

A woman with long dark hair, wearing a grey jacket, is looking down at a tablet computer. She is standing in front of a blurred cityscape at night, with various lights creating a bokeh effect. The background is dark blue and black, with yellow and white light spots.

Decode Cyber

SAS ERM-ESSEC CREAR

Cyber Risk Conference 2018

Jessica Wright
Willis Towers Watson
Regional Associate Director - Cyber

Agenda

1. Global perspective on cyber-crime
2. Insurance market growth and maturity
3. How to build a cyber resilient organisation

Prevalence of Cyber Crime in Business:

37.5%

The percentage of ransomware detections Asia-Pacific accounted for in 2017

\$148b

Estimated market size in 2021.
Insurance and L&D fastest growing

68%

Funds lost
from Cyber
attacks are
unrecoverable

US\$81.3bn

The amount of business revenue lost as a result
of cyber attacks in Asia-Pacific in 2015

Top 3

Most cited
concern across
industries

80%

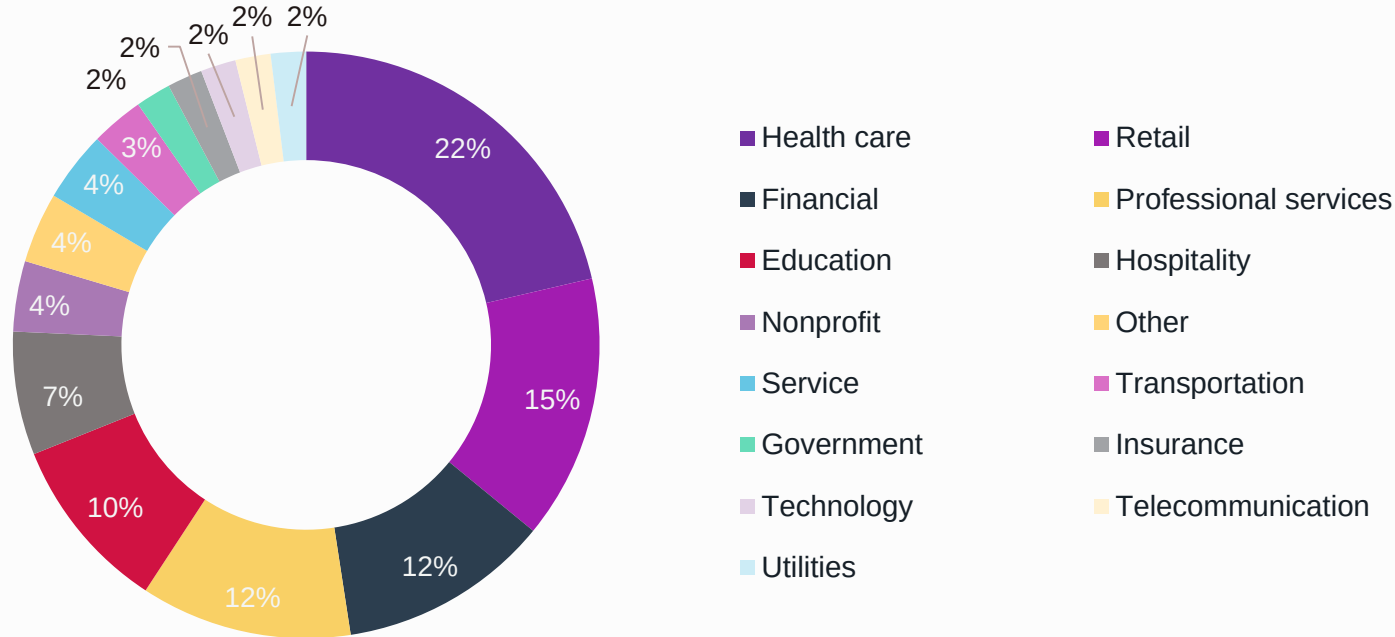
Board members
discuss Cyber at
most or all Board
Meetings

Source: Federal Government Resources

Sector impacts based on WTW cyber claim data



Hacking Incidents By Industry



Inside the Growing Threat Environment . . .



