Decode cyber risk.

Cyber Risk Culture Survey

Diagnosing company culture to mitigate risk

With the majority of cyber breaches resulting from some type of human error or behavior (whether negligent or malicious acts), many organizations have an interest in identifying root causes of these employee behaviors and aspects of workplace culture that may be contributing to information security risk. With combined expertise in human capital and cyber risk solutions, Willis Towers Watson provides insight into the people risk and is well-positioned to help clients address the vulnerabilities created by their workforce.

Sources of risk can include employees' lack of awareness and personal responsibility for cyber risk, poor understanding of steps the organization is taking to address cybersecurity, and a low "cyber IQ" resulting in behaviors that increase risk to internal systems and processes. Vulnerabilities can be present generally or in pockets within the organization.

How employee behavior drives cyber risk

- Employee negligence or malicious acts are responsible for fifty-eight percent of cyber breaches.[1]
- Companies experiencing cyber breaches lack certain critical aspects of employee experience, including:
  - purpose tied to customer centricity (e.g. responsiveness and optimizing processes)
  - work marked by speed and flexibility in making decisions and managing teams
  - people practices that empower staff through voice, respect, support for teamwork
  - stress training and development that align with pay and performance[2]
- Companies' perceptions of their cyber risk readiness and governance are not matched by actual employee actions. For example, nearly half of employees think it's safe to open any email on a work computer.[3]

Only by investigating vulnerabilities, raising awareness and moving employees from compliance to conversion, can organizations begin to understand the risk. Take appropriate preventative measures and move toward sustainable engagement.

[1] Willis Towers Watson 2017 Reported Claims Index
[2] Proprietary Willis Towers Watson analysis of employee survey data against Global High Performance Norm and Global IT Functions Norm benchmarks
[3] 2017 Willis Towers Watson employer and employee cyber risk surveys

Willis Towers Watson

Willis Towers Watson Cyber Risk Culture Survey

Using our vast experience in employee research and cyber risk management, Willis Towers Watson's Cyber Risk Culture Survey collects insights directly from employees regarding frequency of cyber-savvy behaviors and perceptions of cyber risk challenges in the workplace.

The result is a profile of the current state of cybersecurity awareness and employee actions across the organization that points the way to building a cyber smart workforce. Results provide a clear picture of an organization's internal risk culture and allow senior leadership to take decisive action to create solutions.

Deployment options:

1. Vulnerability index (include with existing employee engagement survey)
2. Pulse survey (self-administered and can be deployed to specific groups)
3. Full survey (over 100 customizable questions)

Reports can be created for senior leadership

Arming leadership with key insights

- **Provide data breach benchmarks that help prioritize culture challenges**

Global database of **1.3 million** respondents from companies that have experienced a **cyber incident.**

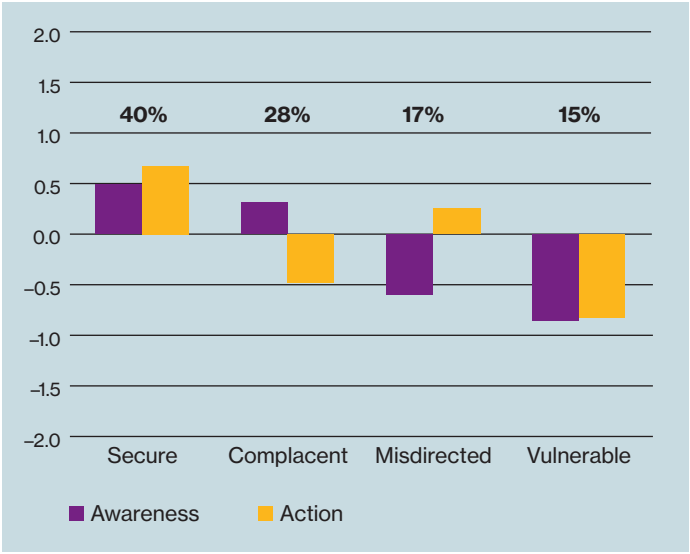
- **Obtain ideas for improvement directly from employees**

Two custom comment questions:

