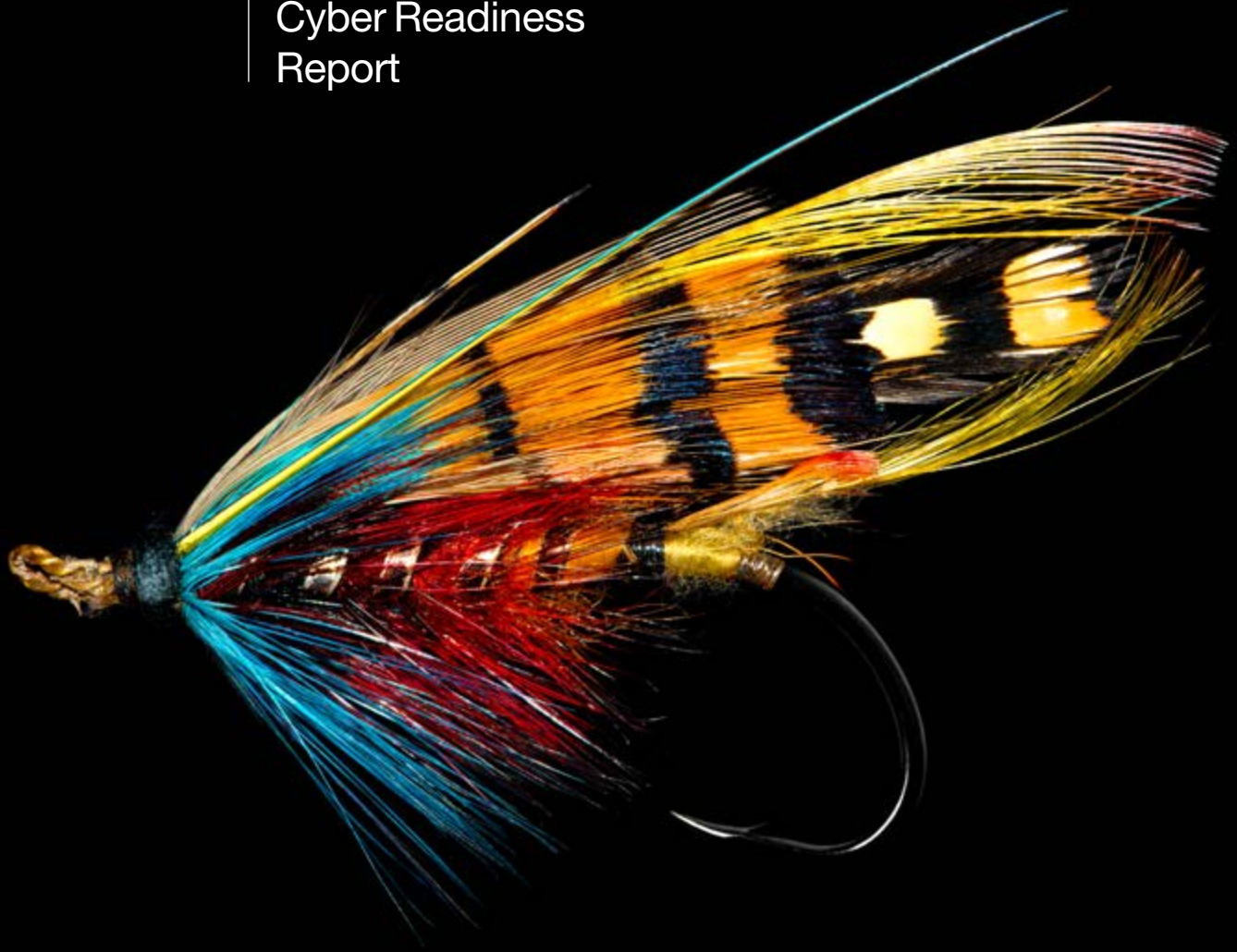
HISCOX

2018 Hiscox Cyber Readiness Report



The Hiscox Cyber Readiness Report is compiled from a survey of more than 4,100 executives, departmental heads, IT managers and other key professionals in the UK, US, Germany, Spain and The Netherlands. Drawn from a representative sample of organisations by size and sector, these are the people on the front line of the business battle against cyber crime. While all are involved to a greater or lesser extent in their organisation's cyber security effort, 45% make the final decision on how their business should respond. The report not only provides an up-to-the-minute picture of the cyber readiness of organisations large and small, it also offers a blueprint for best practice in the fight to counter an ever-evolving threat.

