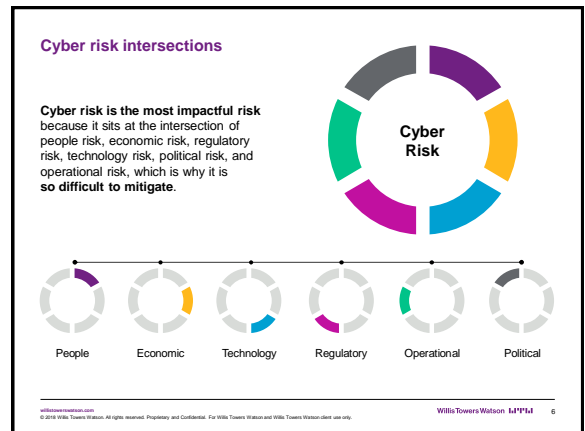
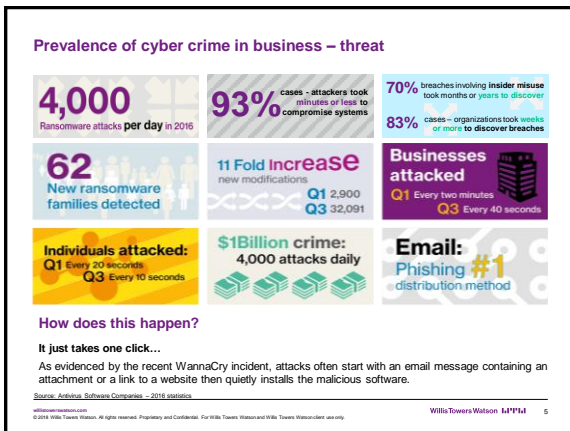
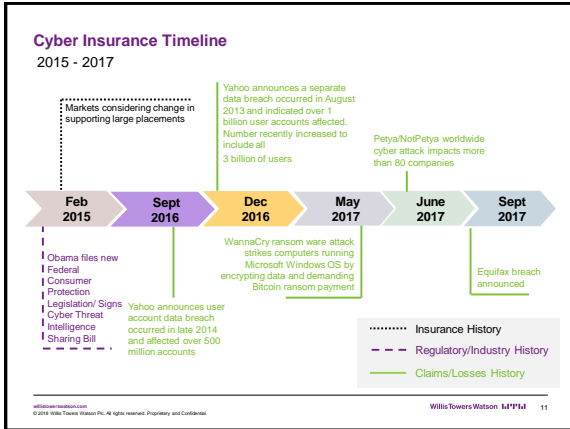
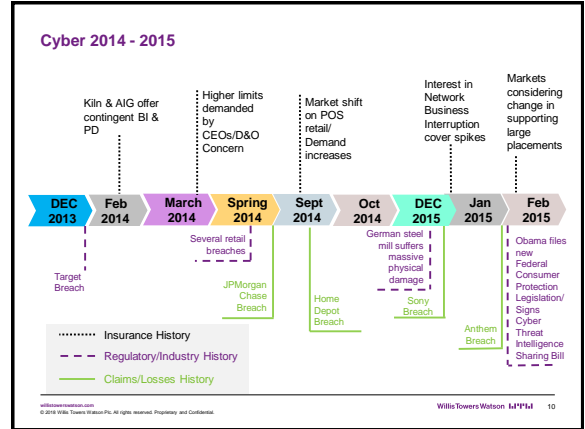
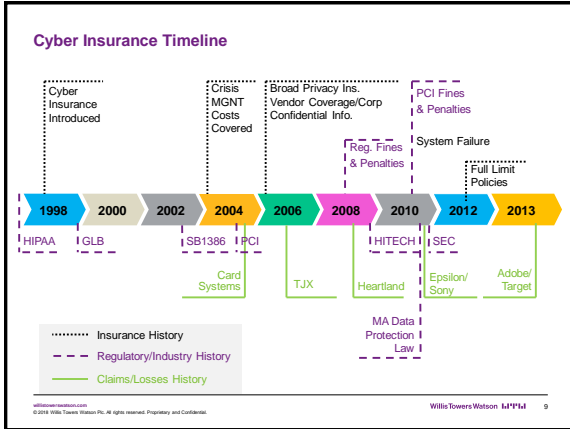


