Cyber Internal Audit
ISACA

Dale Bancroft

January 2019

pwc

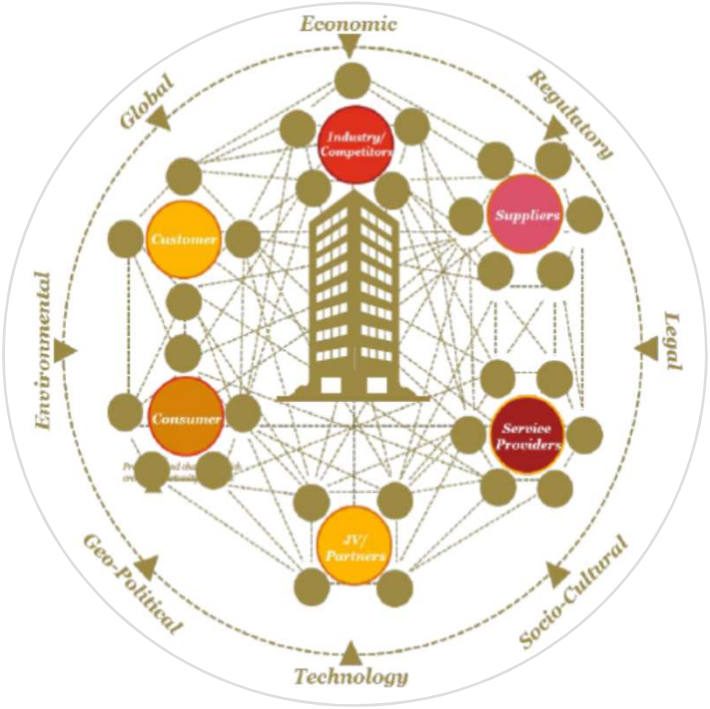
Agenda

- *Cybersecurity Landscape*
- *Keeping CEOs Up at Night*
- *Yesterday's mindset*
- *Three lines of defense*
- *Questions for internal audit*
- *Planning a Cyber Internal Audit program*

Cybersecurity Landscape

Then

- Few standards of connectivity and collaboration
- Integration limited
- Low risk, low opportunity



Now

- Connectivity and collaboration extend to all facts of business
- Integration with wide range of business stakeholders, competitors and trading partners, in a dynamic environment built on trust
- High risk, high opportunity

You're more connected than ever

Business are increasing interconnected, integrated, and interdependence where innovation and technology coverage is creating opportunity and risk.

Keeping CEOs Up at Night

Concerns around **cyber threats** rise

Q: Considering the following threats to your organization's growth prospects, how concerned are you about the following?

