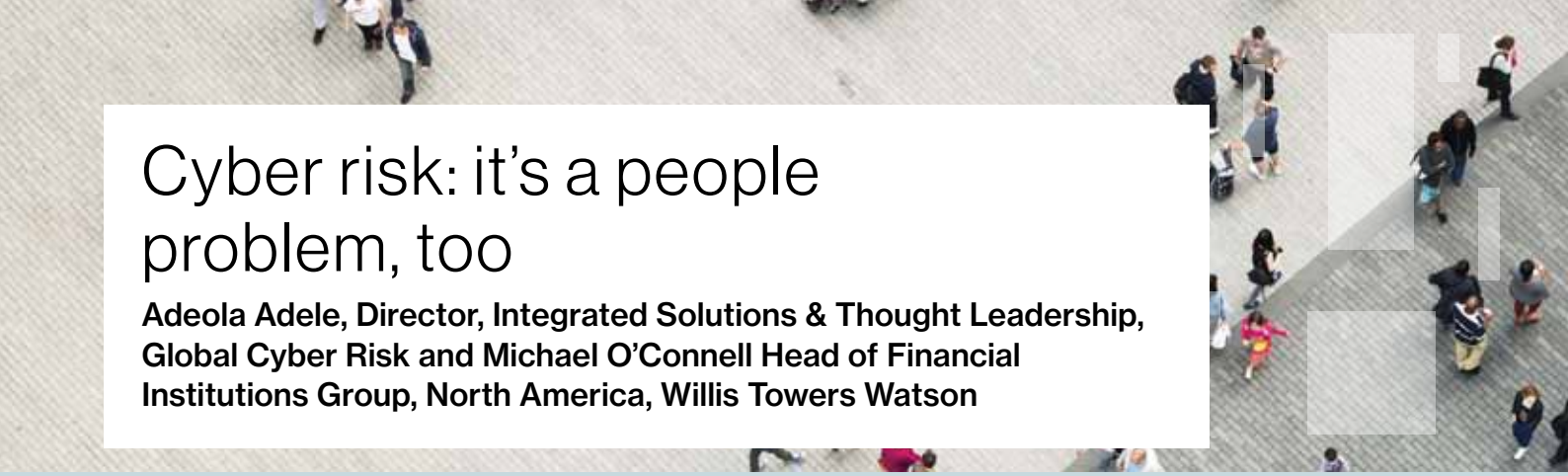
Willis Towers Watson

The future of financial services:

how work is impacted by the connection and convergence of people and technology



Cyber risk: it's a people problem, too

Adeola Adele, Director, Integrated Solutions & Thought Leadership, Global Cyber Risk and Michael O'Connell Head of Financial Institutions Group, North America, Willis Towers Watson

The trillion-dollar problem

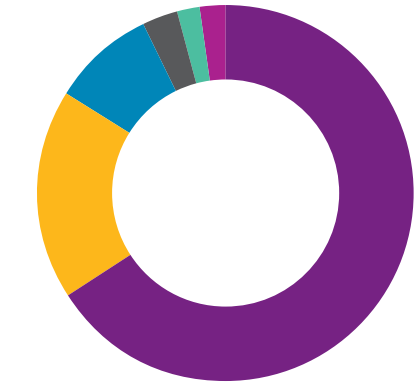
It is estimated that the global cost of cybercrime will reach US$6 trillion annually by 2021[1]. Financial institutions incur a higher annual cost of cybercrime than any other industry: US$16.5 million on average[2]. Cyber attacks against online financial services and lending companies increased 122% in 2016, causing £8 billion in loss value worldwide[3]. The industry also tops the charts for incidents of cyber extortion[4]. Around one in every five financial institutions uses an email service provider with severe security vulnerabilities[5].

Add to this the new EU General Data Protection Regulation (GDPR) that will come into force in 2018 and could see financial institutions penalised up to 4% of their annual turnover for failing to protect personal data and the picture is rather bleak.

The industry is of course responding to this threat. In the US alone, the financial institutions cyber security market will be worth US$68 billion by 2020[6]. Although companies are aware there is more work to do on technological responses to cyber threats, our research shows most feel they are broadly on track and making progress in addressing potential weaknesses in their IT infrastructure.