Foreword
Countering the cyber threat

Cyber security poses a challenge unlike any other. Businesses large and small, both public and private, face an enemy that is unseen and largely unknown, has seemingly shape-shifting powers and appears utterly unrelenting. Each year brings a renewal of the contest but in a subtly different form. This is an enemy that can be confronted but never quite defeated.

If anyone still harboured doubts about the severity of the threat, the events of the past year should have dispelled them. From the WannaCry ransomware attack to the hacking of one of the world's largest credit agencies, 2017 produced numerous reminders that operating in a connected world has fearsome perils. The cost of these attacks has undoubtedly run into the billions.

It is an old adage that you should hope for the best but plan for the worst. That is certainly true when it comes to battling cyber crime. In today's world, there is no alternative to investing in sophisticated prevention and detection systems and supporting them with the people and processes that will make them effective. This study not only reinforces that message but it provides a detailed picture of what cyber readiness really looks like.

This is the second Hiscox Cyber Readiness Report, conducted by Forrester Consulting, and it has been expanded to cover more than 4,100 organisations, large and small, in both private and public sectors, across five countries – the UK, USA, Germany, The Netherlands and Spain.

It puts the spotlight not only on the financial consequences of individual cyber breaches but also on the enormous cost in terms of investment made to counter the threat. Above all, it measures the cyber readiness of respondents using a multi-dimensional model built on best practice in cyber strategy and execution. As an end of term report, it might have the words 'can do better' scrawled on it in red ink. It highlights the cyber readiness shortcomings of the majority of the organisations in our sample, particularly the smaller ones.

On the plus side, however, it offers valuable insights into how firms can up their game and strengthen their defences. Often the answer is not 'more technology' but proactive thinking, more rigorous processes and better trained staff.

Hopefully, this report will provide a spur to further action. It is certainly timely. As the following pages show, if an organisation was spared a serious attack in 2017, there is a good chance it will be targeted in the future. The resultant economic loss is only part of the story; the potential harm to a firm's reputation and its standing with customers can be significantly more damaging.

For an increasing number of organisations, a key part of the solution is to transfer some or all of the risk to an insurer. Hiscox is a specialist provider of cyber and data risk insurance, providing standalone cover to more than 20,000 firms, big and small, around the world under the CyberClear brand. For many of those customers, peace of mind is matched by the knowledge that they can turn to us to help them get back up and running after a serious incident.

As an indication of how seriously we take the issue of customer support in this area, we have just launched a cyber academy, which is designed to aid cyber risk awareness among our customers and improve their ability to detect and respond to cyber threats.

At Hiscox, we will continue to expand our services in cyber and play our part in helping mitigate the impact of cyber crime on our customers. We hope that in aiding understanding of the issues involved, and highlighting cyber readiness best practice, this report contributes to that process.

Gareth Wharton
Cyber CEO
Hiscox

Executive summary

Hope for the best but plan for the worst

Seven out of ten organisations fail the cyber readiness test. We measured organisations' cyber security readiness according to the quality of their strategy (broken down into oversight and resourcing) and execution (processes and technology). From this we produced a cyber readiness model that divided respondents into 'cyber novices', 'cyber intermediates' and 'cyber experts'. Nearly three-quarters of organisations (73%) fell into the novice category, suggesting they have some way to go before they are cyber-ready. Only 11% qualified as experts.

Keen awareness of the threat. While many firms lack adequate defences, most are keenly aware of the potential impact of a cyber attack. Two-thirds of respondents (66%) rank the cyber threat alongside fraud as the top risks to their business.