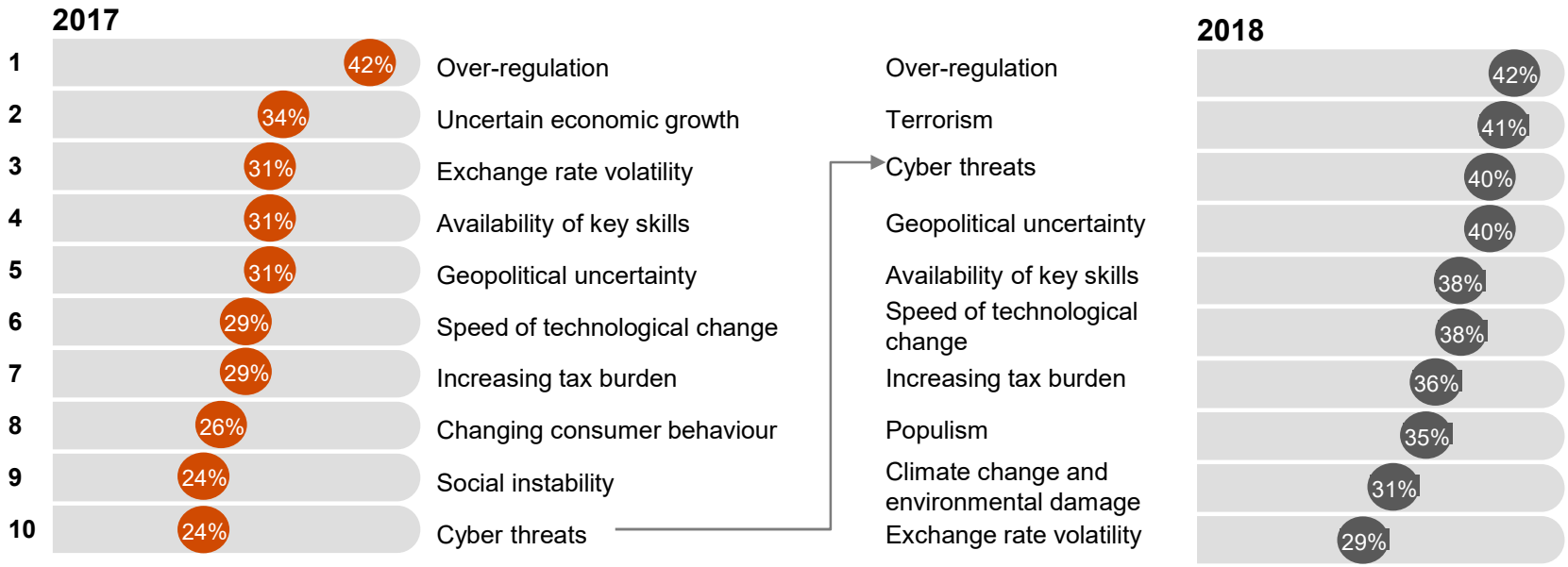
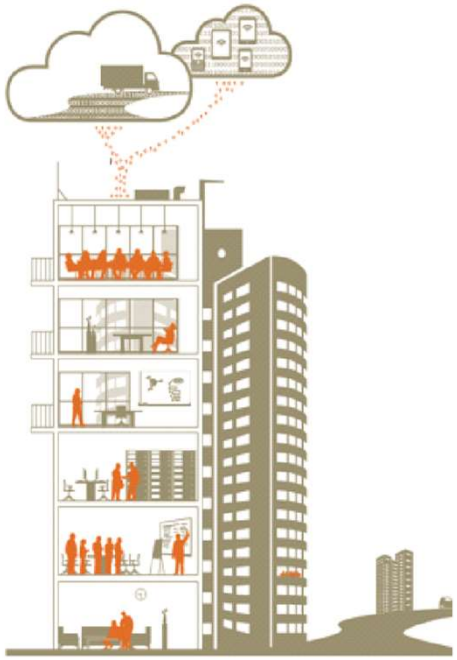


Chart shows percentage of respondents answering '*extremely concerned*'.

Source: PwC, 21st Annual Global CEO Survey

Keeping CEOs Up at Night



As high profile cyber attacks become more common, executive management teams and boards are becoming more concerned around key risk questions relating to cybersecurity:

- Is the business resilient to a cyber attack?
- Are there gaps in our cybersecurity capabilities?
- Which threats should we be most concerned about?
- How much risk are we willing to take?
- Could a cyber incident impact our business?
- Are we spending in the right areas?

91% of interviewed CEOs believe stakeholder trust will be negatively impacted by cyber security breaches on business information or critical systems within the next year 5 years.

Source: PwC's 2017 CEO Survey, January 2017

To exercise their fiduciary duty, boards need comfort that they have a "**defensible**" cybersecurity risk management program in place.

Yesterday's Mindset

Three Lines of Defense

Business

- Articulate business objectives and strategy.
- Own the cyber risks associated with people, processes, and technologies
- Assess material cyber risks and associated threats
- Escalate changes in the business or the risk environment that could affect the exposure to cyber risks

1

Information Technology

- Build and operate the environment in alignment with business objectives and strategy
- Establish and adhere to technical standards and procedures for cyber risk management
- Design, deploy, maintain, monitor and test controls for cyber risk management
- Identify and analyze emerging threats from external sources

Risk Management / Infosec

- Establish risk management frameworks
- Independently identify and assess the material aggregate cyber risks.
- Perform independent risk-based monitoring and testing of key cyber risk-related controls
- Perform a credible challenge of first line of defense
- Report on enterprise-wide material cyber risk

