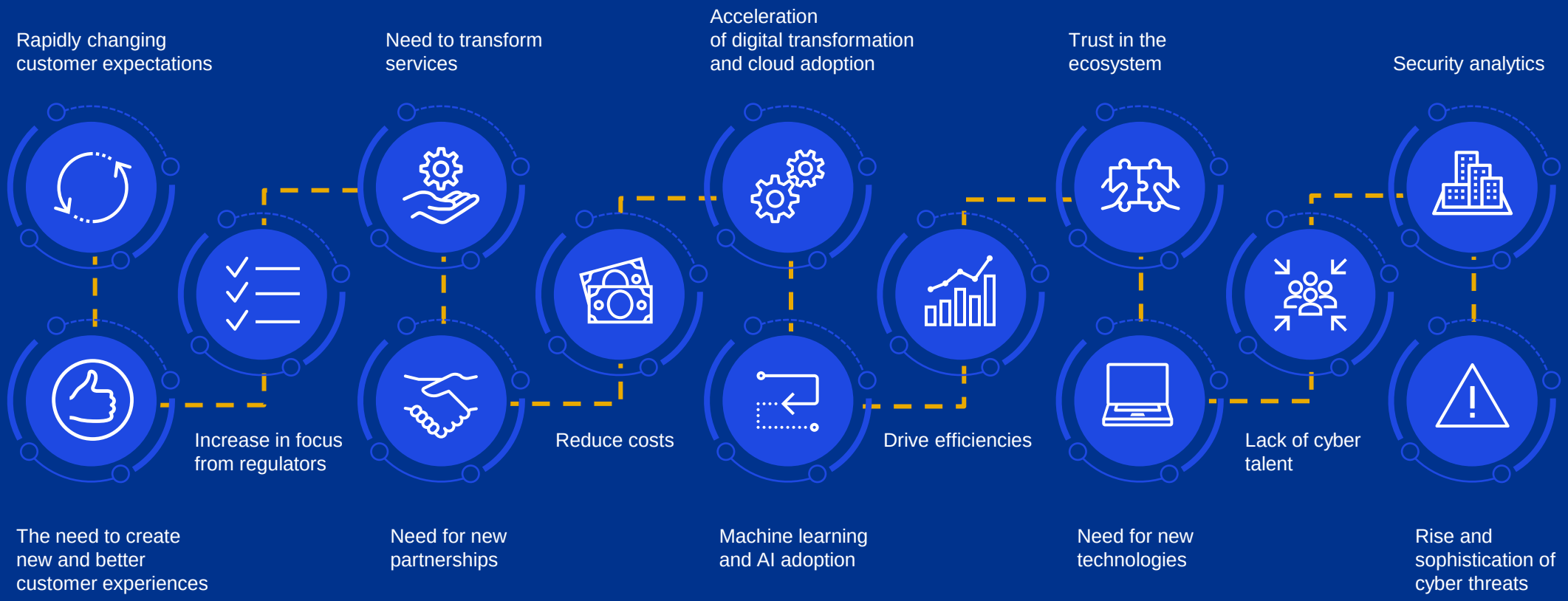
How would you describe your organization's position today in your cyber security journey?



- We are proactive in progressing against our strategy and are continually evolving
- We are behind schedule, even if plans and a vision are in place

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Cyber is a golden thread



Business drivers and outcomes — **Technology drivers and outcomes** — **Cyber drivers and outcomes**

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Reframing the “assume breach” conversation

assume

to take for granted or without proof

anticipate

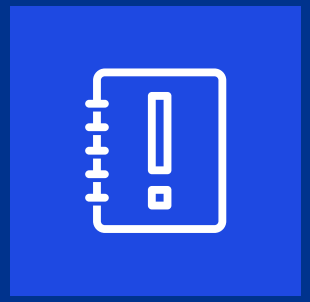
to realize beforehand; foretaste or foresee
to perform (an action) before another has had time to act
to nullify, prevent, or forestall by taking countermeasures in advance

Source: www.dictionary.com

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

What happens if a breach happens?

Start anticipating...



... the breach

... the most realistic breach scenario

... the first 5 days after the breach

... the necessary decisions and decision structures

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Understand, anticipate, and be prepared to recover

01
Evaluate Customer Perspective

Consider how long you can sustain the business if significant functions are down and what it would mean from a customer impact perspective.

02
Evaluate Supplier Perspective

Think about how a significant cyber event would affect your dependency on suppliers.

03
Raise Board Awareness

Elevate the topic of cyber security and cyber resilience to board level.

04
Check/Update Existing Plans

Question whether your current resilience plans are fit for purpose for a cyberattack and take appropriate corrective measures.

05
Challenge Assumptions

Have the humility to acknowledge that your assumptions might be wrong — and an alternate plan that can be operationalized quickly.