What is less certain, however, is how financial institutions are addressing similar weaknesses in their cyber *culture*, or putting it another way, the *people* aspect of cyber threats. According to our research, employee negligence or malicious acts account for two-thirds of cyber breaches (*figure 1*); in contrast only 18% are directly driven by an external threat[7].

Causes of cyber breaches



Source: Willis Towers Watson claim data

Cyber risk therefore, is much more than a pure technology issue. For example, the recent high profile WannaCry attack served as a stark reminder that employees are both the weakest link in an organisation's cybersecurity strategy and the strongest defence. The attack affected more than 230,000 computers and compromised the systems of some banks. Ultimately, it was enabled by employees clicking infected phishing emails.

[1] Cybersecurity Ventures, 2016 Cybercrime Report
[2] Ponemon, 'Cost of Cyber Crime Study & the Risk of Business Innovation', 2016
[3] ThreatMetrix, 'Organised Fraud Rings Turn Their Attention to Online Lenders and Emerging Financial Services', February 2017
[4] Consultancy UK, 'Costs of cybercrime have soared to $280 billion this year', December 2016
[5] Security Scorecard, 2016 Financial Industry Cybersecurity Report
[6] Homeland Security Research, US Financial Services: Cybersecurity Systems & Services Market – 2016-2020
[7] Willis Towers Watson, 'When it comes to cyber risk, businesses are missing the human touch', March 2017

The new frontier: a cyber-savvy workforce

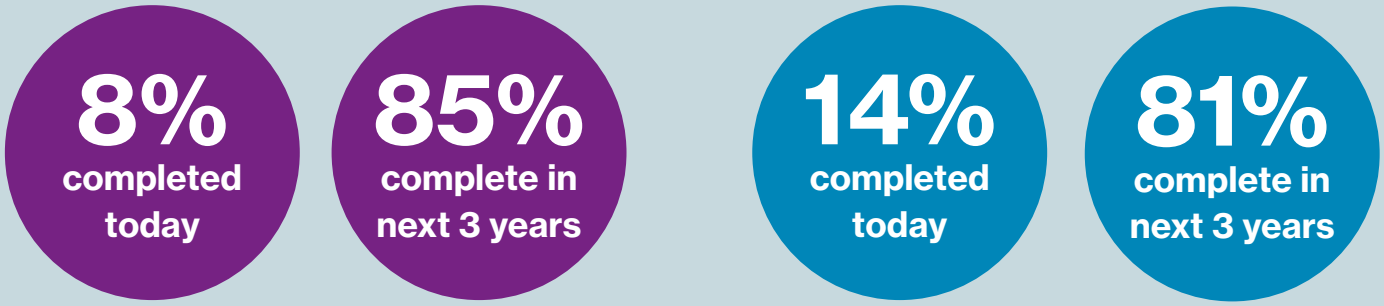
In June 2017 we surveyed a combined 163 US and UK employers and over 4,000 employees on their present and future cybersecurity strategies. This Cyber Risk Survey found that attention is now increasingly turning to the people-related risks that, claims experience shows, leave companies exposed to cyber risk even with state-of-the-art IT approaches.

The survey found that the top cyber risk across both regions is 'insufficient employee understanding of cyber risks'. However, in the UK only 14% of respondents have embedded cyber risk management within their company culture; in the US this falls to just 8%. Yet the tide is turning; in both regions over 80% say they will develop a cohesive culture of cybersecurity in the next three years[8].

Embedded cyber risk management within company culture?

93% of US companies versus **95% of UK companies**

Completed today or plan to complete in next three years



[8] Willis Towers Watson, 2017 Cyber Risk Survey Report, June 2017

Challenges to driving a strong cyber culture

Our survey found that most employees feel they know how to manage data privacy and information security in their jobs. However, there remain challenges that will need to be addressed in order for financial institutions to build the strong cyber behaviours among employees necessary to develop a cyber-savvy workforce and culture.

1 Budgets

Only 43% of US and 50% of UK organisations believe they have adequate budgets to meet all cyber risk management needs. Although many large financial institutions have significant cybersecurity budgets, they should ensure that appropriate capital is allocated to managing the people risks. Small and middle-market institutions tend to be less concerned about cyber risks than their larger counterparts and many do not have the same capital available for mitigation. However, these organisations need to be just as proactive as their larger counterparts: hackers are specifically targeting financial institutions with revenues below US$35 million for their valuable client data[9].