Larger firms show the way. The larger organisations in the sample are better prepared: more than one-in-five (21%) of those with 250 employees or more rank as experts. A further 17% qualify as intermediates. US and UK firms generally score better than the rest (13% are experts) while Dutch firms come bottom of the pile (just 7% are experts). Not surprisingly, perhaps, technology, media and telecoms organisations score highly. At the other end of the scale, professional services firms have some catching-up to do.

Smaller firms lack resources. Organisations with fewer than 250 employees devote a smaller proportion of their IT budgets to cyber (9.8% on average versus 12.2% for larger organisations). In accordance with the findings mentioned above, just 7% of smaller firms rank as cyber experts.

You get what you pay for. On average, the organisations in our sample had an IT budget of $11.2 million, of which 10.5% was devoted to cyber security. However, the cyber experts had markedly bigger IT budgets than the novices ($19.8 million on average versus $9.9 million) and devoted a higher proportion to cyber security (12.6% versus 9.9%). Some firms spent a lot more – with 37% devoting between 11% and 25% of their IT budgets to cyber. Financial services firms are the largest spenders on cyber, followed by the pharmaceuticals and healthcare sector and then government entities.

Experts more proactive. What sets the cyber experts apart from the cyber novices? Nine out of ten (89%) have a clearly defined cyber strategy, most (72%) are prepared to make changes after a breach and 97% incorporate security training and awareness throughout the workforce. Seven out of ten (72%) have conducted phishing experiments to gauge employee preparedness and three out of five (60%) say they have cyber insurance.

Evens chance of being targeted. Almost half (45%) of the 4,103 organisations surveyed were hit by at least one cyber attack in the past year and two-thirds of those targeted suffered two or more attacks. Spanish organisations were the most heavily targeted (57% suffered an attack). Financial services, energy, telecoms and government organisations are prime targets for hackers.

Costs range up to $25 million. Taking only those organisations that were targeted, the average cost of cyber crime, aggregating all incidents, to each business over the past year was $229,000. But the average masks some wide variations. For the largest organisations in the report (those with 1,000-plus employees), the average costs ranged between $356,000 in Spain and $1.05 million in the US. Some organisations faced still higher costs – up to $25 million in the US and $20 million in Germany and the UK. For the very smallest (those with fewer than 100 employees), average costs ranged between $24,000 in Spain and $63,000 in Germany.

German firms face costliest incidents. We asked organisations to estimate the cost of their single largest incident. German firms reported the highest average figures with the highest cost for a single incident of $5m. At the other end of the scale, Spanish organisations contained the cost per incident to a maximum of $800,000.

Spending set to rise. Nearly three out of five respondents (59%) plan to increase their cyber security budgets in the year ahead. New technology tops the shopping list despite this being the area where the bulk of firms appear best prepared. The experts lead the way: for example, more than half (55%) plan to increase spending on awareness training compared with only 29% of novices.

Watershed year for cyber insurance? The EU's General Data Protection Regulation (GDPR) comes into force in May. With tough penalties for the loss of personal data, it is expected to provide a boost to European take-up of cyber insurance. The report shows that one-third (33%) of respondents currently have standalone cyber cover while a further quarter (25%) say they plan to take out cover in the coming year. Nearly two out of five (38%) still say they have no plans to take out cover. Most likely to be covered are financial services firms (48%). The report also reveals considerable confusion over the extent to which firms are covered for cyber incidents under their general business policies.

25%

Large UK organisations (more than 250 employees) rank among the most cyber-ready in the study. A quarter of them qualify as cyber security experts. The figure is topped only in the US (26%).

$20m

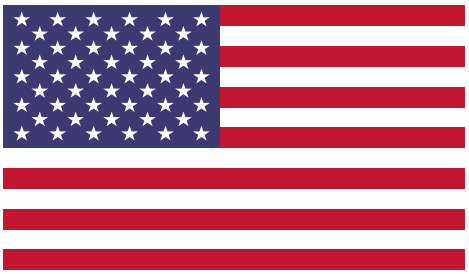
With the largest average IT budgets, UK firms top the table for spending on cyber security. However, the cost of breaches is still among the highest in the survey: for larger UK firms that were targeted in the past year, costs ran to $20 million, with an average of $463,000.

