MARSH

WHY INSURANCE IS KEY TO MANAGING CYBER RISK

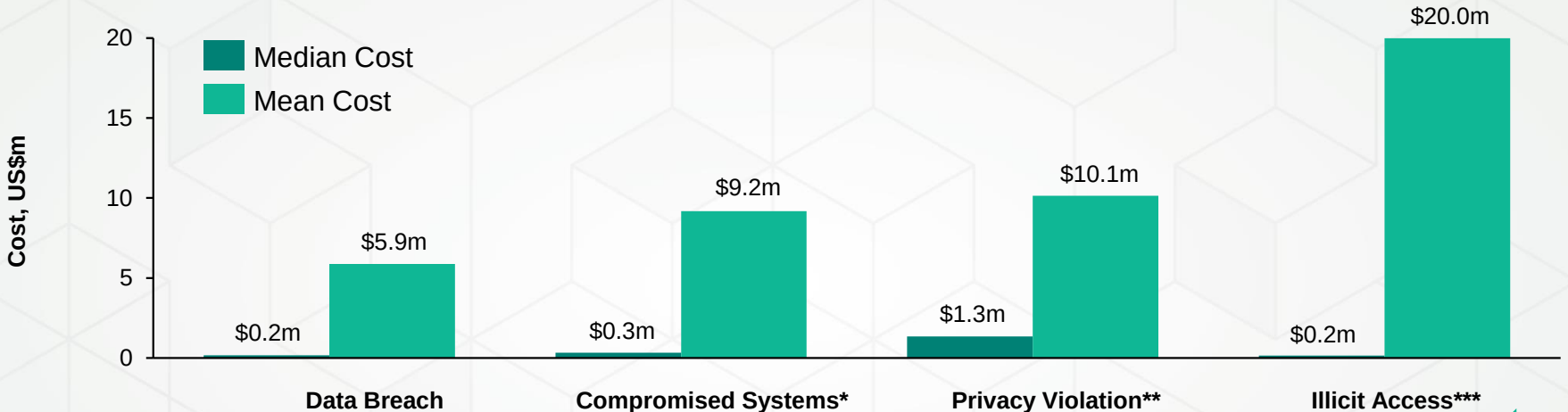
PETER JOHNSON
Marsh UK Cyber Advisory Leader

AGENDA

1. The cyber situation.
2. Lessons on managing cyber risk.
3. Insurance and cyber risk.
4. Questions every organisation should be asking themselves.

CYBER SITUATION

The Median Cost of an Event is Low, But There is a Large Tail Risk



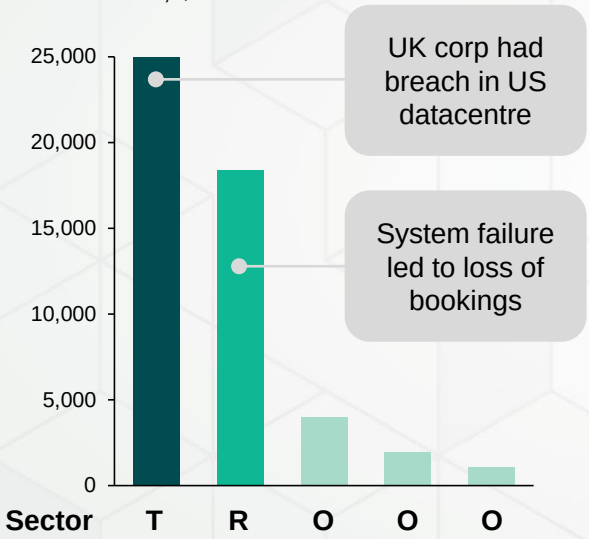
	Data Breach	Compromised Systems*	Privacy Violation**	Illicit Access***
Maximum Cost, $m	$572m	$100m	$750m	$710m
Number of Events	602	36	234	49

