Willis Towers Watson

Decoding cyber risk: Driving a cyber-savvy workforce

Willis Towers Watson 2017 Cyber Risk Survey

People are the next frontier in cyber risk management, according to Willis Towers Watson's U.S. and UK employer and employee Cyber Risk surveys.

Introduction

One in five U.S. and UK organizations that participated in the Willis Towers Watson 2017 Cyber Risk Surveys reported that their organizations have suffered a cyber breach in the last year with 6% of those incidents having been significant, consistent with publicized recent large cyber breaches.

Two thirds of U.S. companies, and just under half of UK businesses, see cybersecurity as a fundamental challenge to their organization as reflected in the priority given to cybersecurity – 85% of U.S. employers, and 72% in the UK, regard it as a top priority.

To date, technological responses have led the way. However, growing recognition of the human element in cyber risk means that most companies that responded to the survey expect to focus more heavily on operating procedures and creating a more cyber-savvy workforce in the months and years to come.

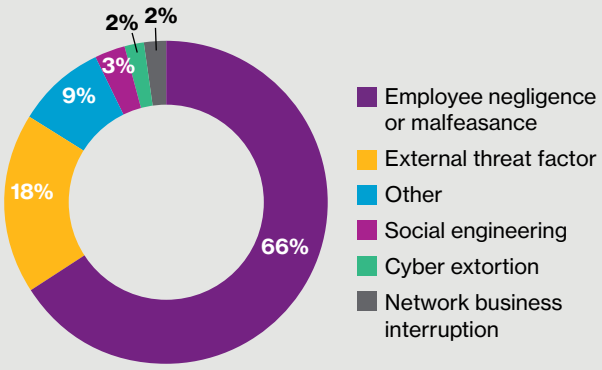
And with good reason it would seem. Willis Towers Watson's recent Cyber Claims Database shows that by far the largest proportion of cyber claims reported to insurers stems from employees' actions, or collective inaction *(Figure 1).*

The concurrent employee view of the survey appears to offer some explanation for the claim statistics, by showing a disconnect between cyber awareness and accountability of the workforce and organization's views of their preparedness.

Moving towards a culture of cybersecurity

While most companies feel they are on the right track in terms of data privacy and information security, many say they are looking to create a culture of cybersecurity in their organization. Most admit, however, to being currently on the lower rungs of the ladder to reach this goal, although they have aspirations to climb it quickly. Over half have no formally articulated cyber strategy now, but over 80% want to have cyber risk management embedded in their company culture within the next three years.

Figure 1. **Percentage of U.S. cyber insurance claims by breach type**



Source: Willis Towers Watson claim data

So, how will they get there?

The unequivocal answer on both sides of the Atlantic is by making more progress on improving business and operating processes and on addressing factors tied to human error or actions *(Figure 2).*

Business-related activities expected to figure prominently in companies' plans include more stringent reviews of contractors and third-party suppliers and testing of emergency response plans. To offset risk, a large majority of companies are also reviewing or adding to their cyberinsurance coverage. The available insurance market has expanded, with the higher levels of activity seen in the U.S. so far reflecting the fact that American companies have historically bought more of this type of cover, compared to European companies that have tended to focus more on business interruption and continuity. Fifty four percent of U.S. companies have added to or enhanced cyber coverage in the last two years, compared to 26% of UK companies. Notably, however, an additional 45% of the UK businesses surveyed said they expect to review cyber insurance cover in the next two years (before taking into account the recent WannaCry ransomware incident that has accelerated inquiries from UK businesses about cyberinsurance).

Two thirds of companies on both sides of the Atlantic have also already taken steps to centralize data privacy and information security. This may account for most companies believing they have or need appropriate levels of corporate support and clear lines of responsibility for data privacy and information security – leaving more to do on supporting processes and employee engagement.

Two thirds of companies on both sides of the Atlantic have also already taken steps to centralize data privacy and information security.

Among the specific people-related actions that companies expect to take in the next couple of years, training programs for both employees and contract workers frequently top the agenda. This is particularly the case in the UK, where the survey figures indicate there is some catching up to do relative to the U.S. on the people-related risks. For example, UK employers believe that over 60% of their employees don't understand cyber risks to a great or moderate extent. This compares with 34% of U.S. employers who feel the same. These figures allude to the fact that organizations, even across the Atlantic, are at different stages of their cyber resiliency journeys. The difference in results also highlights the need for HR and risk management functions to work more closely together on cyber risk mitigation strategies, something that only a third of companies reported they are currently doing.

