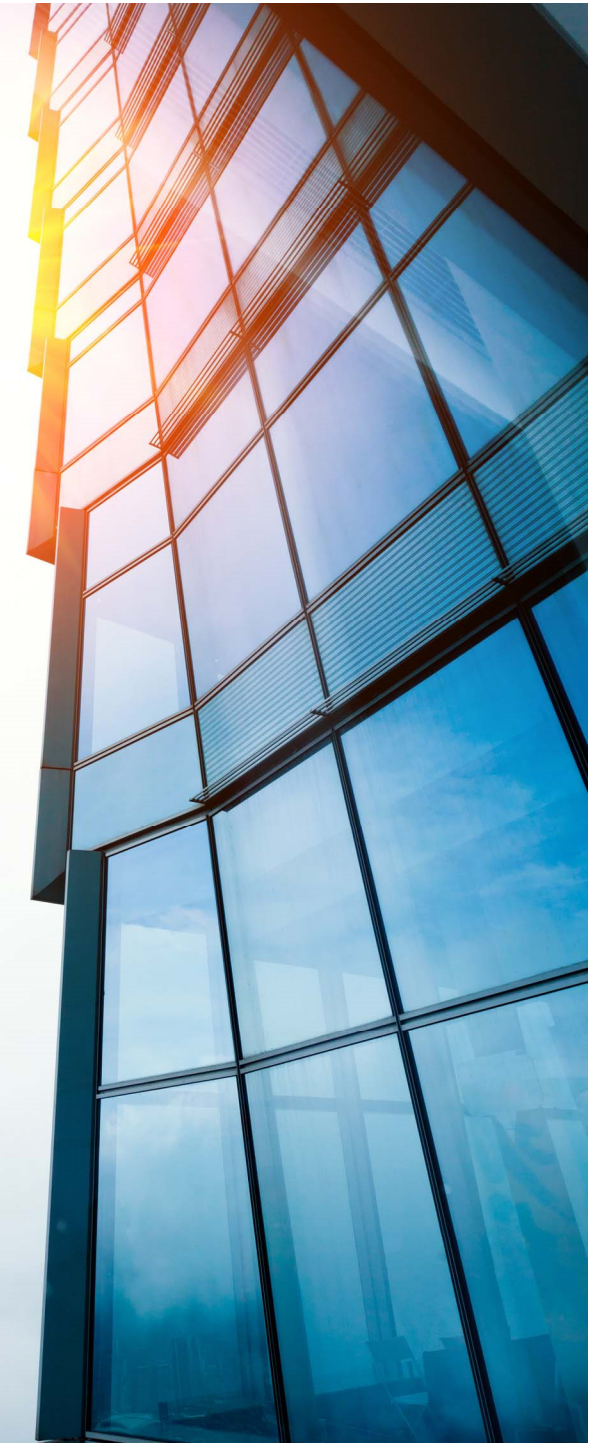
KPMG

Cyber Security Panel

MFM Conference – Panel Discussion with Tribune Media Company

May 21, 2019



Agenda

- KPMG Cyber Security Trends and the Evolving Threat Landscape
- Tribune Cyber Security History and Perspectives
- Lesson Learned from Recent Cyber Incident at Tribune
- Questions

Forbes Insights and KPMG Cyber Survey	
What would your organization need the most to be more effective in cyber security?	
Stronger processes	27%
More technology	22%
Better strategy	21%
Increased funding	19%
Better quality staff	7%
More staff	4%

Do We Have Our Eyes Open?

More than half of organizations say it is unlikely or **highly unlikely that they would be able to detect** a sophisticated attack. (iTreasurer)

Once detected, it can take **months** to resolve a breach (Verizon)

Data production will be **44 times greater** in 2020 than in 2009 (IDC) making analysis and monitoring even more difficult

For most companies, it takes **over 6 months** to even realize they have been breached. (Ponemon)

Only 31% of organizations discovered they were breached through their own resources - Most are **informed of a breach by third-parties** (Mandiant/FireEye)

In recent years, the percentage of companies affected by a successful cyberattack is **71%** (NetIQ)

In 60% of cases, attackers were able to compromise an organization **within minutes** (Verizon)

Just 55% of organizations feel they have adequate resources for handling security incidents (KPMG Survey)

…There is a growing deficit between how quickly attackers can compromise vs. how quickly organizations can detect and respond. *In other words, Attackers are improving faster than defenders…*

KPMG

Cyber Security Trends and the Evolving Threat Landscape

Changing Board Reporting Trends

Board level awareness of emerging cyber threats and direct involvement in determining the response is critical and growing.