*Compromise or disruption of corporate IT systems or intellectual property – e.g. a DDoS attack
**Unauthorised collection, use and/or sharing of PII by a firm
***Computer or electronic crimes directly against other individuals or firms including phishing attacks, identity theft, or skimming attacks
All data refers to a 10-year period from 2005 to 2014 for a sample of incidents where cost estimates are publicly available
Source: S. Romanosky, "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, August 2016
M=million

CYBER SITUATION

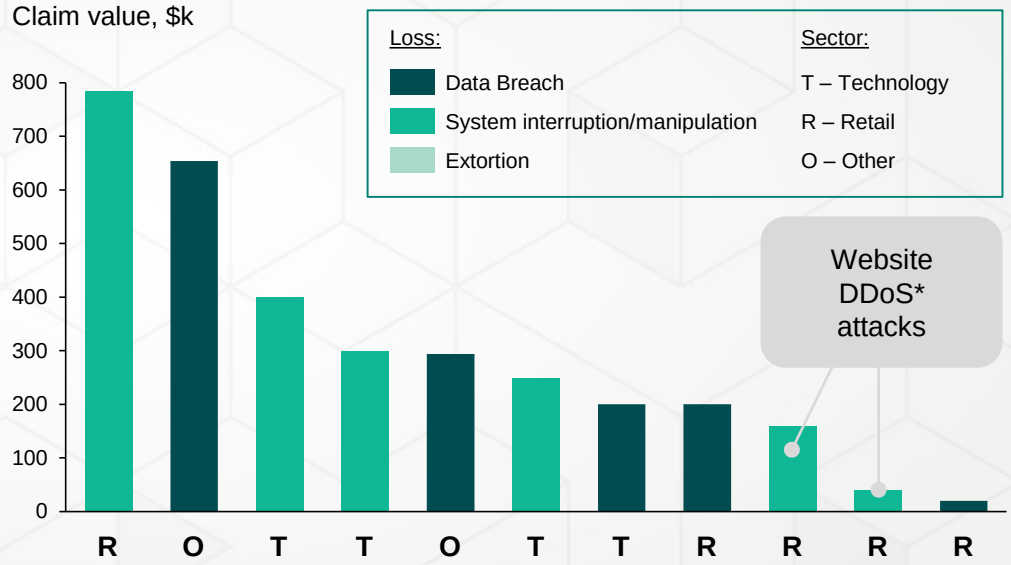
We are Seeing a Variety of Claims Across Multiple Sectors

