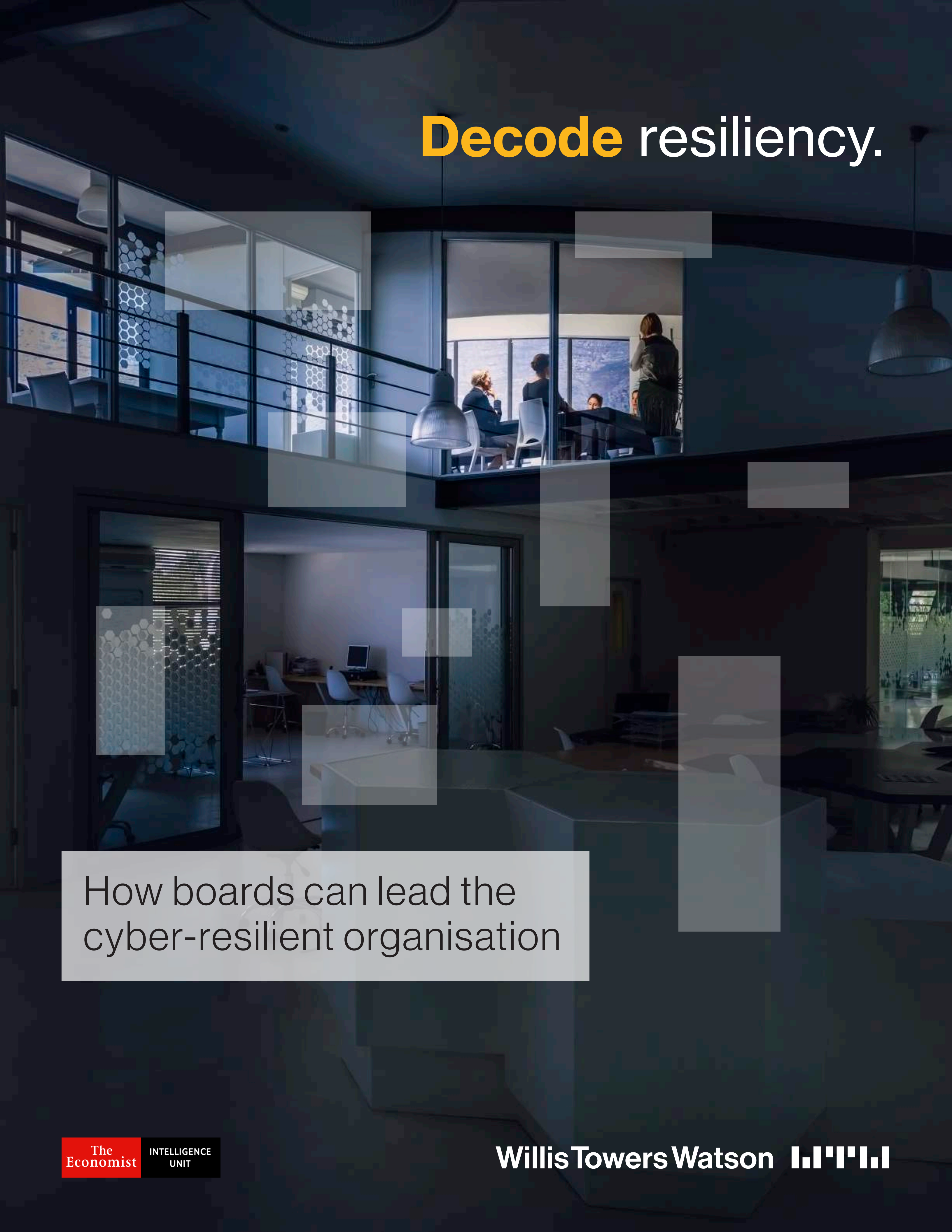


Decode resiliency.

How boards can lead the cyber-resilient organisation

The Economist INTELLIGENCE UNIT

Willis Towers Watson

How boards can lead the cyber-resilient organisation

Introduction

In the cyber world, many are attacked but not all are victims. Some organisations emerge stronger. The most cyber-resilient organisations can respond to an incident, fix the vulnerabilities and apply the lessons to strategies for the future. A key element of their resilience is governance, a task that falls to the board of directors.

"The board helps us to make sure we're preparing for the inevitable – that we have the organisation, the people and the plan to protect ourselves," says Richard Rushing, Chief Information Security Officer (CISO) at Motorola Mobility. "Because when it comes to being attacked, it's not a matter of if but when."

To learn more about the challenges of governing a cyber-resilient organisation, The Economist Intelligence Unit (EIU) conducted a global survey, sponsored by Willis Towers Watson, of 452 large-company board members, C-suite executives and directors with responsibility for cyber-resilience.

Among the findings:

- In the past year, a third of the companies surveyed experienced a serious cyber-incident – one that disrupted operations, impaired financials and damaged reputations – and most placed high odds on another one in the next 12 months.
- Many companies lack confidence in their ability to source talent and develop a cyber-savvy workforce.
- Executives cite the size of the financial and reputational risk as the most important reason for board oversight.

Governing cyber-risks doesn't require that board members become experts in the more technical aspects of cyber-security. Says Ed Amoroso, former CISO of AT&T and a veteran of several boards: "The key is an understanding of risk and good intuition: following your nose on issues that aren't always in the numbers and perhaps just don't feel right."