Among the specific people-related actions that companies expect to take in the next couple of years, training programs for both employees and contract workers frequently top the agenda.

Does employee behavior match company policy?

As companies adapt their cybersecurity approaches to more actively address people risks, they will of course need employees to step up to the plate and play their part.

Combining the results of our employee and employer surveys shows they have some work to do here, including doing more in some cases to create and maintain an environment in which employees are comfortable reporting data privacy and security incidents.

Figure 2. **Progress made in respective areas to mitigate the vulnerability of a cyber-attack over the last/next three years.**

U.S.

	Over the **last** three years	Over the **next** three years	Changes
Improve the technology systems and infrastructure	76%	68%	▼–8
Improve business and operating processes	58%	72%	▲+14
Address factors tied to human error or actions	52%	74%	▲+22

Note: Percentages indicate 'To a great extent' or 'To a very great extent'.
Source: 2017 WTW Cyber Risk Survey, employer survey, US.

UK

	Over the **last** three years	Over the **next** three years	Changes
Improve the technology systems and infrastructure	75%	66%	▼–9
Improve business and operating processes	46%	69%	▲+23
Address factors tied to human error or actions	40%	75%	▲+35

Note: Percentages indicate 'To a great extent' or 'To a very great extent'.
Source: 2017 WTW Cyber Risk Survey, employer survey, UK

One dangerous but apparently common belief among employees is that the company's IT and security systems are the ultimate protector. Even though a significant majority of companies feel they are doing what they need to in setting up and communicating robust protection systems, policies and processes, the message does not always resonate, judging by some current employee behaviors. Around 40% use a work computer or cellular device to access confidential company information and discuss work-related topics in public places. About 30% admit to logging in to a work device on an unsecured public network or using a work computer in public settings. Roughly 25% take confidential paper files home and use unapproved devices to do work at home. Some employee attitudes toward opening email attachments, changing passwords regularly and sharing personal information, such as employer name and job title, on social media sites may also leave companies more vulnerable, particularly to social engineering, where cyber criminals use impersonation techniques to trick employees into divulging confidential information or data.

One dangerous but apparently common belief among employees is that the company's IT and security systems are the ultimate protector.

Given these findings, there certainly seems to be a need to more closely assess the reasons why employees continue to engage in risk producing behaviors.

A root cause may be that nearly half of both the U.S. and UK employees surveyed said they spent less than 30 minutes on data protection and information security training last year. Around 60% said they had only completed any training because it was a company requirement, although many claimed to have derived some knowledge and benefit from whatever they had done.

Segmenting employees

Such results inevitably lead to employees with different levels of understanding, accountability or engagement with cyber risk management. It may benefit companies, therefore, to segment their awareness training and other learning tools in order to refine an approach for different groups of employees/workers. For example, executive-level employees may need more training on confidential corporate information and use of company devices while traveling in foreign countries, while HR training may focus primarily on protection of employee data.