Key trends include:

Boards have moved to at least a **Quarterly** update on Cyber Security and its impact to Strategy discussions. *(Is Cyber part of the Board's regular strategy discussions?)*

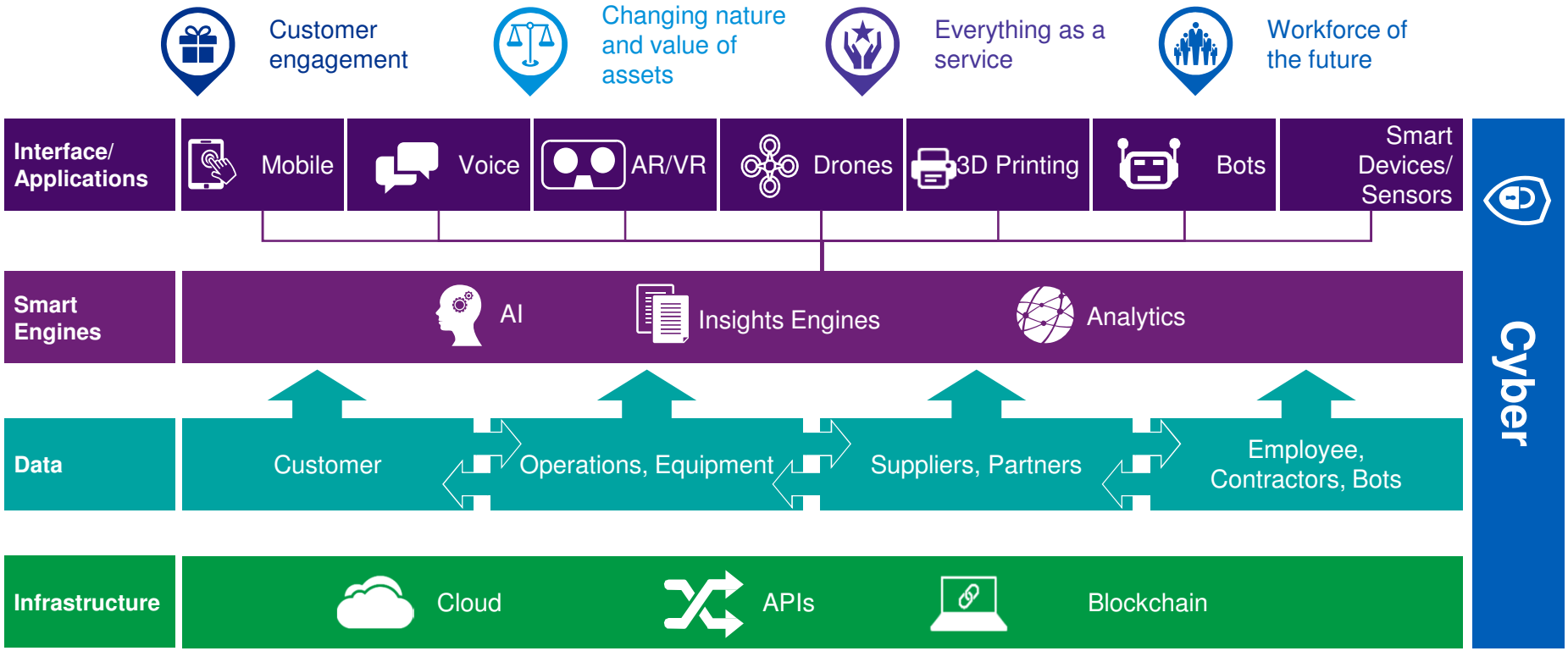
Boards want to know the CIO / CISO **know when and how to act** in a Cyber incident, and are **empowered** to act.

Key shift in direction from reactive and detection to **proactive** and **resilient**

- Are we Resilient enough to meet out risk and downtime tolerances?
- What progress have we made in moving from reacting to anticipating cyber attacks?