"It's no different than the oversight responsibility for other risks," adds Ellen Rinaldi, CISO of Vanguard Investments. "It's helping management get where it needs to be, which is to have a strategy for the mitigation of cyber-risk."

About the survey

In March 2018 The Economist Intelligence Unit (EIU) surveyed 452 senior executives and board members with cyber responsibilities on how their companies were attempting to become more cyber-resilient. The survey was sponsored by Willis Towers Watson.

The survey sample is a senior group: half of the respondents are CEOs, presidents, owners or board members; the other half are directors and other C-suite executives. Among those heading up functions, the most common titles are CIO or CISO (80), CFO (23), CRO (16) and CHRO (15).

The companies range in size from US$100m in annual revenue to more than US$25bn. A third of the companies are in North America (the US and Canada), a third in Asia (Tokyo and Singapore) and a third in Europe (100 in the UK and 52 spread across France, Spain, Italy, Germany and the Netherlands).

Respondents are widely distributed across industries: manufacturing and technology (12% each), retail and construction/real estate (10% each) and financial services (9%) are the largest sectors.

The journey to cyber-resilience

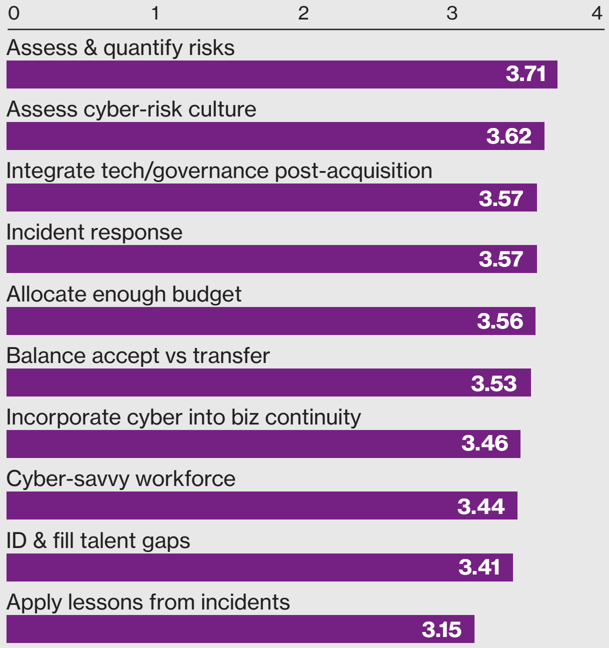
A striking aspect of the EIU survey results is the confidence that many executives possess in their companies' cyber-resilience abilities. Using a scale of one to five, where five is "well above average" and one is "well below average", the survey asked executives to rate themselves relative to their peers on ten areas of cyber-resilience. *(Figure 1)*

Any rating over three is above average, and respondents gave themselves ratings over three in every area of cyber-resilience. Since not everyone can be above average, at least some are overconfident. Nevertheless, the relative rankings of their assessments offer clues as to where companies are lagging in their journey to resilience.

Specifically, a large number of executives feel they're not doing as well as they could in learning from failures. *(Figure 2)*

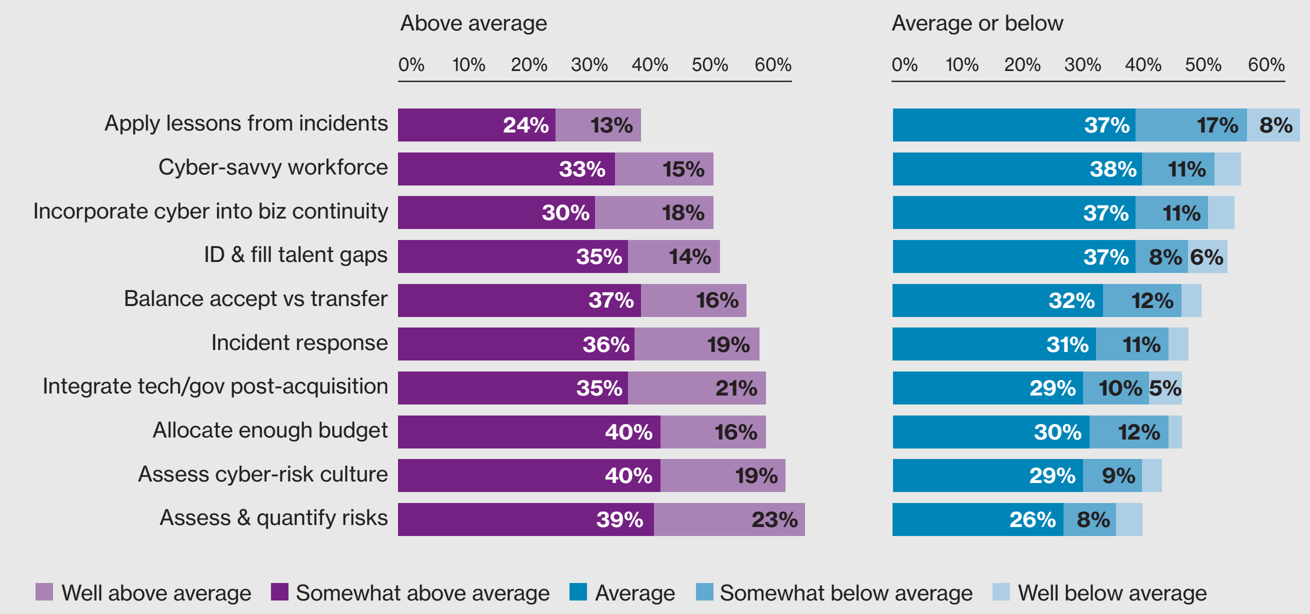
Only 13% —the smallest proportion of any of the competencies measured —give themselves a rating of well above average compared with peers in applying the lessons of security incidents.