82%

More than four in five (82%) Dutch organisations rank as cyber novices. Despite the fact that they are most likely to have suffered at least three cyber attacks in the past 12 months (experienced by 47% of Dutch respondents), they come bottom of the table for both IT spend and for the proportion devoted to cyber security.

42%

Dutch firms lag in other areas too. For instance, they are least likely to provide cyber security training and awareness programmes across the workforce: only two in five (42%) do so.



30%

US organisations emerge as the most cyber-ready. Some 30% of US respondents rank either as cyber security experts or intermediates. Nearly half (45%) have a formal cyber security strategy and two-thirds (67%) consistently deploy antivirus or antispyware technologies.

53%

More than half (53%) of the US government entities in the survey report an attack in the past year. Among the larger US organisations that were targeted, the cost of cyber attacks ran to $25 million with the average coming out at $578,000.

11%

Spanish organisations devote the largest proportion of their IT budgets to cyber at 11%. Two-thirds of firms targeted(67%) made changes after an attack (compared with 53% across the five countries).

57%

They are the most heavily targeted, with 57% reporting one or more attacks in the past year. They are most likely to cite external attacks as the most common source of cyber incidents that have interrupted their business in the past 12 months (29% of them).

64%

German firms are most likely to involve the board in the strategy-setting process (64%, do so), but only 38% have a formal cyber security strategy.

$5m

Among the smaller firms in the survey (up to 250 employees), German ones have been hit hardest by cyber crime, with an average cost of $55,000 over the past year. When it comes to individual incidents, German organisations also report the highest cost figures – ranging up to $5 million.

A watershed year for cyber
Commentary by Robert Hannigan

Robert Hannigan is a former director of the UK Government's Communication Headquarters and was responsible for setting up the UK's National Cyber Security Centre. He is an adviser to Hiscox.

Last year was the moment when major international cyber attacks hit the headlines and affected individuals and companies simultaneously in dozens of countries.

High profile victims suffered severe reputational and financial damage, sometimes because they had not taken the threat seriously and done the basics, and sometimes because their handling of the breach revealed deeper corporate failings. For smaller companies, the inability to operate, for example after a ransomware attack, was fatal for the business.

If minds were not already focused by this, 2018 promises to be the year when mandatory reporting of cyber breaches raises awareness and reputational risk further, as the EU General Data Protection Regulations (GDPR) come into force.

The cyber threat itself is set to grow in volume and severity, as criminal groups gain access to more sophisticated tools and become more reckless. The rapid growth of the 'internet of things' will amplify insecurities by adding millions of new devices with minimal built-in security. For those trying to protect against attack, the shortage of cyber skills will continue to be chronic.