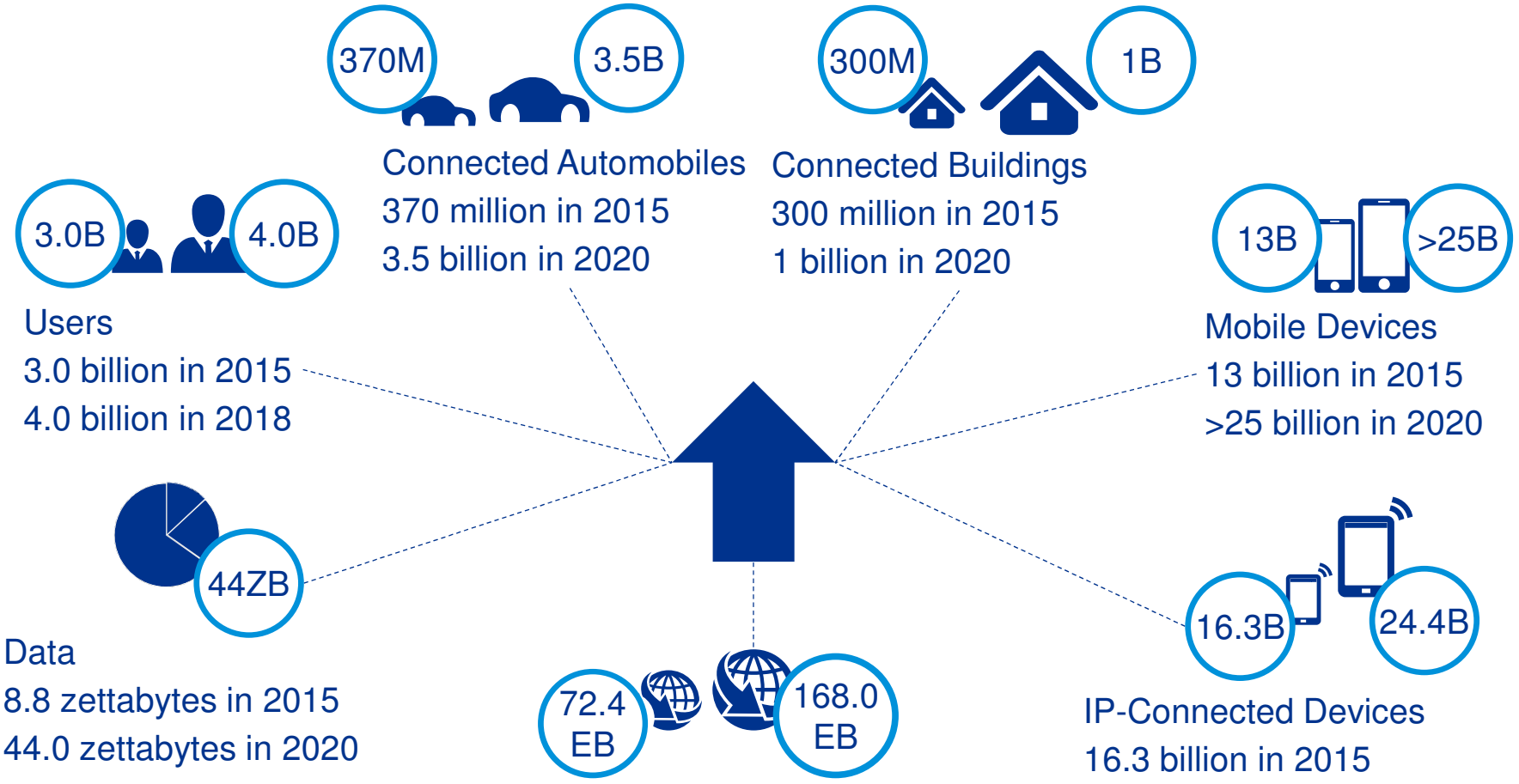
Boards want to know how the Cyber threats translate into a **Business Context** and compare to other risks. *(How do we demonstrate the ROI on our Cyber Investments?)*

The 21st Century Enterprise



Security by Design must be at the heart of the digital transformation efforts underway across numerous industries and technology enablers.