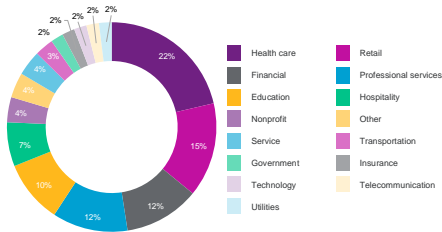
CYBER ATTACKS AND DATA BREACHES



CYBER ATTACKS AND DATA BREACHES

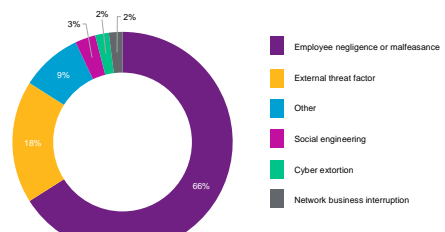
Sector impact

Hacking Incidents By Industry

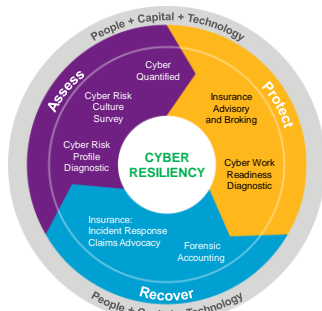


Employee factors have become the top source of breaches

Percentage of claims by breach type



Willis Towers Watson Cyber Risk Offerings



How cyber savvy and resilient is your 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 CSO the right fit for the job and have you recently evaluated your IT talent and emerging skills?
- 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?

Cyber risk

Why this matters to you now

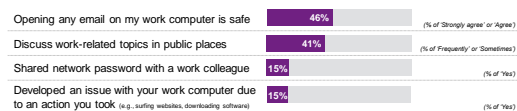
- Traditional focus on risk transfer and technology solutions has excluded the human element from cyber risk management strategy considerations
- Employees are the main cause of incidents, whether because of accidental errors, malicious insiders, or talent shortage/skills deficit
- Organizations like yours are planning to increase investments in human capital solutions in the next three years
- A growing disconnect between employers' view of cybersecurity readiness and employees' behavior and engagement creates new vulnerability
- Digitization is creating skills deficits and talent shortages in IT departments and among non-technical employees generally
- The C-Suite and Boards are increasingly accountable for cyber risk and are looking to CISOs, CHROs, and CROs to lead solutions

Managing Cyber Risks

Employer View



Employee Behavior



CYBER ATTACKS AND DATA BREACHES

Culture and risk of cyber breach: the connections

Learnings from organizations experiencing cyber incidents

To understand how culture matters to cyber risk, we searched for organizations experienced a data breach AND for which we conducted an employee survey at or about the same period. We identified 12 such organizations with data for study.

Using their survey scores, we compared the 12 organizations to two survey benchmarks:

- The Willis Towers Watson Global High Performance Norm – a benchmark of companies with above-sector average financial results over three years (involves all employees in the comparison)
- The Willis Towers Watson Global IT Functions norm – a benchmark from IT workers in 448 companies (involves ONLY the IT staff, a critical function in cyber defense, in the comparison)

Environments experiencing cyber breaches scored **lower** in three areas:

- 1 A laser-sharp focus on customers and responsiveness to their needs
- 2 A positive company image fostered among employees, reflecting strong corporate commitment to social responsibility
- 3 Comprehensive training, especially among IT staffers, that helps employees understand jobs thoroughly

These results drove the design of a broad employee engagement survey focused on cyber risk culture...

willistowerswatson.com
© 2018 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only. Willis Towers Watson | **WTTW** | 13

Insurance market statistics

\$3.0b (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

Key cyber insurance markets

AIG
XL Catlin
Beazley
Chubb
Lloyd's

60+ Insurance companies with a cyber product offering

willistowerswatson.com
© 2018 Willis Towers Watson. All rights reserved. Proprietary and Confidential. For Willis Towers Watson and Willis Towers Watson client use only. Willis Towers Watson | **WTTW** | 14