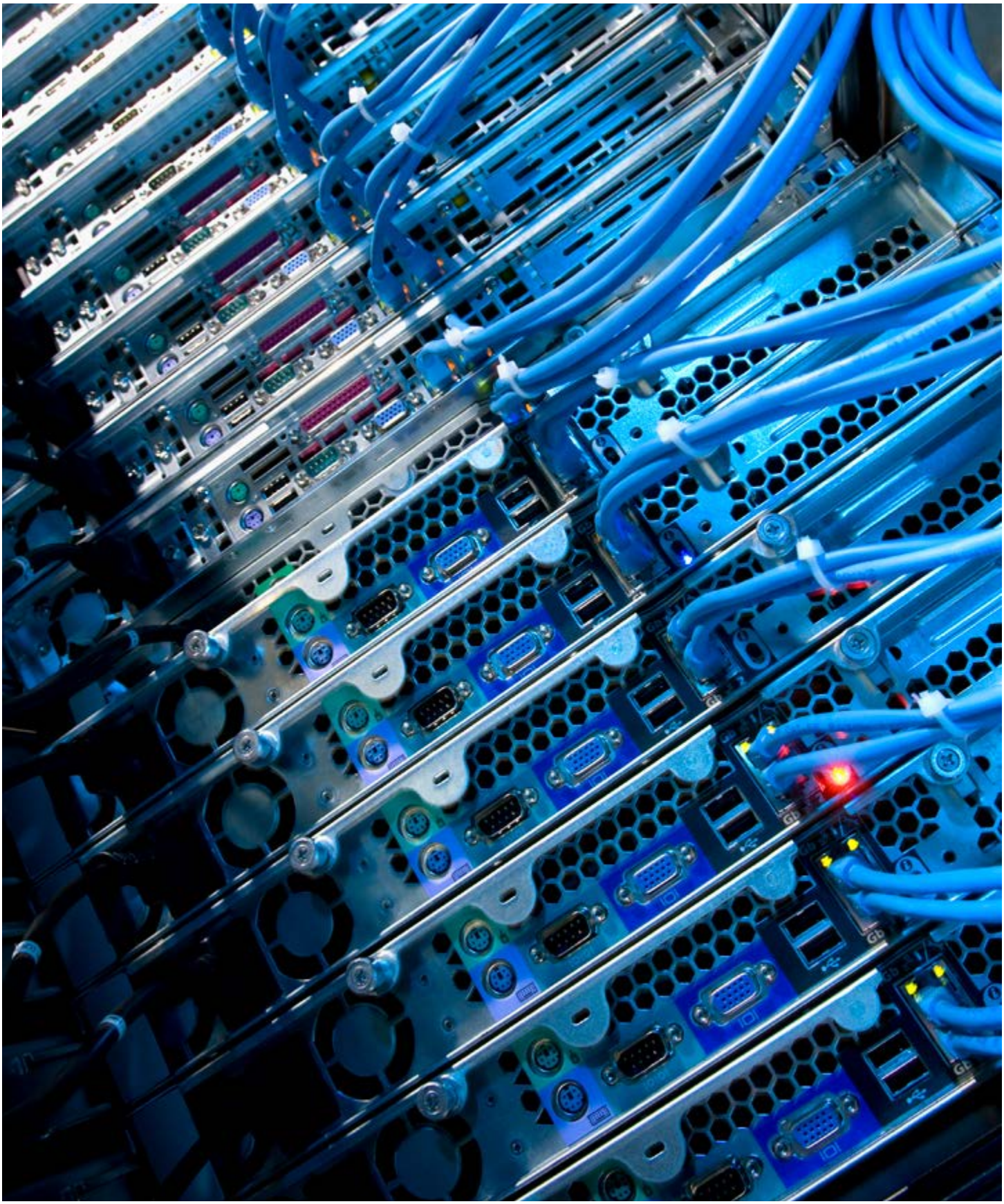
Against this background, Hiscox's Cyber Readiness Report once again gives a fascinating snapshot of how companies have been affected and how prepared they are. Nearly half of the organisations surveyed knew they had been attacked; the rest had either successfully prevented attacks or, particularly in the case of smaller companies, may have missed breaches altogether.

The average losses for companies are substantial: anything from $55,000 for smaller businesses in Germany to $25 million for a large enterprise in the US.

The survey highlights a widening gulf between those who 'get' cyber security, take it seriously, and spend appropriately, and those who still regard the issue as someone else's problem. Cyber security is not an IT issue but rather a risk for the whole organisation; tackling it is more about people, behaviour and culture than clever technology.

Those companies which have successfully prevented attacks or handled them well when they got through, have understood that cyber is a fast-moving but manageable risk. Insurance has a key role to play in helping companies to get that risk management right, both in prevention and incident response.

The growth of the cyber insurance market, especially in the US, underlines this. Together with more assertive activity from regulators in many countries, insurance will help to raise the baseline of security for the whole economy as well as saving many smaller companies from severe damage.



In May 2017, the WannaCry ransomware attack affected up to 300,000 computers in 150 countries, making it the largest such attack to date. The cost has been estimated at up to $4 billion.

Gauging the scale of the cyber threat
What keeps business people awake at night?

The answer is the double risks of cyber attack and fraud. Increasingly, the two are linked as fraud moves online. We asked our survey group of more than 4,100 managers and senior executives in five countries to rate their concern over different types of risk and the potential impact they could have on the organisation in the coming year. Two-thirds (66%) put the cyber threat on a par with fraud at the top of the list.