Claims > US$1M



Claims < $1M

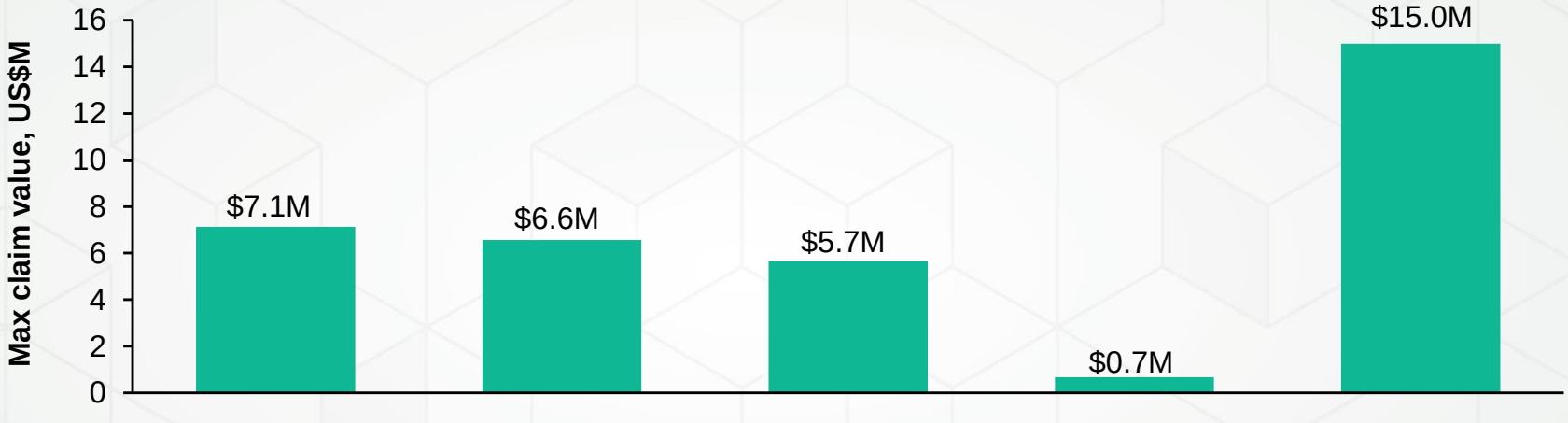
Note: Representative but non-exhaustive



Source: Marsh claims (selected)
'Other' sectors include gambling, construction, education, hospitality, and professional services
*DDOS: Distributed Denial of Service

CYBER SITUATION

Smaller Companies Can Still Have Large Losses



	Nano-Revenue (<$50m)	Micro-Revenue ($50m-$300m)	Small-Revenue ($300m-$2bn)	Mid-Revenue ($2bn-$10bn)	Large-Revenue (10bn+)
Number of Claims	86	44	23	10	9

Source: NetDiligence 2016 Cyber Claims Study
Sample size of survey:176; 4 with unknown revenue not shown
M=million
Bn=billion

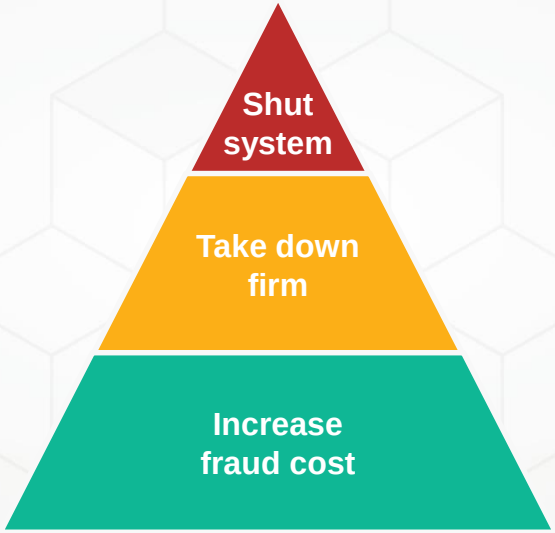
LESSONS ON MANAGING CYBER RISK

Focus on Big, Avoidable Impacts

MOTIVATION

Take data
Steal money
Steal IP
Prevent trading
Embarrass firm
Cause damage

IMPACT



SANCTIONS

Client contracts
GDPR/NISD
FTCA (US)
ICO
Viability statement
FCA/SMR

GDPR: General Data Protection Regulation
NISD: Network and Information Security Directive

FTCA: Federal Tort Claims Act
ICO: The Information Commissioner's Office
FCA/SMR: Financial Conduct Authority/The Senior Managers Regime

LESSONS ON MANAGING CYBER RISK

Cyber is Not an 'IT' issue

WannaCry* – Ransomware attack

- **Cause:** Worm that exploited unpatched vulnerabilities of Microsoft Windows.
- **Immediate impact:** Encrypted HDs, causing systems to stop working.
- **Business impacts:**
  - IT Disaster recovery – IT problem.
  - Business continuity – halting of operations (services/production).
  - Quality of operations – inability to access/record patient records.
  - Crisis management – press, customers, front line staff.
  - Global economic losses estimated at US$8 billion** (Cyence).