Figure 1. **Average self-assessment on a scale of 1 to 5**



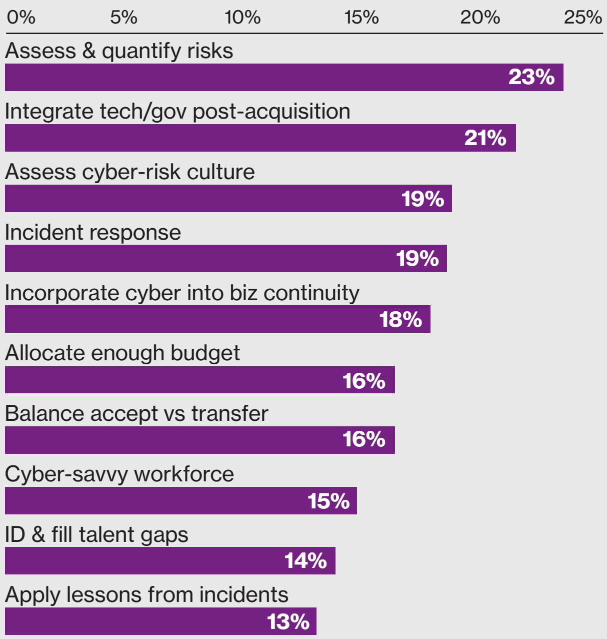
(Note: Since five is "well above average", the higher the number, the higher the self-assessment.)

Figure 2. **How companies assess their cyber-resilience competencies**



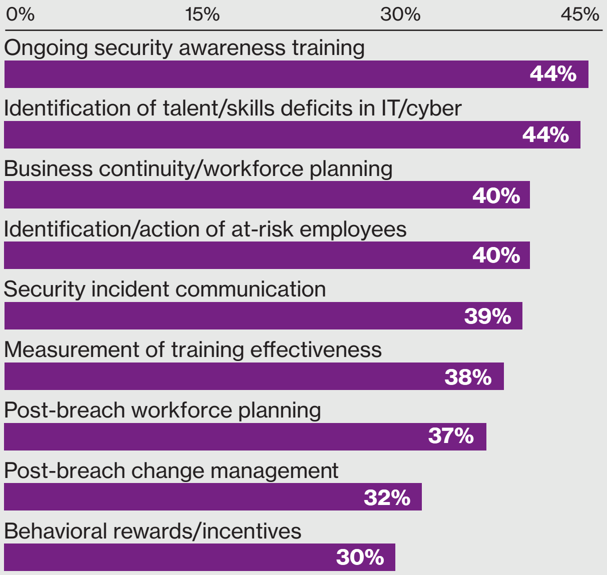
Two other areas in which executives see a deficit are the ability of their organisations to identify and fill gaps in cyber-talent along with the capacity to develop a cyber-savvy workforce. While boards generally don't focus on cyber-talent issues beyond the qualifications of the CISO, these deficits speak to cultural issues that do fall within the board's remit. The human side of cyber-resilience is clearly an area that the C-suite and board members believe their organisations could improve. *(Figure 3)*

Figure 3. **How companies assess their cyber-resilience: Percent who say they're "well above average" relative to peers**
(A closer look at the "well above average" ratings from Figure 2)



The survey supports this view. Less than half of companies surveyed had implemented seemingly basic cyber-related human resource policies, such as ongoing security awareness training, identification of at-risk employees and internal communications after a security incident. The presence of such policies indicates a strong and broadly accepted culture of cyber-security governance. Their absence suggests that many companies are remiss in building a culture of cyber-resilience — a matter that should be of concern to the board. *(Figure 4)*

Figure 4. **The % of respondents who employ the following policies**



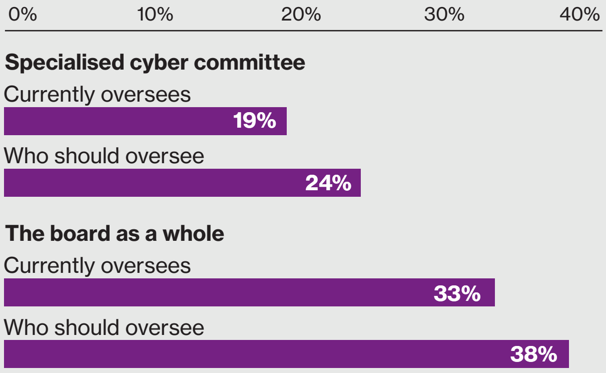
Who leads?

At the board level, cyber presents a dilemma. It's both critical enough to demand the attention of the board as a whole and specialised enough to require expertise that generalists don't have. This problem isn't unique to cyber: delegating specific types of risk to subcommittees could lead to mirroring silos at the board level, countering the board's need to keep its focus on risks that affect the entire enterprise.