Hacker



Malicious
Employee



Negligent
Employee

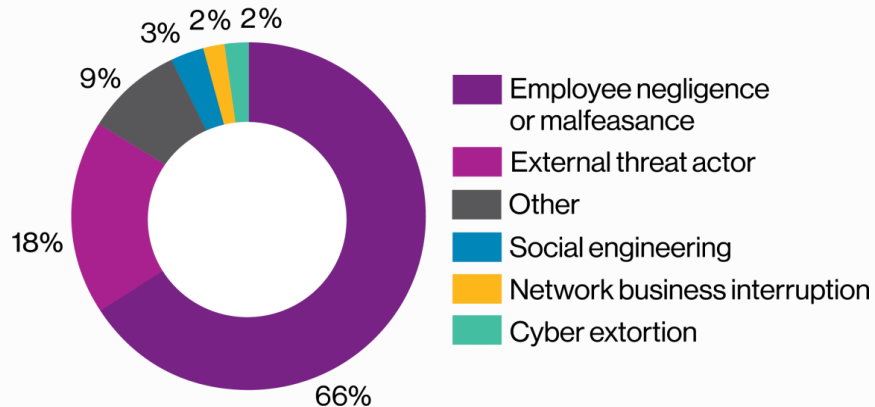


Hacktivist

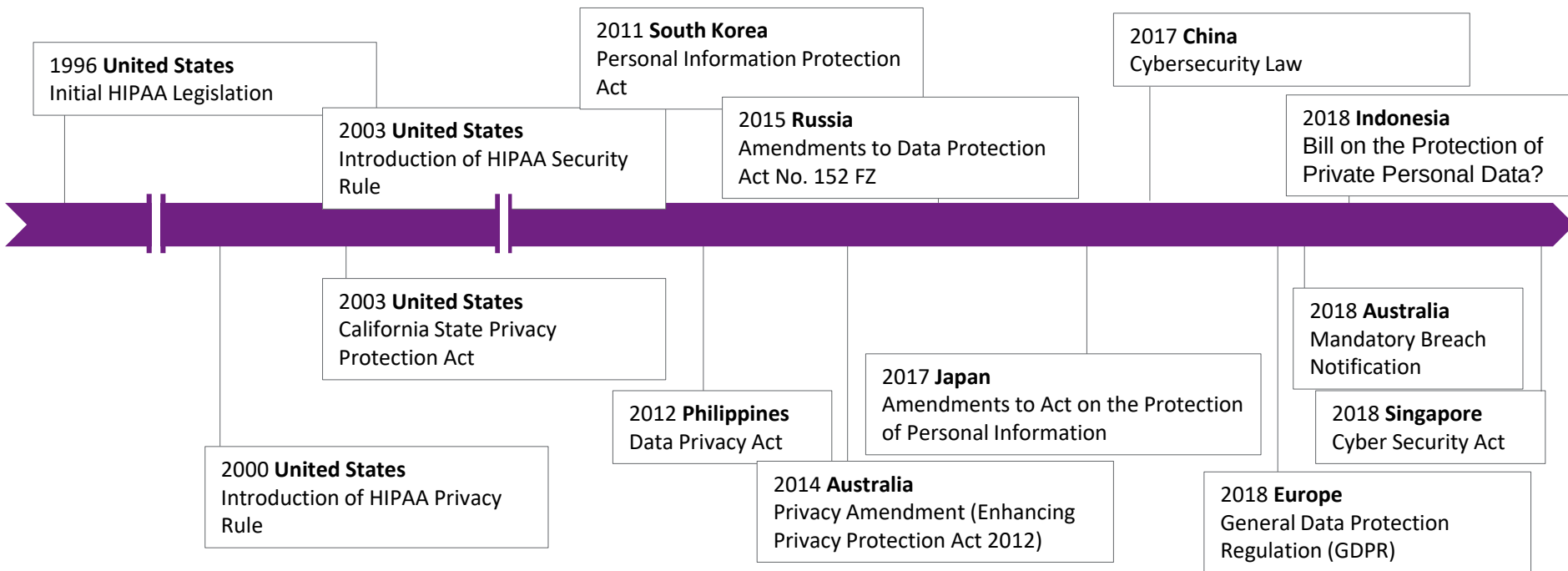


Cloud
Provider

Percentage of claims by breach type



Increasing Data Protection and Data Breach regulation globally



Insurance market statistics

\$3.0bn

(2017)