06
Exercise

Help the C-suite develop their crisis management capabilities and their individual roles in the event of a cyberattack through regular, real-world simulations.

KPMG

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Document Classification: KPMG Confidential

Using a Zero Trust framework to connect the silos

01 Business drivers

- Digital Transformation & Cloud
- Global supply chain
- Remote working/ Global workforce
- 3rd party ecosystem & Partners
- M&As/ Divestitures

02 Enterprise concerns

- Flat network allowing Lateral movement
- Limited Asset inventory
- Open access (VPN)
- Limited visibility of events, behaviours and risk
- Reactive approach to Security

03 Macro trends and influence

- Market/vendors
- Analysts Forrester/ Gartner etc.
- Security leaders and organisations (NIST, etc.)
- Hyper-scalers (AWS, GCP, MS Azure)
- Federal government and agencies

KPMG

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Document Classification: KPMG Confidential

Zero trust is the way forward

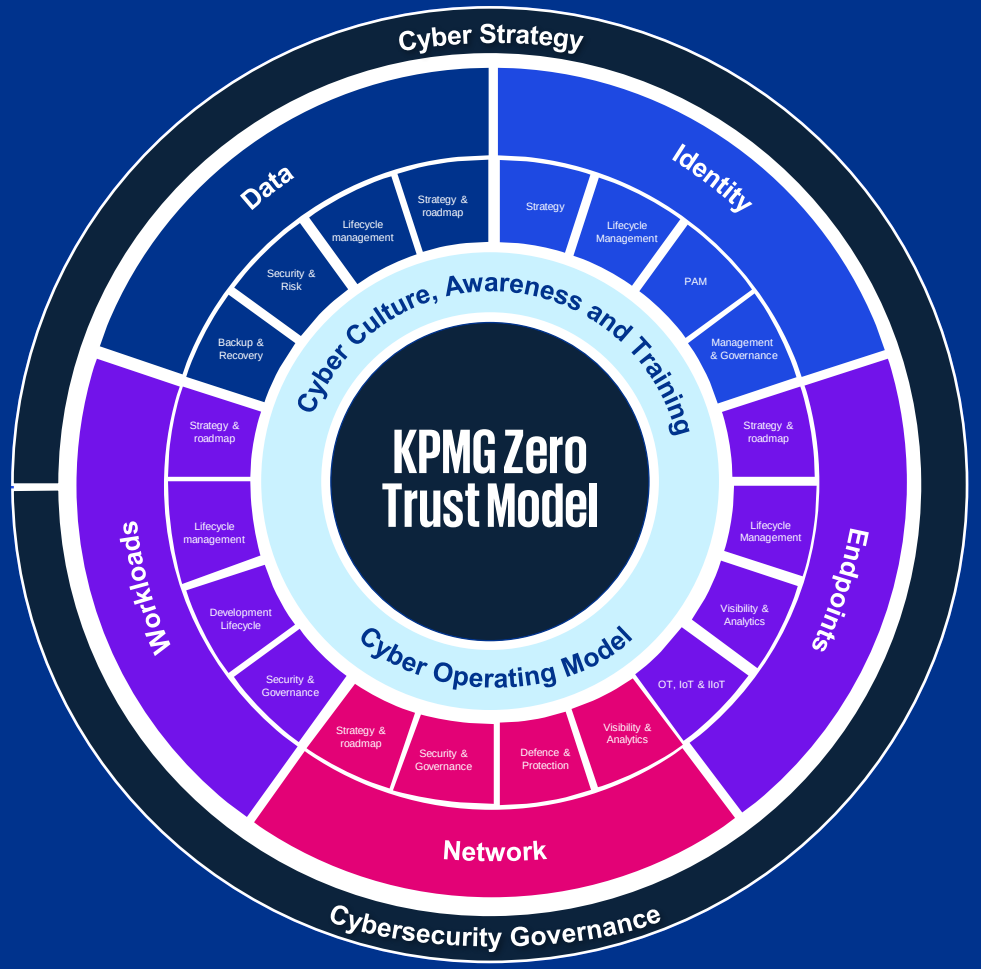
Put user identity, access management and data at the heart of cyber security

3 Key Principles

- Assume nothing (never trust)
- Check everything (always verify)
- Limit access (least privilege)

3 Key Must-Do's

- Ensure that a community is set up and collaborating
- Connect the dots/join the silos/integrate
- Training and awareness so users are the first/last line of defence



© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.


KPMG

Contact

Markus Limbach
Partner, Cyber Security
T +49 174 3001998
mlimbach@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft
Barbarossaplatz 1a
50674 Cologne
Germany

kpmg.de/socialmedia

kpmg.de

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG AG Wirtschaftsprüfungsgesellschaft, a corporation under German law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Document Classification: KPMG Confidential