2

Internal Audit

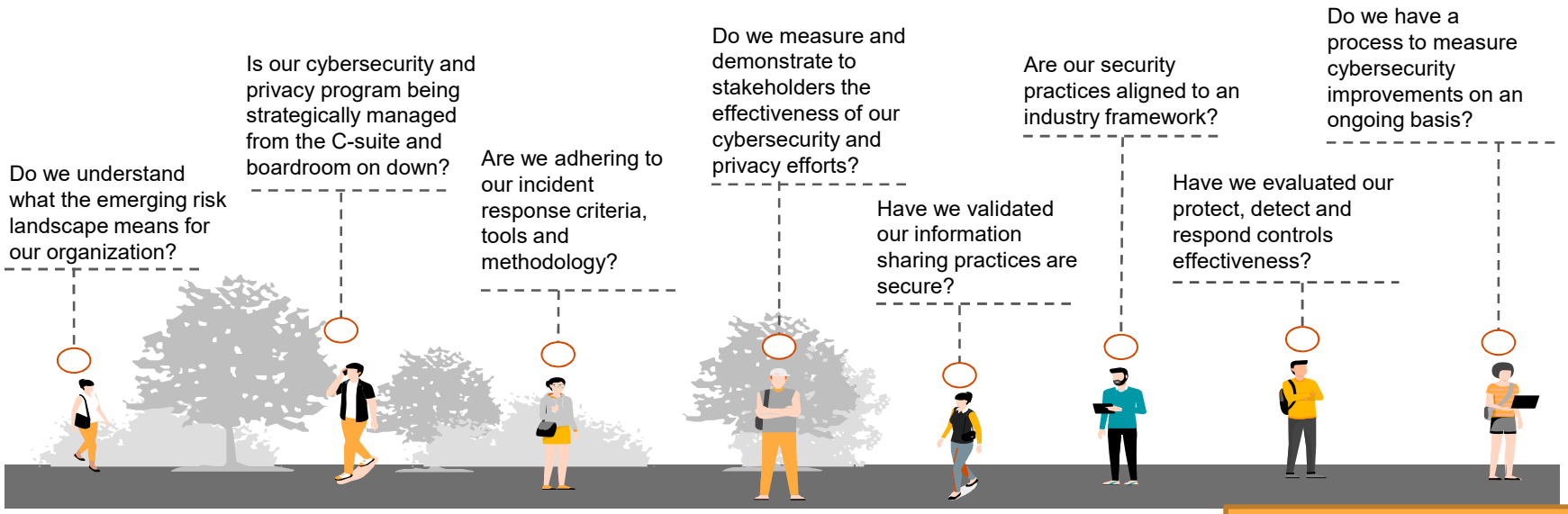
- Provide independent review of the cyber risk management framework
- Perform independent review and assessment of cyber risk program effectiveness
- Update leadership, appropriate management and risk committees, and the Board on the effectiveness of the cyber risk management program and activities

3

Questions for Internal Audit

As data, and then information, take on a digital form, the ability to manage, govern, and secure it becomes increasingly more important. Internal audit teams can help validate that day-to-day controls for security and privacy are effective.

Internal Audit should be asking these questions:



Example: 3-Year Audit Program

A Cybersecurity and Privacy audit plan can be developed by grouping risk areas that make sense together into auditable areas, and prioritizing based on risk and last review. A baseline plan with five audits per year is shown (topics/numbers will vary).

Year 1	Year 2	Year 3
Cybersecurity Maturity Assessment	Nontraditional IT (OT, IOT, or RPA) Risks	Vendor cyber risk management
Incident response and recovery	Encryption/Data Protection/Data Loss	SDLC/Web application testing
Active directory/PAM/IAM	Cloud (IaaS, PaaS, or SaaS)	Contextual regulatory (HIPAA or PCI)
Privacy (overall)	Resiliency to attacks	Key Cyber Technology Audits
Internal/external penetration testing	Vulnerability and patch management	Internal/external penetration testing

While some organizations have moved away from multi-year audit planning to be more responsive, cyber and privacy are areas where it makes sense for most firms to still have a multiyear outlook, given how expansive the topics are.

The audit plan should be re-evaluated on an annual basis and adjusted as needed. Note that **the above baseline plan is not meant to be adopted without customization**, but it does showcase key risk areas for many companies.