As this report shows, for organisations in both the private and public sectors, there is now an evens chance of at least one cyber incident in any 12-month period. Just under half (45%) of respondents say they suffered a cyber attack in the past year. Of those organisations that were targeted, more than two-thirds (67%) suffered two or more attacks and just over one in five (21%) suffered four or more. A small number were targeted more than ten times in the year.

The pain in Spain

Spanish organisations have the dubious honour of topping the table of likely targets, with 57% reporting one or more attacks. Seven out of ten Spanish technology, media and telecoms firms (72%) and three-quarters (75%) of financial services and energy firms report an attack. It will be of some comfort that the average cost of an incident in Spain is lower than for the other four countries in our survey. (see *Wide cost range per incident* – page 7).

The Netherlands comes second in the table at 50%, with around two-thirds (65%) of Dutch financial services and energy firms reporting attacks. Worryingly, 8% of Dutch firms do not know whether they suffered an attack or not.

The US finishes fifth, with 38% of respondents reporting an incident. US government entities appear to be particular targets with more than half (53%) reporting an attack. Across the five countries, financial services, energy, telecoms and government organisations are clearly the most likely sectors to be targeted.

Hacking is number one threat

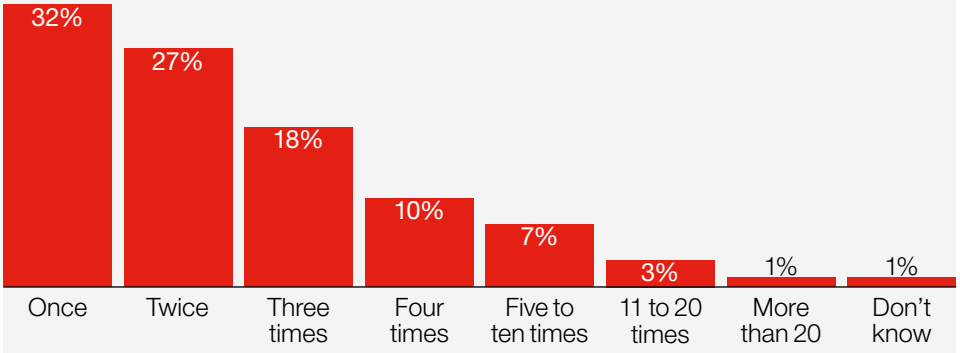
External attacks are the most common form of cyber incidents and the one most feared. They were experienced by 42% of those who suffered an incident and nearly half of respondents (45%) rank an 'external attack targeting our organisation' as having the most impact on business performance.

This year, the most frequently reported types of attack are virus/worm infestation, ransomware and DDOS (distributed denial of service, where multiple compromised systems, which are often infected with a Trojan, are used to target a single system) – mentioned by 21%, 12% and 10% of the full survey sample.

Spanish organisations are markedly more likely to report an incident of virus or worm infestation in the past year (30%). Internal incidents such as an insider threat, a configuration change or an HR incident, rank as the second most serious type of incident (mentioned by 16%) and the loss or theft of devices such as a laptop comes third (14%).

Frequency of cyber attacks

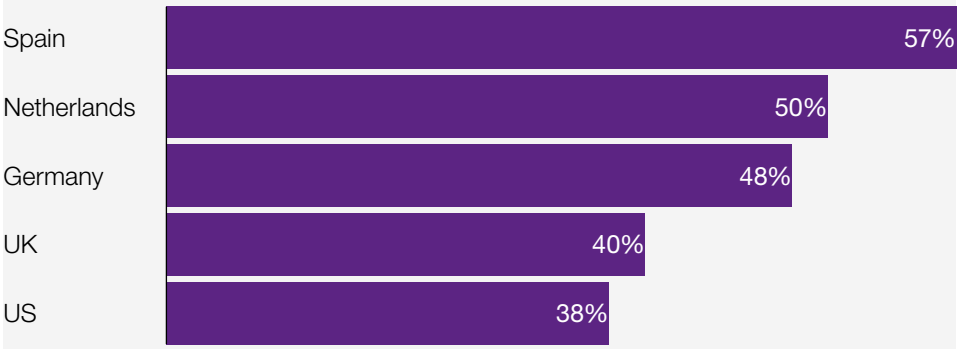
Of the 45% who have suffered an attack in the past 12 months



Survey conducted by Forrester Consulting on behalf of Hiscox.