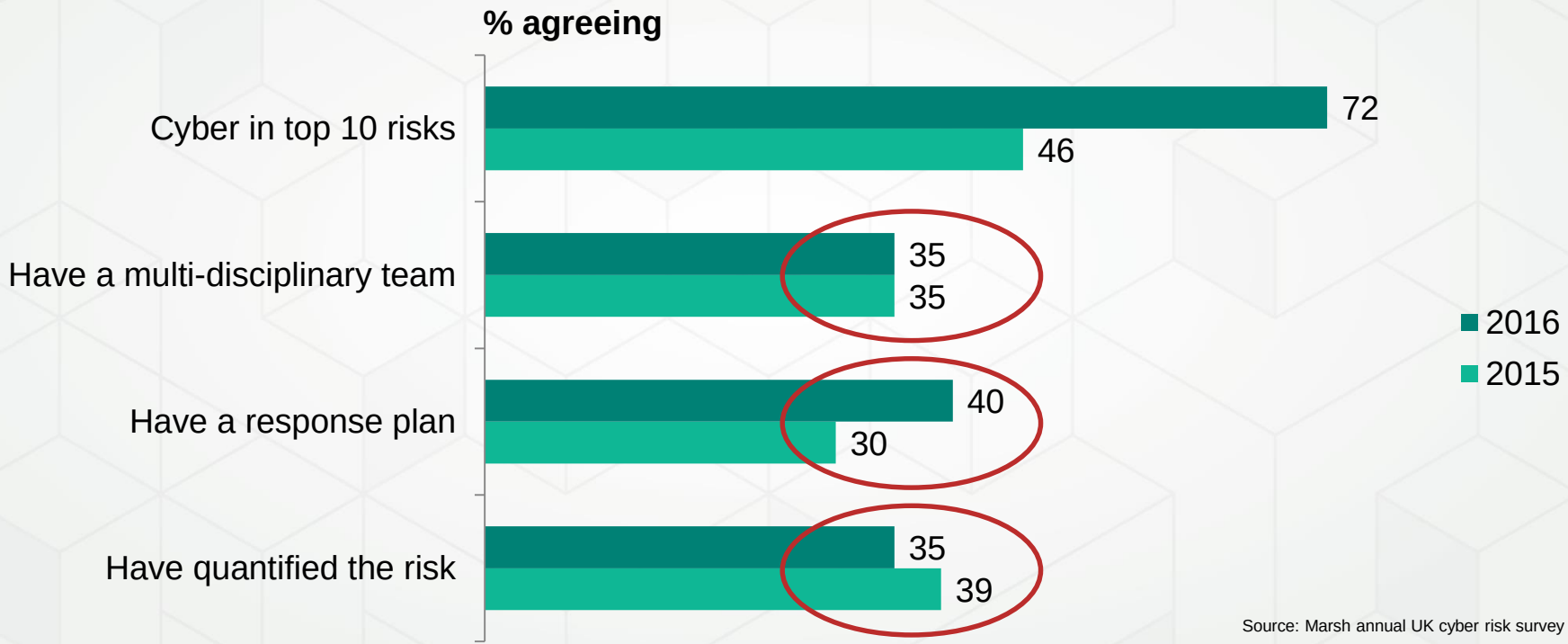
British Airways

- **Cause (official):** Global IT failure due to power surge to the UK data centre.
- **Immediate impact:** Flight-grounding systems to stop working.
- **Business impacts:**
  - IT Disaster recovery – IT problem, back-up servers failing.
  - Services disruption – 75,000 of grounded passengers, flights cancelled***.
  - Increased cost of working – additional passenger services/ compensation due to delay/cancellation.
  - Reputational damage.
  - Financial cost estimated at GBP100+ million****.

*http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/
** http://www.insurancebusinessmag.com/asia/news/breaking-news/reinsurance-to-take-minimal-losses-from-wannacry-am-best-68536.aspx
***http://www.standard.co.uk/news/uk/ba-boss-apologises-for-catastrophic-it-failure-that-caused-havoc-for-75000-people-a3551666.html
**** https://www.theguardian.com/business/2017/may/28/british-airways-faces-100m-compensation-bill-over-it-meltdown