2 Lack of risk management-HR collaboration

Only a third of respondents believe that their company's risk management and HR functions work closely together on cyber risk management. This disconnect can result in ineffective structures and processes, which adds cost and leaves holes in cybersecurity.

3 Overreliance on IT

A large number of employees are overly reliant on company IT to provide cybersecurity and assume they will be protected at all costs.

Alarmingly, nearly half of all employees believe that opening any email on their work computer is safe. While email and online systems are vital

Influencing risk culture

In an increasingly complex corporate world, managing risks related to an organisation's human capital is critical. The management of these risks is often perceived as challenging because it's thought that people-related risks can't be quantified.

The right, balanced risk culture can help financial institutions identify and take advantage of the right opportunities, gaining competitive advantage and reducing the total cost of risk.

Focusing your efforts

To influence and improve risk culture, financial institutions must understand both a top-down and bottom-up perspective. This understanding highlights risky behaviours, which, if reduced, can lead to fewer incidents, accidents, fines and claims, lowering the total cost of risk.

An organisation can improve risk culture holistically and/or by focusing on specific businesses or functions via an operationally focused approach, for example, the trading arms within banks.

Measuring risk culture – the importance of quantification

Measuring risk culture is important for internal risk culture assessment and management. Much of an organisation's risk culture lies 'beneath the surface'. Important cultural characteristics may not be immediately apparent but they can be identified, measured and understood using two key assessments.

Setting the right risk culture

Taking an overly cautious approach to behavioural risk can lead an organisation to achieve below-potential growth, while an organisational culture that is high on the risk spectrum (without suitable frameworks in place) can lead to extreme losses. Additionally, pressure from shareholders to achieve quarterly performance results often forces long-term risk management to take a back seat to short-term targets.

[9] Beazley Insights, 'Hackers target smaller financial institutions' July 2016

for financial institutions to function, employees must be aware of the risks they also present. In addition, they must understand that they, not just IT, are a key component in their organisation's cyber defence.

4 Failure to report

Over a third of all employees have witnessed co-workers behaving in ways inconsistent with data privacy and information security policies. However of these, only 47% and 53% in the UK and US respectively reported the incident to a manager or IT department.

Financial institutions have had their cultures closely examined by the media, consumers and regulators in the last 10 years. The effects of a cyberattack can be devastating to both finances and reputation; so empowering employees to raise concerns and challenge poor behaviours is one way to mitigate this risk.

5 Employee unawareness of emerging threats

Only 40% of employees believe that a disgruntled employee or contractor could deliberately compromise company systems or steal customer data.

Two-thirds only change their password on their work computer when prompted and one-third is happy to share personal information on social media sites.

These attitudes may leave financial institutions more vulnerable to emerging risks, particularly social engineering, where cyber criminals use impersonation techniques to trick employees into divulging confidential information or data.

6 Disconnect between employer and employees

The majority of employers believe that they are doing enough to protect the integrity of customer data.

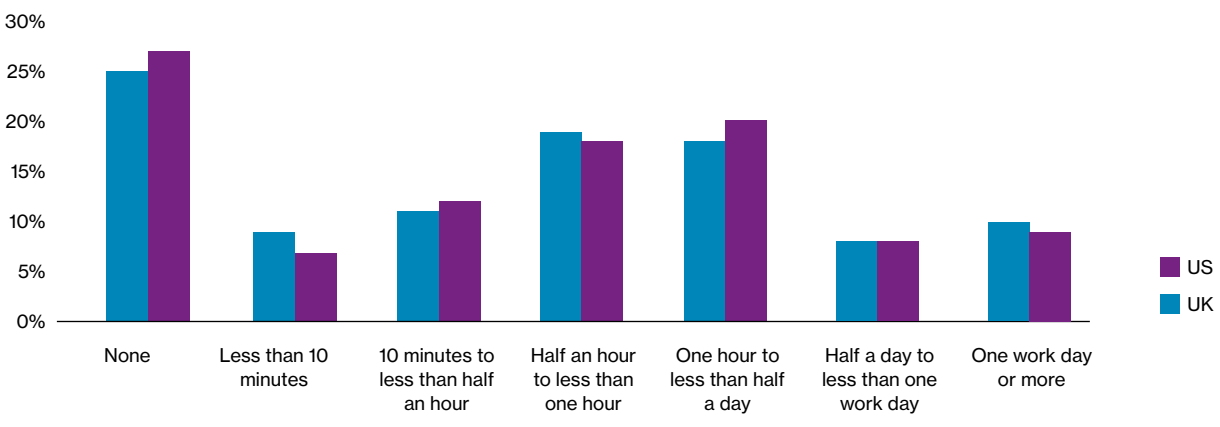
However, around 40% of employees use a work computer or cellular device to access confidential company information and discuss work-related topics in public places. About 30% admit to logging in to a work device on an unsecured public network or using a work computer in public settings. Roughly a quarter take confidential paper files home and use unapproved devices to do work at home. As such, there is a disconnect between company policy and employee behaviours.