New Platforms Mean New Threats



Sources: McAfee Labs (2015)
State of the Market: The Internet of Things 2015, Verizon (2015)

Current Cyber Security Trends

Extortion-driven attacks, **ransomware** and **targeted phishing** attempts will increase and will become more threatening, more sophisticated and destructive

Customer data privacy and protection are driving business decisions and requires new thinking to embed Privacy into the DNA of the business

Widespread Cyber **skills shortages** are amplifying the need to increase **Automation**, AI and SOAR to increase efficiency and effectiveness of human time

Insider threat will be brought into greater focus as technology improves, allowing visibility into credential abuse

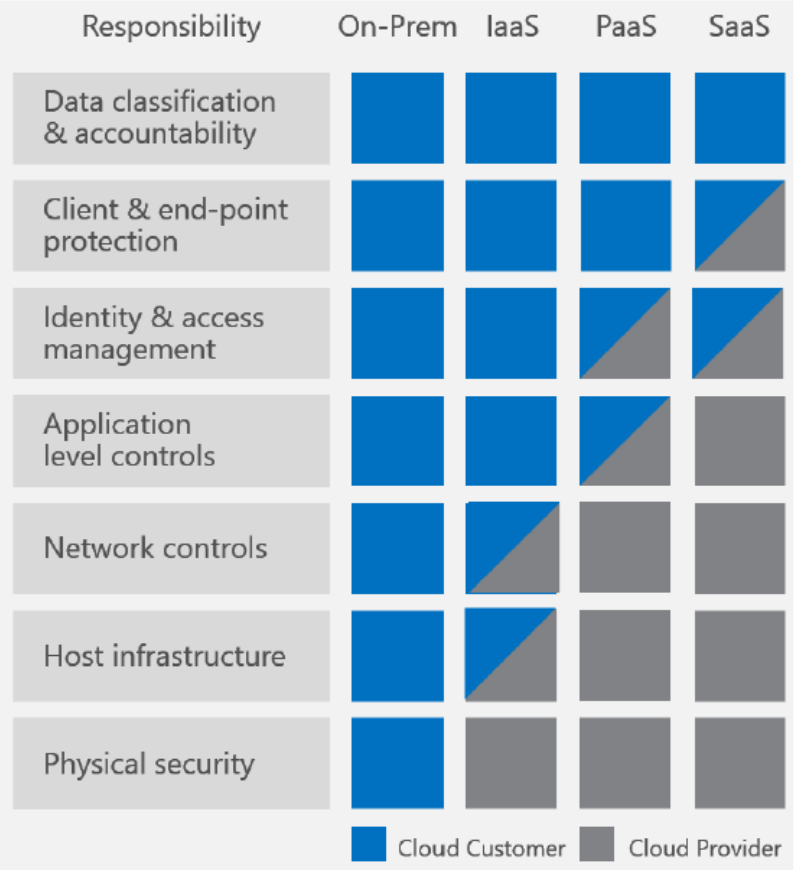
Organizations will focus much more on risks posed by **third-party vendors** and **suppliers**

Advanced **digital identities** and **authentication** are key business enablers that will improve the customer experience, secure data, prevent fraud and engender **trust**

Cloud Risks in part stem from shared responsibility model

1. The adoption of cloud introduces a shared responsibility model for security
2. Consumers have the most responsibility with IaaS and least with SaaS cloud models
3. This shared responsibility model can create confusion and risk exposures for cloud consumers if not properly understood and addressed

Organizations should clearly define cloud security roles and responsibilities and ensure cloud vendor contracts, cloud vendor implementations, and control operations address gaps.



Source: Microsoft what does shared responsibility in the cloud mean https://blogs.msdn.microsoft.com/azure security/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

Call to Action

New threat model

- Organizations have to align their security programs to the new threat model
- Full attention should be paid to the insider threat as well as the external attacker

Compliance does not equal cyber maturity

- Organizations need to assess cyber maturity against a more rigorous standard, not just regulatory compliance
- Integrate cyber security with compliance to drive organization wide initiatives
- Stronger reporting structure for the TOM (target operating model) and responsibility to not just the CIO but also to Compliance and the board

Security threats are not confined to your own organization

- Organizations have to improve their communications both internally and externally
- Integrated cyber security technologies, with strong reporting and monitoring capabilities

Increase cyber Investments – In the right order

- We need to invest in cyber security across the paradigm of people, process and technology
- Only invest in technology with a measurable plan!
- Attend to the basics first, build the right foundation before trying to advance

kpmg.com/socialmedia