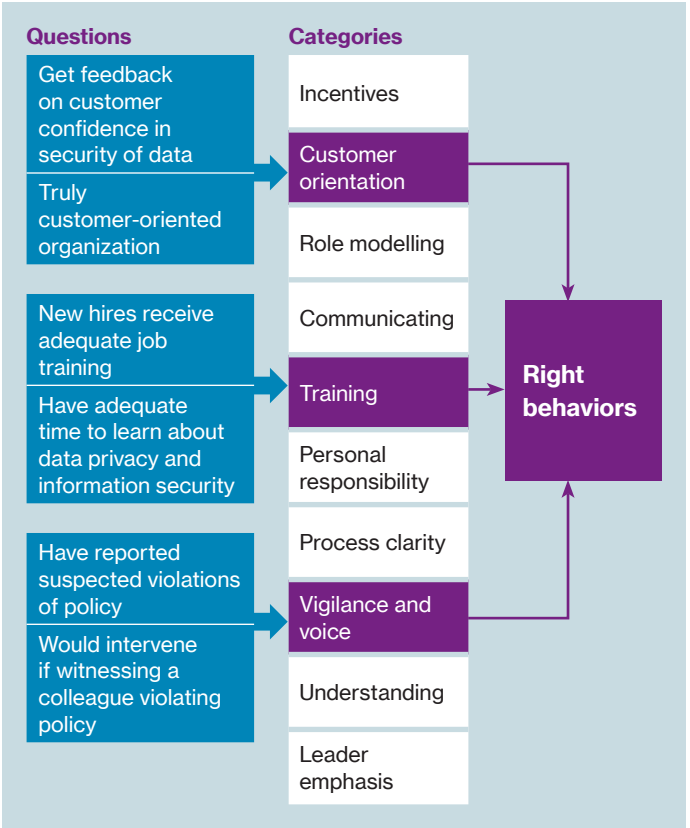
1 What are we doing now that is working well to manage data privacy and information security risks?

2 What actions should we take in the next 12 months to reduce data privacy and information security risks?

- **Segment your workforce to locate the most vulnerable populations**

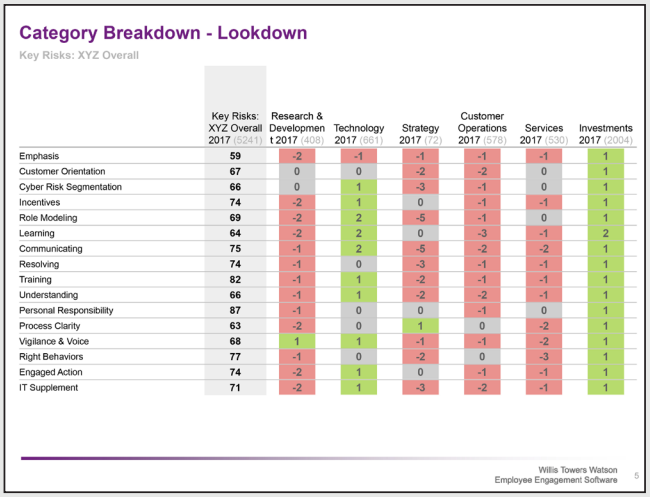


- **Identify what experiences drive optimal behavior**



The reports provide rich cyber risk culture insights that enable you to:

- Identify employees with the greatest likelihood of causing a cyber incident and predict frequency of high-risk cyber behavior.
- Categorize those employees by function, geography, title and/or role – enabling the efficient targeting of an appropriate mitigation plan.
- Prioritize for action to promote a "cyber-savvy" workforce, not one driven solely by compliance.
- Extend to vendors to determine "people risk" of supply chain and other business partners.