Figure 3. **Time spent on cyber training in the last year**

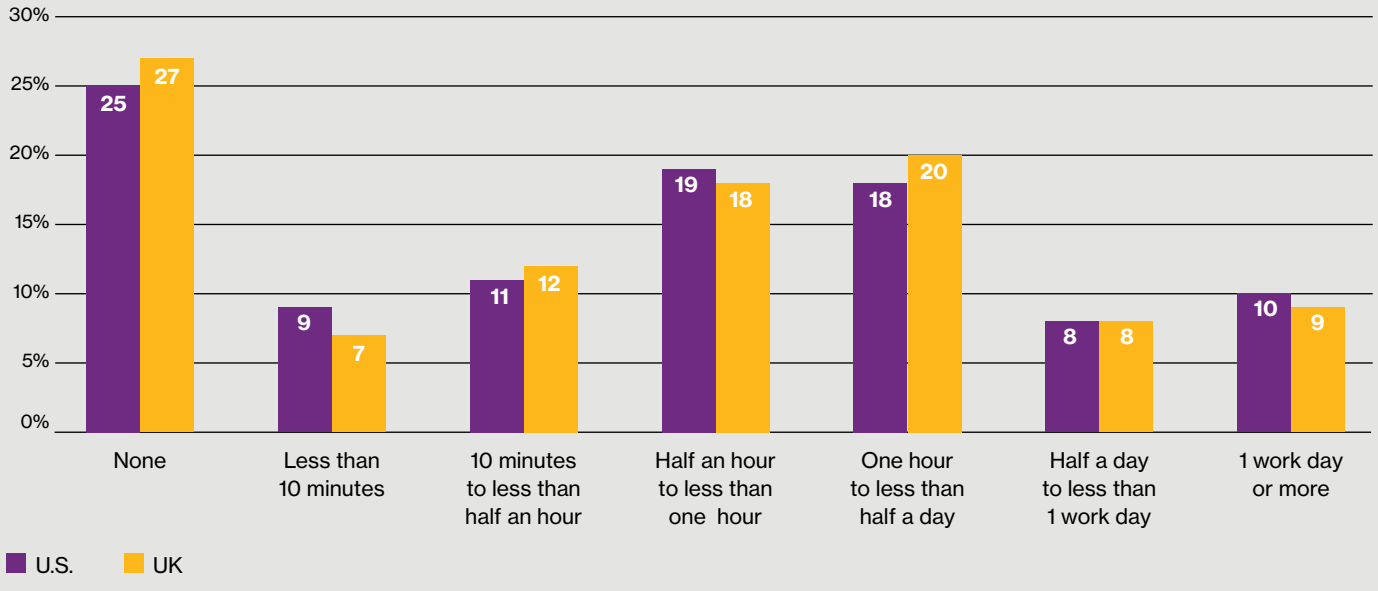
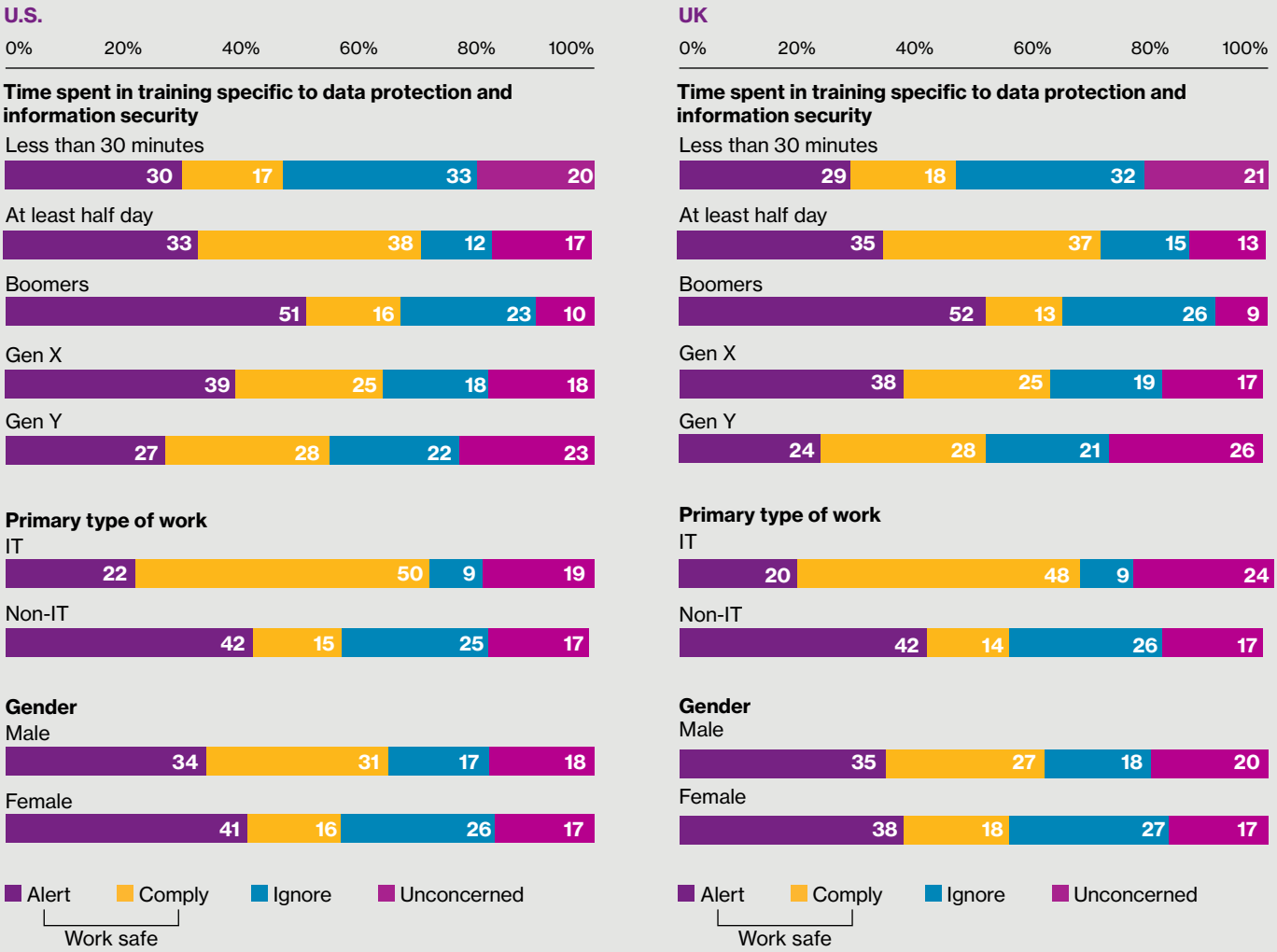