This dilemma is reflected in the survey results. Executives were asked two questions: who at the board level oversees cyber and who should oversee it? A growing proportion of companies believe in one of two things: that cyber should be overseen by the board or by a cyber-committee. A shrinking or stable proportion says it should be the responsibility of audit, risk or some other subgroup. *(Figure 5)*

In fact, it's possible to combine the two approaches: educate the generalists and simultaneously develop a strong and consistent working relationship with a smaller group with more in-depth knowledge. Says Vanguard's Ms. Rinaldi: "It's helpful for the CISO to work with a smaller group that becomes more deeply informed. But there should be a significant amount of cyber-education provided to the whole board."

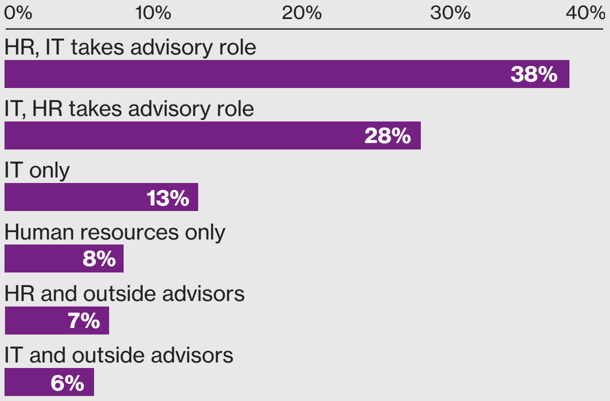
Figure 5. **Where oversight should lie: The board or specialised committee?**



At the operational level, the specialist-generalist issue also arises. Cyber requires specialised knowledge and skills – specialised even within the world of IT – and enterprise-wide business, workforce and process capabilities. In particular, because workforce vulnerabilities contribute to so many intrusions, a strong partnership between HR and IT is imperative. *(Figure 6)*

Two-thirds of the companies surveyed point to this partnership when describing how they develop their employee-related cyber-risk policies. At 38%, HR leads with IT advising; at 28%, IT leads with HR advising. Overall, HR leads the charge at just over half of the companies surveyed, whether on their own (8%), with outside advisors (7%) or working with IT (38%).

Figure 6. **Who takes the leading role in developing employee-related cyber-risk policies?**



But HR's role extends far beyond policy. Just as important is the day-to-day operational relationship with cyber-security staff. Says Motorola Mobility's Mr. Rushing: "When someone changes locations or roles, it can change their access. Are they local or remote? Management or staff? Why do they log in from Chicago one day and Brazil the next? If you get access wrong, the employee can't do their job and sets off alarms unnecessarily. Or you leave yourself open to a breach. That's a line you need to walk. And you can't do it without HR."

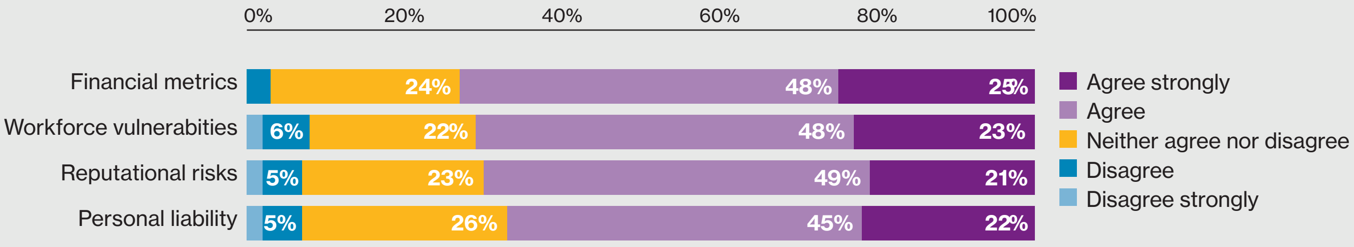
Few would argue about the benefits of a strong relationship with HR. Taking it a step further, Mr. Rushing's comment reflects a specific instance of a broader idea: A culture of co-operation across functions helps make organisations more secure and, in the event of a breach, more resilient.

Getting better at communicating with the board

There's at least a perceived problem in communicating cyber-security issues to the board. Many cyber-conferences offer sessions to train CISOs on how to address management. And CISOs commiserate about the need to "dumb down" their presentations.

Yet companies tend to think their cyber-resilience heads do a good job presenting to the board. Consistent with their high level of confidence elsewhere, no more than 8% of executives disagree strongly with the statement that their cyber-resilience head does a good job communicating the financial, workforce, reputational or personal consequences of cyber threats. *(Figure 7)*

Figure 7. **Our cyber-resilience head does a good job presenting:**



At the same time, there's room for improvement. Only a quarter of executives agree strongly (five on a scale of one to five) that their cyber-resilience heads communicate well, and under 15% give their CISOs or equivalents the top rating on a scale of one to ten.

There is always the potential for trouble when specialists present to generalists. In the case of cyber-resilience, there are two languages at play, one quite technical and one based on a risk framework. The question is how to best bridge the gap.

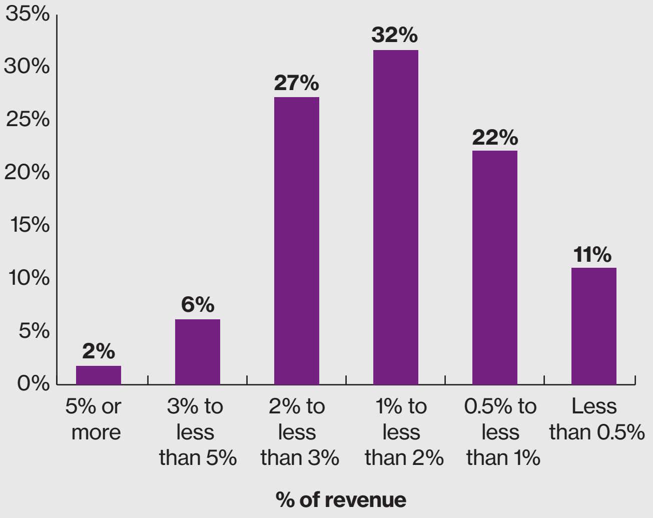
"The board speaks in a language I call boardroom," says Mr. Rushing. "Other languages don't translate well. The common denominator is dollars at risk. You can say, 'we would put US$20m of revenue at risk by doing this,' knowing that the CFO will question each number and you need to be prepared to explain why the number is real."