Financial institutions are continually looking at ways to make their services more personalised, a strategy that requires the collection of vast amounts of consumer data. Each time employee behaviour exposes this data to hackers, the financial institution is exposed to significant financial and reputational damage.

7 Training

Nearly half of employees surveyed spent less than 30 minutes in training specific to data protection and information security in the last year. Yet the benefits of comprehensive training are clear: 77% believe it increased their sense of personal responsibility for data security at work.

Time spent on cyber training in the last year



So how can financial institutions achieve a culture of cybersecurity?

Given these findings, there is certainly a need to more closely assess the reasons why employees continue to engage in risk-producing behaviours.

Effectively managing people risk: key considerations for financial institutions

1. **Increase the level and regularity of employee awareness training in your organisation.** It is important that employees are trained to understand and respond to cyber threats, such as reviewing emails closely to ensure they are from trusted and known senders before clicking on links. A cyber-savvy workforce holds the key to your enterprise resiliency.

2. **Consider innovative ways to deliver employee awareness training.** Financial services employees have a large and increasing training load covering topics from diversity to regulation. Given our survey finding of the low level of understanding of cyber risks, firms may want to use 'learn by doing' training approaches that will help to embed understanding over a longer term. There are several ways to achieve this – without risking the firm's IT infrastructure – including novel approaches such as gamification and 'cyber ambassadors' – employees who champion cybersecurity.

3. **Assess whether your organisation's IT department has the right or sufficient talent and skills** needed in today's environment to effectively handle these emerging threats.

4. **Evaluate whether your organisation's culture is supportive of cyber awareness and action-oriented behaviours.** For example, do leaders model positive behaviours that encourage employees to do the same and do employees truly know how to report a cyber incident?

Conclusions

Increasingly organisations share the view that effective cyber resilience has its roots in corporate culture and people. Solutions are likely to be complex and multidimensional, as is always the case for any kind of cultural change.

Certainly, financial institutions may have to adapt their operations to the constantly changing nature of cyber threats. They should also pay attention to the expanding risk mitigation options available through the insurance market. But employers will increasingly foster a more cyber-savvy workforce, using innovative employee engagement, talent management and reward strategies to fortify their cybersecurity posture.

Banking: in the spotlight

February 2016: hackers transferred US$81 million from the US Federal Reserve accounts of Bangladesh Central Bank – they originally aimed to take US$951 million. The same hackers are reported to have targeted banks in 18 countries worldwide[10].

November 2016: hackers stole money from 9,000 customers of one UK bank, costing the organisation £2.5 million in refunds to affected account holders.

June 2017: a ransomware attack known as NotPetya hit banks in the Ukraine before spreading globally, also affecting the property arm of one of Europe's largest banks.

Opportunity and risk

By 2020 it is predicted that over two billion people will use mobile banking[11]. In Europe, one in five card payments will be contactless by 2021[12]. 'Challenger banks' and digital-only start-ups are pushing traditional banks to upgrade legacy systems and quickly adapt to new methods of distribution, transaction and customer interaction. For every new technology implemented to deliver customer satisfaction and gain competitive advantage, banks increase their exposure to a range of digital threats such as social engineering, theft of data and cyberterrorism.

Developing threats

The cyber threat landscape is constantly evolving. Social engineering attacks have developed in complexity: from the original 'advance-fee' scams targeting individuals to the more sophisticated 'fake president' frauds that seek to gain access to an entire organisation.

As these attacks develop so too must risk management strategies. However hackers often have the first mover advantage. For example, banks may find there are gaps in their protection when it comes to social engineering as often neither cyber insurance policies nor traditional fidelity policies singularly cover the scope of losses associated with social engineering claims.