Figure 4. **Behaviour is strongly linked to training time, type of work and age**



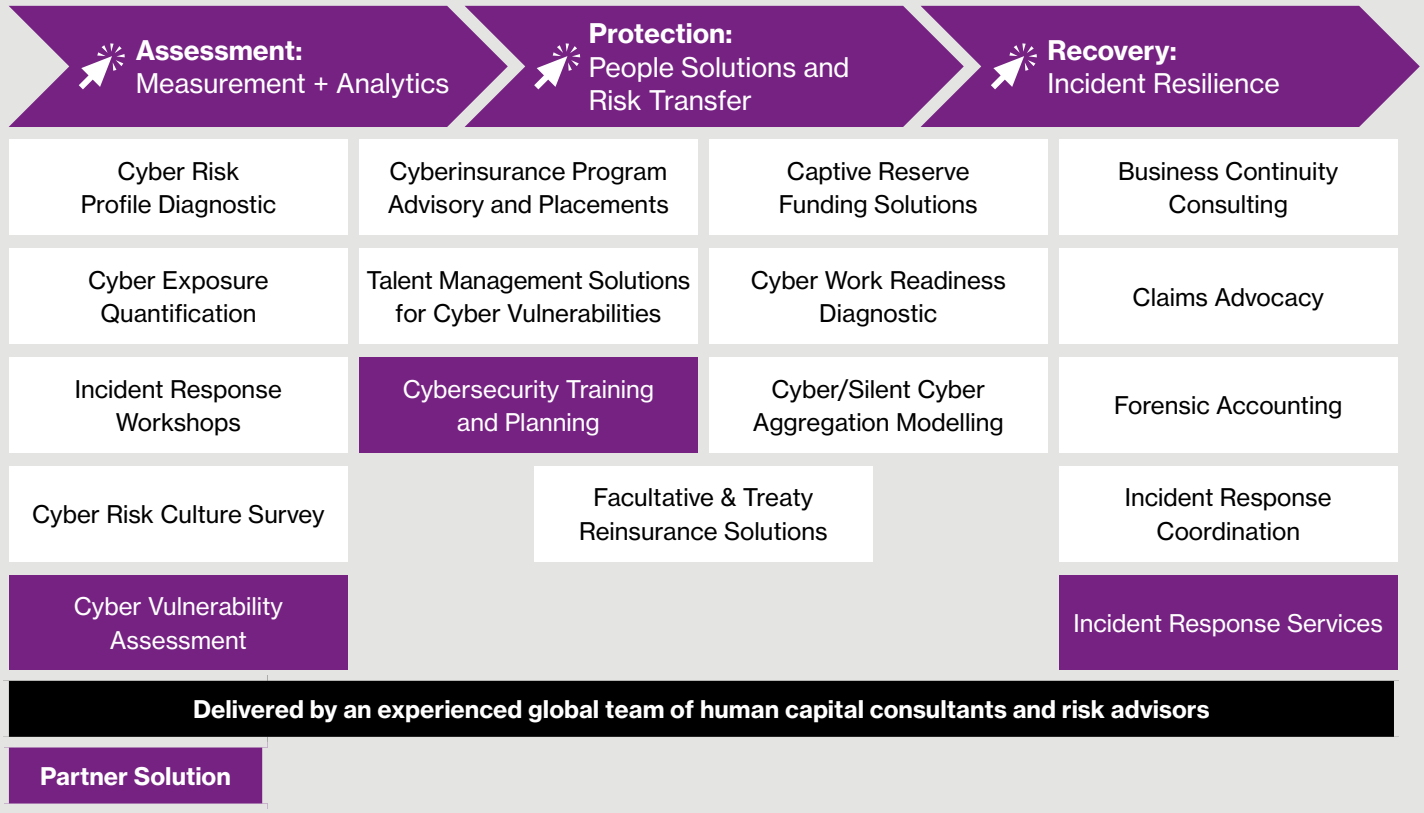
From the responses to a range of questions on the employee survey, we have defined four types of employees according to how they use technology at work or at home.