Estimated global Gross
Written Premium(GWP)
from cyber insurance

Over \$600m

Total aggregate
capacity available
for a single risk

80%

GWP from U.S.
domiciled entities

**Key
industry
sectors**

- FI
- Retail
- Transportation
- Health Care
- Manufacturing

60+

Insurance companies
with a cyber
product offering

Key cyber
insurance markets in Asia

Allianz

Chubb

AIG

Zurich

XL Catlin

Decode resiliency

How boards can lead the
cyber-resilient organisation

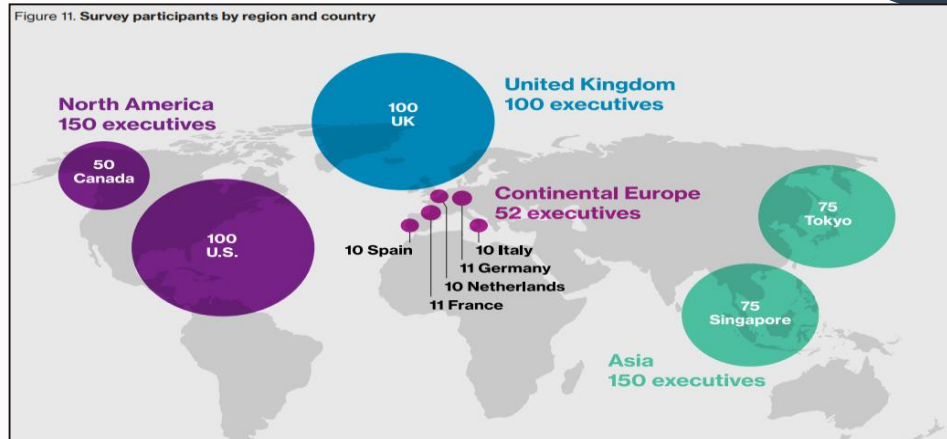
The
Economist

INTELLIGENCE
UNIT

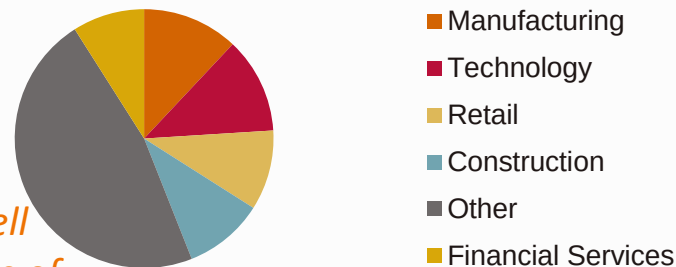
Background & Survey Scope

To learn more about **cyber risk management challenges** organisations are facing and provide insight into improvements that executives can make to create a more cyber-resilient organization, The Economist Intelligence Unit (EIU) conducted a global survey of **452 large company board members, c-suite executives and directors**. The survey was sponsored by Willis Towers Watson.

Only 13% — the smallest proportion of any of the competencies measured — give themselves a rating of well above average compared with peers in applying the lessons of security incidents.



Respondents by Industry



Is our organisation investing enough into Cyber Security and Cyber Resilience?

Only 15% say that their companies are spending the right amount, with the average spend being about 1.7% of total revenue.

Figure 9. How should our spending on cyber-resilience change?