Executives don't believe they're spending enough

Given the magnitude of the risk, most executives think they aren't spending enough on cyber-security and cyber-resilience. There's no clear consensus on where the extra dollars should go. But widely used risk frameworks can provide some guidance.

Among the 452 companies surveyed, the average spend on cyber-resilience is about 1.7% of revenue. Spending is close to normally distributed around the mean: a third spend 1-2% of revenue, a third spend more and a third spend less. *(Figure 8)*

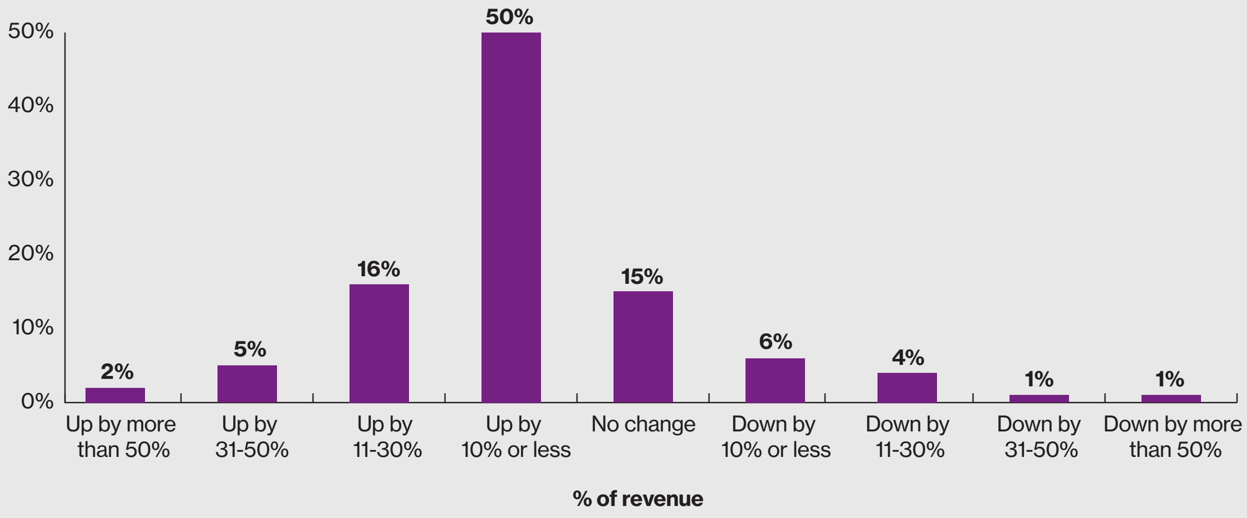
Figure 8. **Cyber-resilience spending as a percent of revenue**



However, few think they're spending enough.

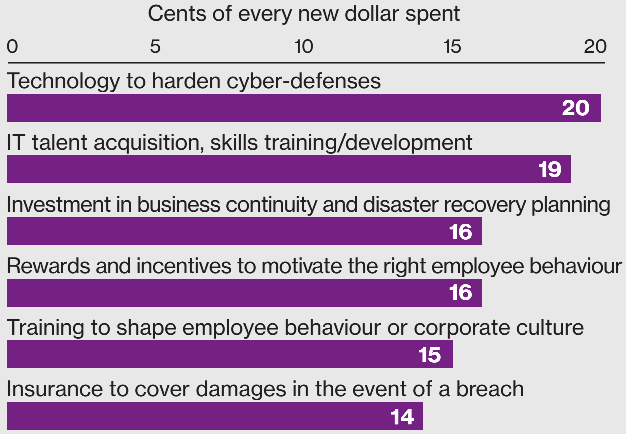
Three-quarters of the survey respondents say that the risk of cyber-intrusions mandates that they invest more – half up to 10% more, and another 23% more than 10%. Only 15% say that they are spending the right amount, and 12% believe they should spend less. *(Figure 9)*

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



Where should the new dollars go? It's difficult to generalise across companies in different situations and industries, and there is indeed little consensus among executives on how to allocate new money. The rote answer to all cyber-security questions is technology, and "technology to harden cyber-defences" did come in first – but just barely, with 20 cents of every new dollar. *(Figure 10)*

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



However, there is no significant difference between the votes for spending more on technology and investments in talent and training (19 cents). In fact, if all of the human capital-related expenditures is added up, it totals 50 cents out of every new dollar – and it could be argued that business continuity and disaster-recovery planning is human capital-related as well.

Insurance comes in last, at 14 cents of every new dollar, even though sales of insurance against breaches are growing fast. Nevertheless, 14% of new spending on cyber-resilience could still be a large sum. And since most large corporations already have cyber-insurance in place, the survey response could simply represent first-time buyers.