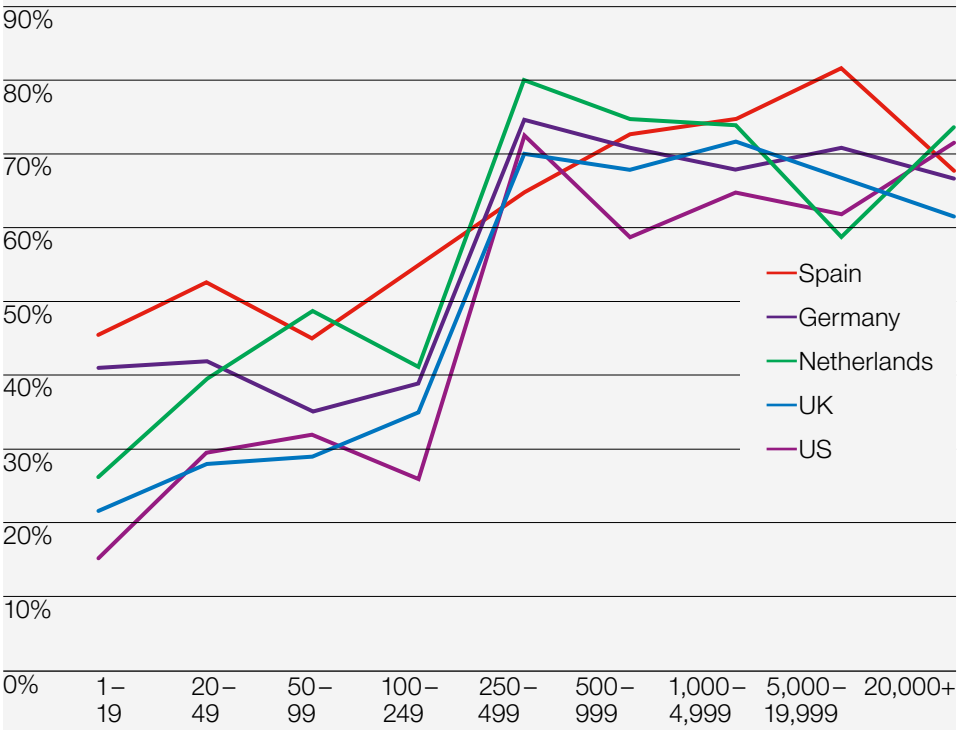
Cyber attacks by country

Percentage of respondents targeted



Survey conducted by Forrester Consulting on behalf of Hiscox.

Bigger organisations more likely to be targeted
Proportion of organisations reporting attacks (by number of employees)



Survey conducted by Forrester Consulting on behalf of Hiscox.

Bigger organisations targeted

It is the larger firms in the study that appear to be the hackers' favourite targets – not surprisingly, perhaps, as there are richer pickings to be found. As the chart (right) shows, the proportion of respondents reporting one or more attacks in the past year rises sharply for organisations with 250 employees or more.

Counting the financial cost

Cyber crime is costly for the victims. We asked those organisations that had suffered an attack (1,853 out of the 4,100 survey sample) to estimate the financial cost of all the cyber security incidents they had experienced in the past 12 months. Nearly a third of them replied 'don't know'. The average among the remainder was $229,000.

The averages mask some wide variations. For smaller organisations, average costs ranged between $22,000 in Spain and $55,000 in Germany. For larger ones the average costs ranged between $259,000 in Spain and $579,000 in the US. For the very largest organisations (with 1,000-plus people) the range was between $356,000 (in Spain) and $1 million (in the US).

However, some organisations suffered much higher costs: up to $25 million in the US and $20 million in Germany and the UK.