Given the acceleration in number and complexity of attacks for banks in particular, it is imperative to fully understand the potential impact of a cyber event and ensure the right business continuity plans and insurance protection are in place.

[10] Asia Finance, 'Cyber attack threat intensifies for Asia Pacific banks', May 2017
[11] Juniper Research, 'Mobile banking users to reach 2 billion by 2020', October 2016
[12] Pymnts, 'Contactless card usage in Europe exploding', November 2016

Cyber risk security

66% of employers viewed cyber security as a fundamental challenge for their organisation

85% of employers think of cyber security as a top priority for the organisation

8% Today

85% In three years

Embedded cyber risk management within their company culture

but only 37% of employers think risk management and HR work closely on cyber risk management

Reporting cyber breaches

Employers

93%

of organisations believe that they have provided an environment in which employees are comfortable reporting about data privacy and data security

43% of employees

received a suspicious email at work meant to trick them into opening a harmful link or attachment

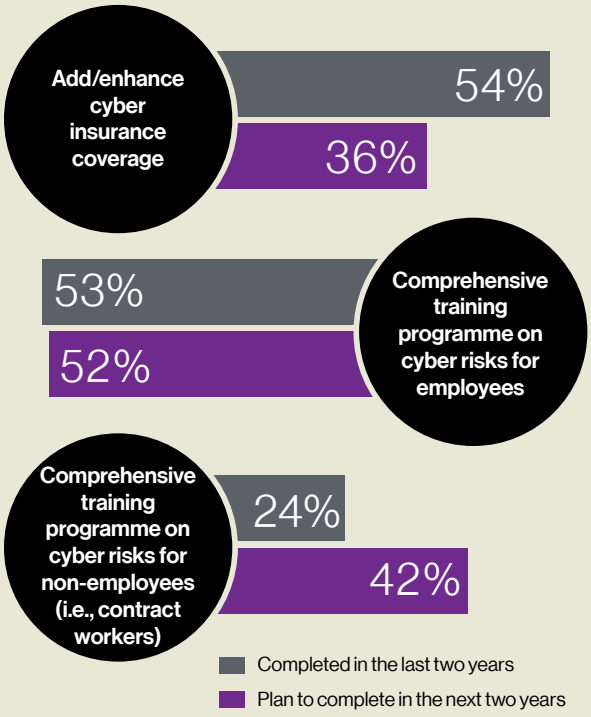
34% of employees

witnessed co-workers behaving in ways inconsistent with data privacy and information security policies

15% took no action

Human factors and business processes will receive the most attention over the next three years

Top actions in the next two years are adding or enhancing cyber insurance coverage and training for employees and contractors and cyber insurance gap



Employees benefit from the training

78%
It improved my understanding of the steps I need to take to better protect confidential information

77%
It increased my sense of personal responsibility for data security at work

63%
It motivated me to change how I manage my personal computing devices

The vulnerabilities around employee behaviours of using technology

82%
of employees have read and understand their company's policies regarding data privacy and information security

41%
use their work computer or cellular device to access confidential company information

22%
use personal computing devices that have not been approved by their company's information technology department to do work at home

32%
log into their work computer or cellular device using an unsecured public network (Wi-Fi)

31%
use their work computer in public settings (for example, while commuting, on airplanes/trains, at cafes)

34%
share personal information (for example,birthdate, employer name, job title) in profiles on social media sites

Source: 2017 Willis Towers Watson Cyber Risk Survey, employer survey, US. Survey respondents include 2,073 U.S. employees and 92 U.S. employers.

Contact details:

Mary O'Connor
Head of Client, Industry and Business Development and Global Head of Financial Institutions Group
Mary.OConnor@willistowerswatson.com

Alexander Van Kuffeler
Head of Financial Institutions Group, EMEA
Alexander.Vankuffeler@willistowerswatson.com

Andre Van Hooren
Head of Financial Institutions Group, Western Europe
Andre.Van.Hooren@willistowerswatson.com

Christopher Nelson
Head of Financial Institutions Group, Australasia
Christopher.Nelson@willistowerswatson.com

Jonathan Bush
Head of Financial Institutions Group, GB
Jonathan.Bush@WillisTowersWatson.com

Michael O'Connell
Head of Financial Institutions Group, North America
Michael.OConnell@willistowerswatson.com

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, optimise 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

20489/09/17

willistowerswatson.com

Willis Towers Watson