Cyber-resilience professionals have more definitive ideas about how to spend new budget. Says Mr. Rushing: "The NIST Framework has five categories: identify, protect, detect, respond and recover. You could invest 20% in each bucket. The technology falls mostly in the protect category, and lots of companies spend 75% on protect. That means the other four are shortchanged."

He also makes a case for spending more on identifying vulnerable assets. "I laugh when someone estimates how many computers are on their network. Why is it approximate?

If you don't know exactly, you should spend more on identification. You can't fix your vulnerabilities if you can't identify which assets are yours."

Ms. Rinaldi highlights the need to pay attention to resilience as well as protection. "I think many companies have concluded that they have to spend more time and effort getting recover and respond down," she says. "But that doesn't solve the problem. For that you need to remediate – to fix whatever the issues are so it doesn't happen again."

Learning from failure

Nobody likes to fail. And often a cyber-intrusion is seen as a failure on the part of the CISO, who might pay for it with their job.

But failure can be seen in a positive light as well. When there are no intrusions, it's often unclear what an organisation did right, and it's easy to become complacent. "A lack of obvious problems often causes security processes to suffer," says Mr. Rushing. "In the most extreme form, people start saying, 'look, we have back-up tapes. Maybe that's enough.'"

Failure usually teaches a lesson. In the words of Nassim Taleb, "difficulty is what wakes up the genius." The key is to learn from each intrusion. And that's exactly what many survey respondents say they aren't very good at.

The executives surveyed consider their organisations good at incident response –19% say they are well above average and another 36% consider themselves above average. But they are more circumspect about their ability to learn from their failures. When asked to rate themselves on "incorporating learnings from incidents into new defensive strategies," only 13% say they are well above average (and a quarter admit to being below average, the highest proportion of any of the ten competencies).

However, the cyber-professionals interviewed have plenty of advice on learning from failure. "You don't have to restrict yourself to failure in your organisation. Intrusions are reported in the press every day," says Ms. Rinaldi. "When you see one, you ask, 'could this have happened here? What would have caused it to happen here? What can we put in place so it won't happen here?'"

"On the technical side, you now have the availability of sandboxes to test how the threat would operate within a particular technological environment," she continues. "You figure out the protections you can put in place and then you put them in place."

Ms. Rinaldi concludes: "When there's an incident in your own organisation, you need the discipline to consistently set up post-breach meetings, walk through the exact process and issues, lay out a follow-up plan and follow that plan to the end."

Remember that a plan is not the same as the real thing, warns Mr. Rushing: "In some places, after an intrusion, it has taken three to four weeks to get everything back up and operational. There was a plan, but that's all it was – not much vetting, no dry runs, no tabletops."

Finally, don't punish failure. Says Mr. Amoroso: "If a company gets hacked, the CISO gets fired. That's the opposite of what should happen."

Conclusion

Despite the confidence expressed by survey respondents, there is broad consensus that more cyber-resilience education is needed, both within the workforce and at the board level.

Cyber-resilience only came onto the radar when the internet came of age in the early 2000s. As a result, it is often the digital natives that have the most exposure to, and knowledge of, cyber-security issues. “Their instincts are a hundred times better than even the most experienced board member,” asserts Mr. Amoroso. “That’s good news. They’re going to come up through the ranks and they get it.”

Education will speed the transition. It can be argued that the education that may have the biggest payoff will focus on the least tech savvy and yet most influential members of the organisation: those on the board.

That’s not where education should end, of course. The survey highlights the need for investments to address skills deficits and win the war for talent. The high marks executives give themselves on risk assessment and technology integration also suggest that investments in these areas – associated with the identify and protect phases of risk management frameworks – have diminishing returns relative to the more human capital-related respond and recover phases.

Technology is less of a differentiator than it used to be, necessary but not sufficient. As the emphasis shifts from cyber-security to cyber-resilience, the business, process and workforce aspects increase in importance relative to specialised technical expertise.

“Resilience is a combination of things. It’s technology, it’s people, and a lot of it is process and an integration between the technology side and the business side. It’s what I believe, and it’s what I believe the board should be looking at as well,” says Ms Rinaldi.