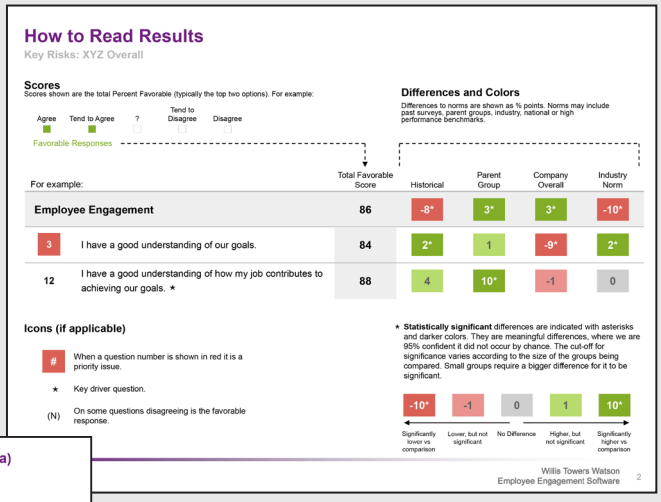


Category Breakdown - Lookdown

Key Risks: XYZ Overall

	Key Risks: XYZ Overall 2017 (6241)	Research & Development 2017 (408)	Technology 2017 (861)	Strategy 2017 (72)	Customer Operations 2017 (578)	Services 2017 (530)	Investments 2017 (2004)
Emphasis	59	-2	-1	-1	-1	-1	1
Customer Orientation	67	0	0	-2	-2	0	1
Cyber Risk Segmentation	66	0	1	-3	-1	0	1
Incentives	74	-2	1	0	-1	-1	1
Role Modeling	69	-2	2	-5	-1	0	1
Learning	64	-2	2	0	-3	-1	2
Communicating	75	-1	2	-5	-2	-2	1
Resolving	74	-1	0	-3	-1	-1	1
Training	82	-1	1	-2	-1	-1	1
Understanding	66	-1	1	-2	-2	-1	1
Personal Responsibility	87	-1	0	0	-1	0	1
Process Clarity	63	-2	0	1	0	-2	1
Vigilance & Voice	68	1	1	-1	-1	-2	1
Right Behaviors	77	-1	0	-2	0	-3	1
Engaged Action	74	-2	1	0	-1	-1	1
IT Supplement	71	-2	1	-3	-2	-1	1

Willis Towers Watson
Employee Engagement Software 5



How to Read Results

Key Risks: XYZ Overall

Scores
Scores shown are the total Percent Favorable (typically the top two options). For example:

Agree | Tend to Agree | ? | Tend to Disagree | Disagree

Favorable Responses

Differences and Colors
Differences to norms are shown as % points. Norms may include past surveys, parent groups, industry, national or high performance benchmarks.

For example:	Total Favorable Score	Historical	Parent Group	Company Overall	Industry Norm
Employee Engagement	86	-8*	3*	3*	-10*
3 I have a good understanding of our goals.	84	2*	1	-9*	2*
12 I have a good understanding of how my job contributes to achieving our goals. ★	88	4	10*	-1	0

Icons (if applicable)

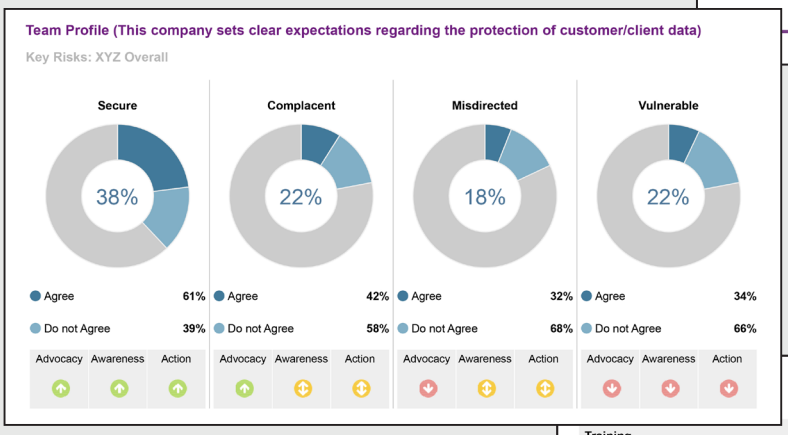
- # When a question number is shown in red it is a priority issue.
- ★ Key driver question.
- (N) On some questions disagreeing is the favorable response.

* **Statistically significant** differences are indicated with asterisks and darker colors. They are meaningful differences, where we are 95% confident it did not occur by chance. The cut-off for significance varies according to the size of the groups being compared. Small groups require a bigger difference for it to be significant.