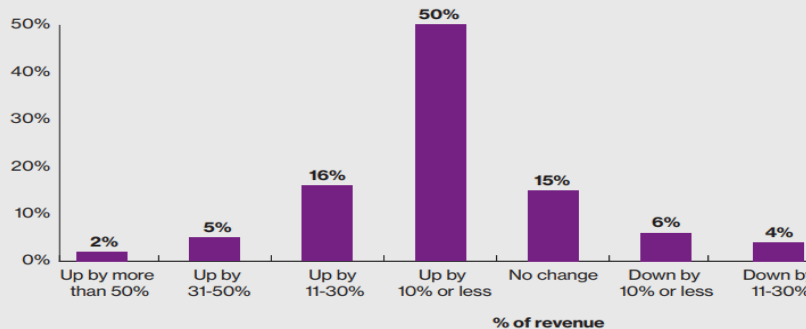
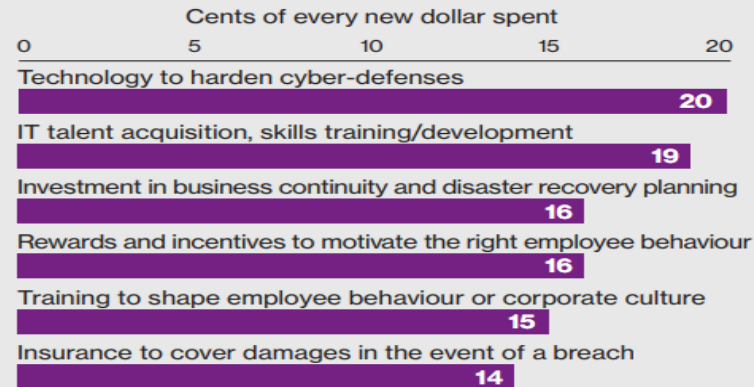


Figure 10. How should new spending on cyber-resilience be allocated?



Ensuring *Compliance* but also *Responsiveness & Resilience*

How can insurance assist with incident response?

- **People** (an incident response team or individual, technical experts, fast access to decision-makers, representation from key suppliers)
- **Process** (such as knowing what to do, how to do it and when to do it – detecting, containing, eradicating or recovering from a cyber security incident)
- **Technology** (knowing their network topology, providing the right event logs)
- **Information** (having information close to hand about business operations and priorities; critical assets; and key dependencies, such as on third parties, important locations or where relevant information resides).

Building a cyber savvy and resilient organization



- ☐ How holistic and comprehensive is your cyber risk management strategy? How do your protocols compare to those of your peers and industry best practices?
- ☐ Have you identified your “crown jewel” assets and quantified the financial impact of a cyber exposure?
- ☐ Have you assessed the role that company culture and employee behavior play in enabling or preventing cyber incidents, beyond just changing passwords?
- ☐ Have you done the appropriate due diligence of your third party vendors?

- ☐ Do you know the breadth of coverage available from cyber insurance to help pay losses and expenses associated with a breach, including first-party, third party and business interruption losses?
- ☐ Is your CISO the right fit for the job and have you recently evaluated your IT talent and emerging skills?
- ☐ Are key functions (e.g., CISO, CHRO, RM, CFO) aligned and collaborating on your cybersecurity risk management strategy?

- ☐ Do you have an incident response plan in place and has it been tested?
- ☐ What are steps you should take when notifying your insurer of a cyber incident to maximize recovery?”
- ☐ Have you reviewed your business continuity plan in the context of cyber risk, including as relates to your employees?

Real Life Claims



- [Singapore: large APAC FMCG company] Payroll system was hacked and their employees' bank account details changed. Employee salaries transferred to incorrect accounts, approx. USD 55,000 in total. Costs also incurred to determine the cause and scope of the breach through forensics.
- [New Zealand/Australia: global financial services firm] Senior partner's email was hacked as a result of him clicking on a link in a phishing email. A virus was then sent to all of the partner's contacts. USD38,000 in costs to determine the cause and scope of the breach (ensuring that no sensitive data had been accessed), and reserve for legal costs.
- WannaCry: Mostly affected SME's in APAC. Generally claims averaged at USD 20,000 for data reconstitution, IT and forensics.



Jessica Wright is Willis Towers Watson's
Regional Associate Director for Cyber,
based in Singapore.