LESSONS ON MANAGING CYBER RISK

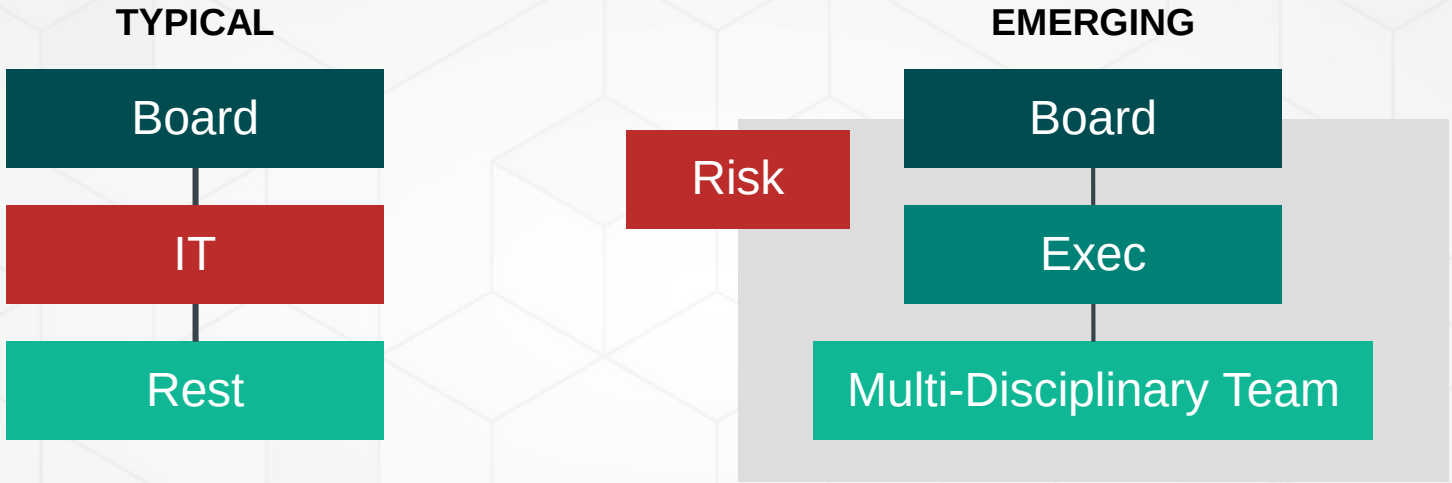
Firms are Improving, but Slowly



Source: Marsh annual UK cyber risk survey

LESSONS ON MANAGING CYBER RISK

Improve Governance



95% of cyber incidents result from human error*

52% of data breaches are caused by employees**

*Source: IBM Security Services 2014 Cyber Security Intelligence Index report, page 3. https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

**2015 year study from CompTIA, research across 12 countries https://www.comptia.org/about-us/newsroom/press-releases/2016/07/21/comptia-launches-training-to-stem-biggest-cause-of-data-breaches

INSURANCE AND CYBER RISK

Risk Managers and the Insurance Community Need to do More

Risk continues to increase

- Growing set of high profile breaches.
- Added cost of sanction to worry about.
- Risk frequency and severity likely to rise.

Risk management is subjective

- Signs of greater awareness and action.
- Too reliant on experts stopping a breach.
- Lot of activity, little objective challenge.

Risk transfer is insight free

- Doubts over cover and claims.
- Doesn’t stop breaches happening.
- Doesn’t get your reputation back if they do.

INSURANCE AND CYBER RISK

Insurance Should be Key to Managing Cyber Risk

Helps define the risk

- Narrows scope to key scenarios you face.
- Forces quantification of impact.
- Connects you to lessons from other firms.

Forces financial decisions

- Defines your exposure and possible loss.
- Provides a catalyst for risk management investment.
- Creates rational financial choices.

Assists risk management

- Benchmarks your risk and risk management.
- Challenges expert opinion.
- Provides a large, reliable financial safety net.

INSURANCE AND CYBER RISK

Many Firms Appear Willing to Share Their Information

Sample size of survey:1004
Source: Cyber: in search of resilience in an interconnected world, Swiss Re/IBM, 2016

INSURANCE AND CYBER RISK

Some Common Myths

MYTH	REALITY
Only covers data breach	Most risks insurable, some already covered. Need to construct from components.
Doesn’t pay	Many large claims are being paid. Problems often stem from wrong cover.
Not enough to be relevant	Limits rising fast – GBP500 million our current ceiling. Even a small amount adds good discipline.
Doesn’t solve the problem	A rich source of benchmark information. Can drive better cyber risk management.