- **Alert** – those who protect personal information in daily life and are aware of information security at work.
- **Comply** – those who follow data/information protection policies at work but are careless on a personal level.
- **Ignore** – those who pay attention to protecting personal information, but who don't act with the same care at work.
- **Unconcerned** – those whose technology usage patterns at home and work may lead to potential cyber risks.

The percentage of survey respondents falling into each category in the U.S. and UK was remarkably similar, with just over a third in each country meeting the 'Alert' criteria. Furthermore, the behavior of each group was found to be strongly linked to training time, type of work and age *(Figure 4)*. For example, IT and non-IT staff have very different knowledge and behaviors, and hence different training needs. Similarly, younger employees in general report more risky behaviors and a more cavalier approach to technology and compliance, suggesting that companies may need a different approach to engaging and educating Generation Y groups in cyber risk mitigation.

Our cyber risk offerings

Integrated across people, capital and technology



Conclusion: beyond technology

The findings from our surveys signal a shift in cybersecurity strategies. Although companies still think there is more work to do on technological responses, most feel they are broadly on track and making progress in addressing potential weaknesses in their IT infrastructure.

Attention is now increasingly turning to the operational- and people-related risks that cyber claims experience shows leave companies exposed to cyber risk even with state-of-the-art technology strategies.

There is growing impetus behind the view that building effective cyber resilience has to have its roots within the organization culture and its people. Solutions are likely to be complex and multidimensional, as is always the case for any kind of cultural change. Certainly, companies may have to adapt their operations to the constantly changing nature of cyber threats. Nor should they ignore the expanding risk mitigation options available through the insurance market. But employers will increasingly look to foster a more cyber-savvy workforce, including the use of innovative employee engagement, talent management and reward strategies, to fortify their cybersecurity posture.

Further information

For more information about survey results, or to discuss the findings and our observations, contact:

Adeola Adele
Tel: +1 212 915 8889
adeola.adele@willistowerswatson.com

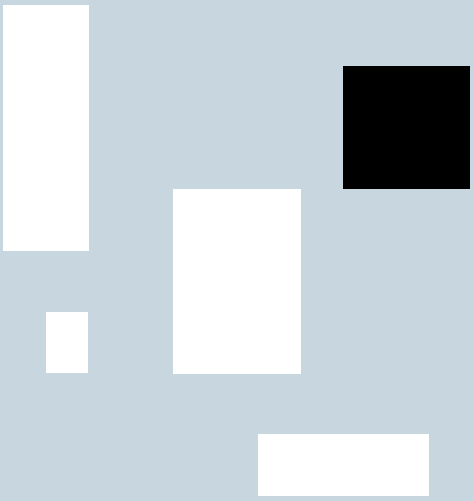
Anthony Dagostino
Tel: +1 212 915 8785
anthony.dagostino@willistowerswatson.com

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

Tracey Malcolm
Tel: +1 416 960 4490
tracey.malcolm@willistowerswatson.com

About the surveys

Willis Towers Watson carried out web-based surveys with a combined 163 U.S. and UK employers, and with over 2,000 employees in each country, a quarter of whom work in a corporate IT function.



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 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.

willistowerswatson.com/social-media

WTW-GL-17-SAL-7656

willistowerswatson.com

Willis Towers Watson