-10* | -1 | 0 | 1 | 10*

Significantly lower vs comparison | Lower, but not significant | No Difference | Higher, but not significant | Significantly higher vs comparison

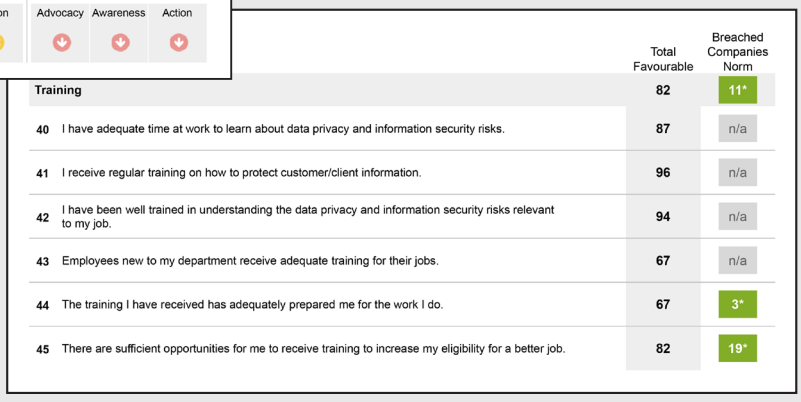
Willis Towers Watson
Employee Engagement Software 2



Team Profile (This company sets clear expectations regarding the protection of customer/client data)

Key Risks: XYZ Overall

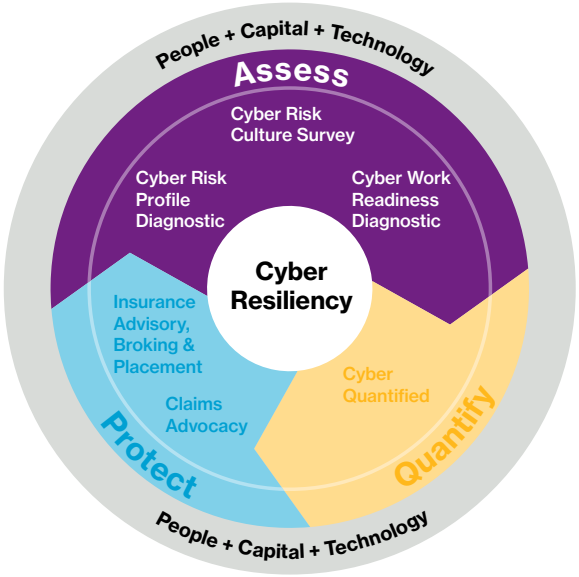
Secure	Complacent	Misdirected	Vulnerable
38%	22%	18%	22%
Agree 61%	Agree 42%	Agree 32%	Agree 34%
Do not Agree 39%	Do not Agree 58%	Do not Agree 68%	Do not Agree 66%
Advocacy ↑ Awareness ↑ Action ↑	Advocacy ↑ Awareness ↔ Action ↔	Advocacy ↓ Awareness ↔ Action ↔	Advocacy ↓ Awareness ↓ Action ↓



		Total Favourable	Breached Companies Norm
Training		82	11*
40	I have adequate time at work to learn about data privacy and information security risks.	87	n/a
41	I receive regular training on how to protect customer/client information.	96	n/a
42	I have been well trained in understanding the data privacy and information security risks relevant to my job.	94	n/a
43	Employees new to my department receive adequate training for their jobs.	67	n/a
44	The training I have received has adequately prepared me for the work I do.	67	3*
45	There are sufficient opportunities for me to receive training to increase my eligibility for a better job.	82	19*

Why Willis Towers Watson?

More than half of all cyber incidents begin with employees, so it's a people problem. And the average breach costs $4 million, so it's a capital problem, too. No one decodes this complexity better than Willis Towers Watson. As a global leader in human capital solutions, risk advisory and broking, we are well prepared to assess your cyber vulnerabilities, protect you through best-in-class solutions and radically improve your ability to successfully recover from future attacks. Explore comprehensive cybersecurity solutions at willistowerswatson.com/cyber.



About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

For more information

Patrick Kulesa
+1 212 309 3746
patrick.kulesa@willistowerswatson.com

Kelly Harkcom
+1 312 288 7131
kelly.harkcom@willistowerswatson.com

willistowerswatson.com/social-media

WTW-GL-18-SAL-4445

willistowerswatson.com

Willis Towers Watson