INSURANCE AND CYBER RISK

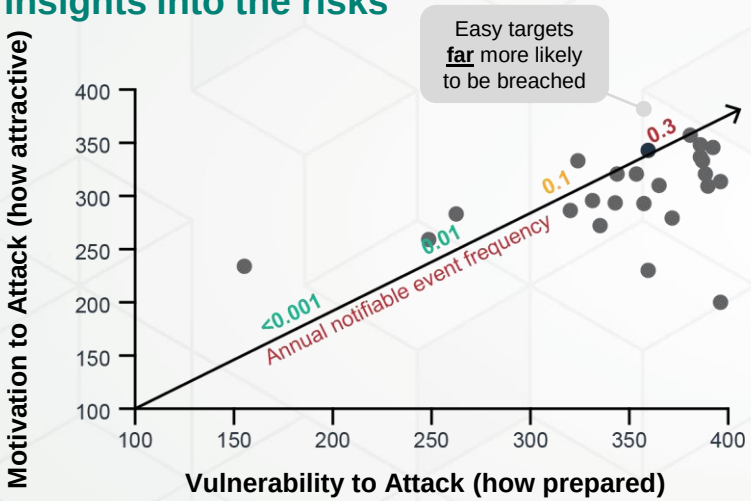
What is Currently Available

- Core coverage generally consists of:
  - Privacy liability.
  - Incident response expenses (including forensic investigation costs).
  - Digital asset damage.
  - Network business interruption.
  - Cyber extortion.
  - Multimedia liability.
- Some policies include **retroactive cover** – incidents occurring before purchase, but unknown or undiscovered until after purchase, may still be covered.
- Some policies include additional cover, with an additional limit, for **claims preparation expenses**.
  - These help you present and verify business interruption claims to insurers.
- Policy limits are available up to GBP500 million.

INSURANCE AND CYBER RISKS

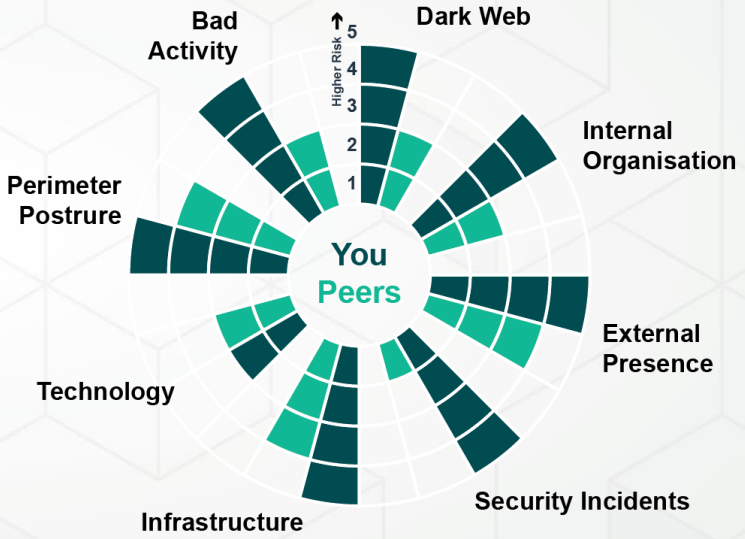
Underwriting Tools Provide Objective, Data-Driven Insights

Underwriting tools provide stochastical insights into the risks



- Non-invasive tool used by underwriters.
- Score predicts breach risk versus peers.
- 19,000 UK firms tracked, updated quarterly.

Insights into risk drivers



- Drivers of breach risk.
- Objective external data.

Source: Cyence

QUESTIONS EVERY ORGANISATION SHOULD BE ASKING THEMSELVES

1. What do senior management see on cyber risk management?
2. Are your particular risks known and quantified?
3. Do you know your vulnerability compared to peers?
4. How are expert opinions validated?
5. Do you have plans in place for a breach?
6. Has cyber turned into an insurance question?
7. Does the board think it is already covered?
8. Will your insurance pay?

MARSH

REIMAGINING RISK