North America: More attacks, more to come, more resilience

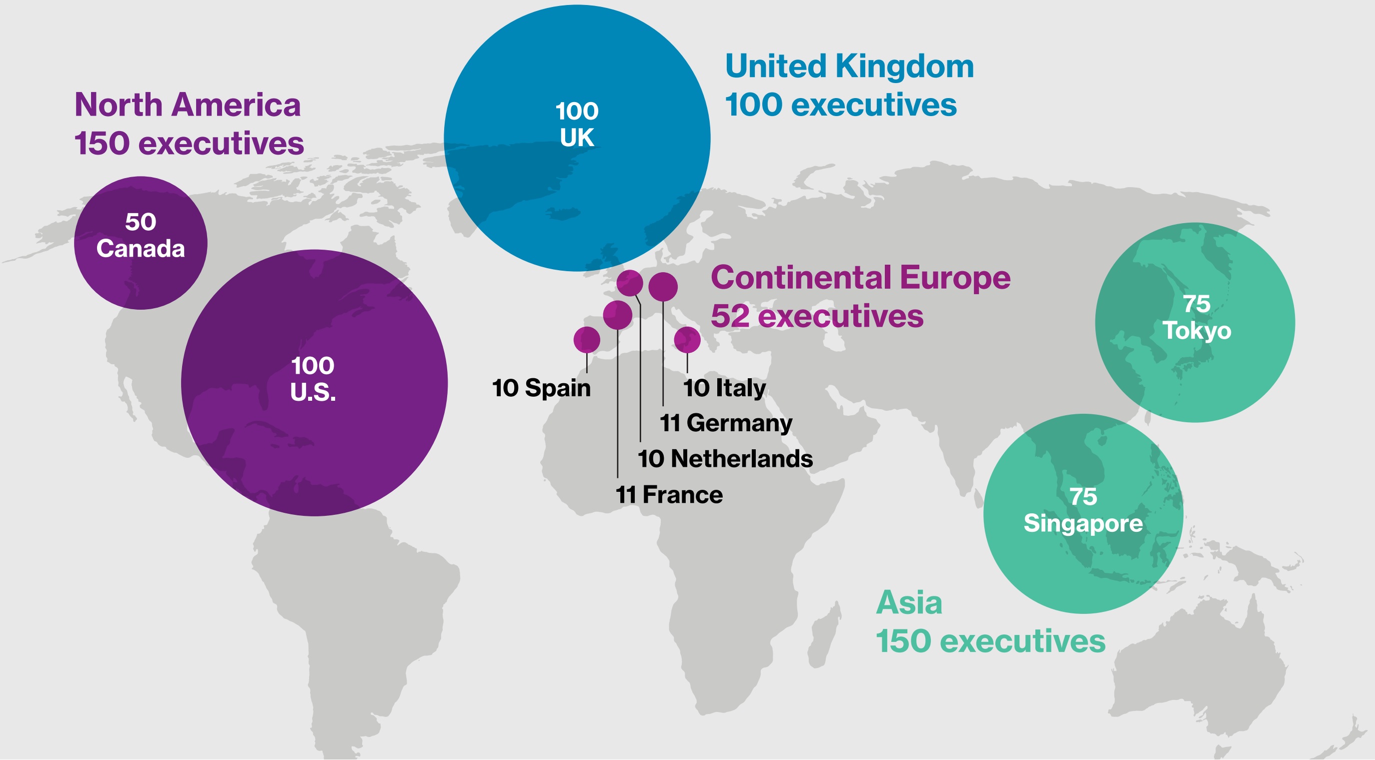
Cyber-resilience is a global issue. In most areas of the Economist Intelligence Unit survey executives respond in similar ways irrespective of where they are located. But companies in the US and Canada contrast strongly with their peers in Asia, and to some extent Europe, in the following areas:

1. Frequency and impact of attacks and expectations of new intrusions;
2. Confidence in their ability to recover from such intrusions; and
3. Belief in their board’s expertise and plans to recruit new board members.

More US and UK survey respondents report that they have been attacked. The US also ranks first, usually by a large margin, in the proportion of companies who say:

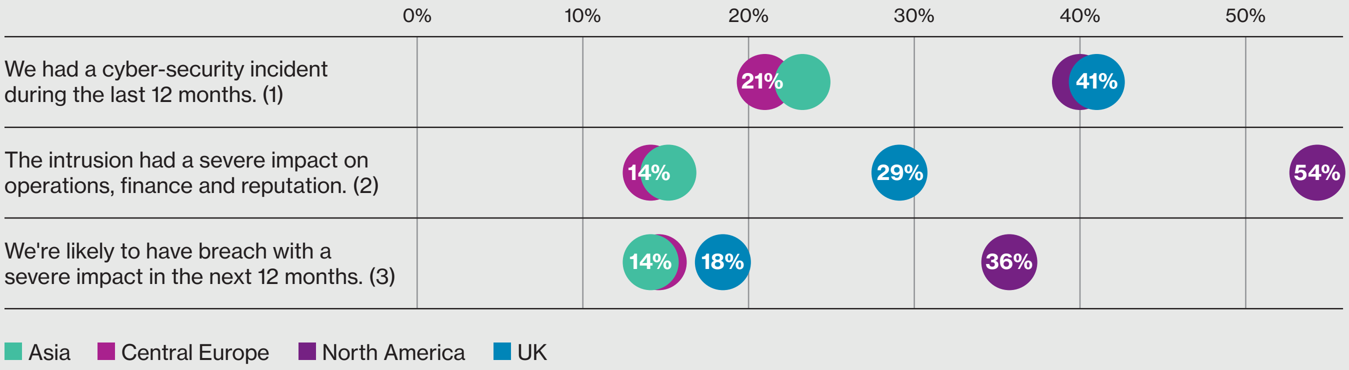
- The intrusions had a severe impact;
- They expect to be attacked in the future;
- They’re well prepared for intrusions;
- Their boards are well-versed in cyber;
- Yet they’re also aggressively recruiting more cyber-expertise.

Figure 11. **Survey participants by region and country**



Frequency and impact of attacks and expectations of new intrusions. UK (41%) and North American (40%) companies were much more likely than those in other regions to have experienced an intrusion in the last year. (Note that the North American figure averages the US and Canada, and a higher proportion of US firms experienced an intrusion.) North American companies were far more likely to say the intrusion had a serious impact on their operations and financial results, and to gird themselves for another attack in the months to come. *(Figure 12)*

Figure 12. **North America and the UK suffer from intrusions the most (and they're more serious)**



(1) Respondents who answered "yes."
(2) Respondents who rated the severity of the impact one on a scale of one to five, averaged across the systems/operations, financial and reputational impacts.
(3) The average percentage of respondents who rated the probability of a breach one on a scale of one to five.

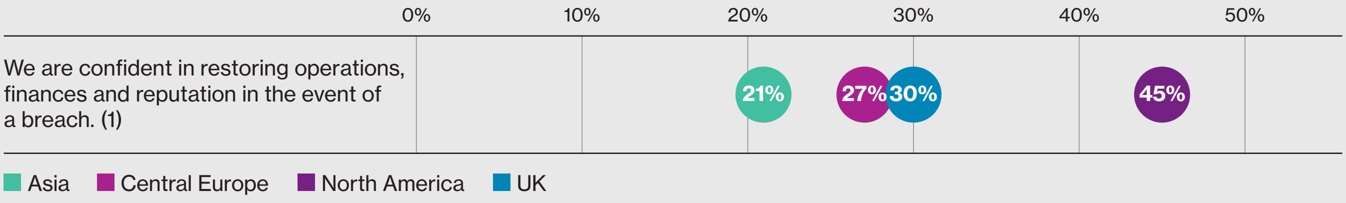
While a significant proportion of Asian and European companies said the same, the numbers were far lower. Surprisingly, even though 41% of UK executives reported an intrusion during the past year, only 18% expected it to happen again during the coming year. Indeed, in every region, more executives reported past intrusions than expected future ones. Is this a sign of strengthened defenses or one of complacency? The answer is critical to their cyber-resilience efforts.

Confidence in their ability to recover. North American and UK firms were attacked far more than those in other regions. More North American firms characterised the damage from their attacks as serious and more expected another attack in the near future. And far more North American firms also expressed confidence in their capabilities to repair the damage and proceed with business as usual. *(Figure 13)*

Note that the chart shows averages across three intrusion impacts: operations, financial results and reputation. In every region and across the survey as a whole, the executives said reputation was the toughest to restore.

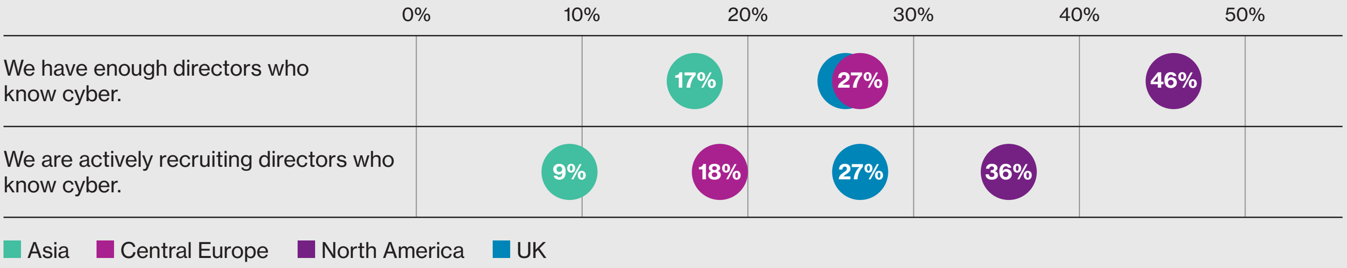
You can't have too much cyber-expertise. A third area in which North American firms differ is in their active recruitment of board members with cyber-expertise – even though nearly half of the North American executives surveyed already gave themselves high marks for board expertise. The biggest contrast was with Asia, where relatively few (17%) companies had a high level of cyber-expertise, and even fewer (9%) saw a strong need to bring cyber-expertise on their boards. *(Figure 14)*

Figure 13. **North American firms are most confident in restoration after a breach**



(1) Respondents who rated themselves one on a scale of one to five (average across the operations, financial results and reputation).

Figure 14. **North American firms are both confident in board expertise and seeking more (1)**

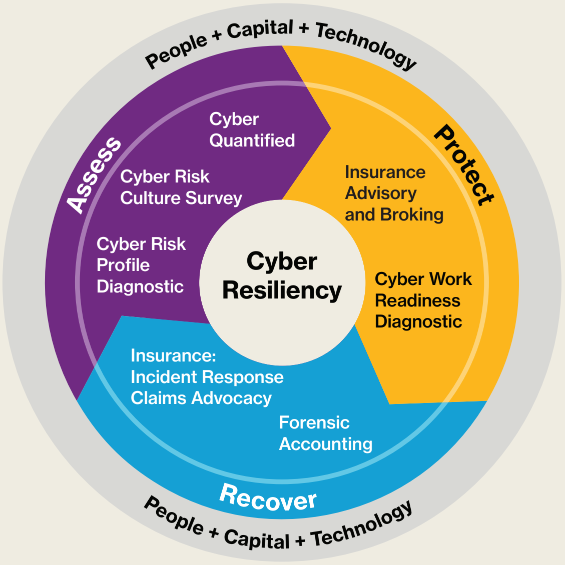


(1) Respondents who rated themselves one on a scale of one to five

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.

People + Capital + Technology = Cyber Resiliency


People + Capital + Technology
Assess
Protect
Recover
Cyber Quantified
Cyber Risk Culture Survey
Cyber Risk Profile Diagnostic
Insurance Advisory and Broking
Cyber Work Readiness Diagnostic
Insurance: Incident Response Claims Advocacy
Forensic Accounting
Cyber Resiliency
People + Capital + Technology

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.

willistowerswatson.com/social-media

WTW-GL-18-RES-5381a

willistowerswatson.com