At the top end of the scale – among the very large entities – it is US organisations that are paying the highest price. The $1 million average cost of cyber incidents in the past year for firms with 1,000-plus employees is almost exactly twice the average for the other four countries. At the bottom end, among firms with up to 250 employees, it is German organisations that report the highest average cost of cyber crime, at $55,000.

Wide cost range per incident

We also asked organisations to estimate the cost of their single largest incident. The responses reveal a wide range of experiences. German organisations report the highest average figures in each size bracket and the highest cost for any single incident – at $5 million. By contrast, Spanish organisations managed to contain the cost per incident better than the rest.

Cost of all cyber security incidents
Average estimated cost of all of an organisation's incidents in the past 12 months

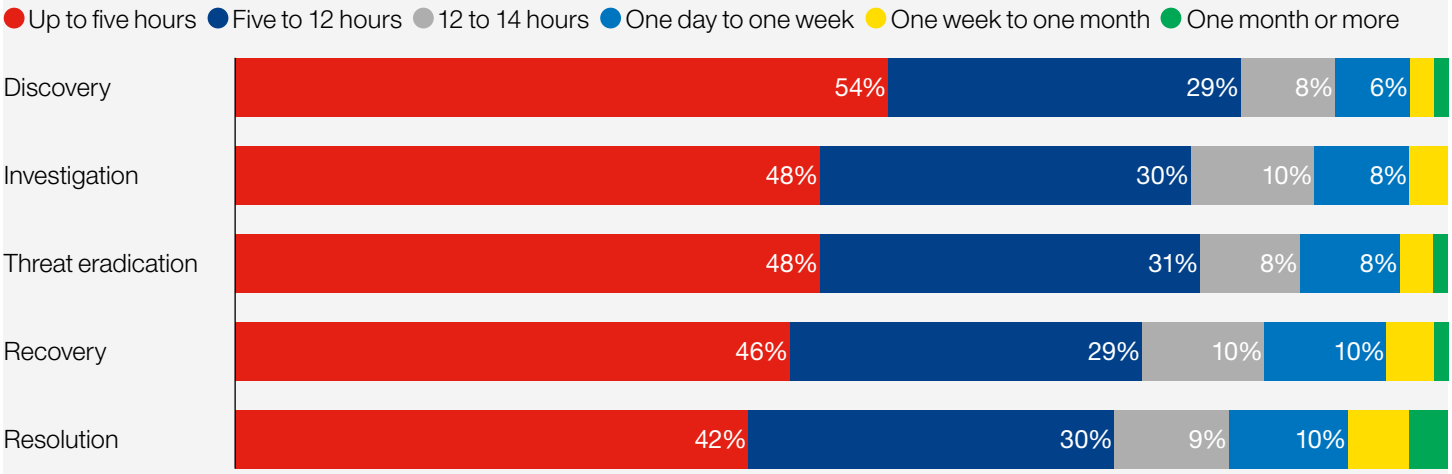
	249 or fewer employees	250 or more employees	1,000 or more employees	Overall range
Germany	$55,067	$406,653	$640,408	$500 – $20m
Netherlands	$32,760	$280,784	$531,158	$1,000 – $10m
Spain	$22,175	$259,230	$355,761	$500 – $5m
UK	$33,787	$462,633	$554,596	$1,000 – $20m
US	$34,604	$578,762	$1,047,465	$350 – $25m

Cost of largest cyber security incident
Average estimated cost of an organisation's largest incident in the past 12 months

	249 or fewer employees	250 or more employees	1,000 or more employees	Overall range
Germany	$11,918	$86,834	$150,891	$10 – $5m
Netherlands	$4,489	$66,767	$127,417	$10 – $2.5m
Spain	$3,789	$31,359	$41,733	$20 – $800,000
UK	$4,063	$56,870	$65,668	$10 – $1.2m
US	$4,883	$60,258	$106,583	$20 – $2m

In March 2016, the Petya virus encrypted the hard drive of thousands of computers worldwide and demanded payment in order to decrypt them. NotPetya emerged in June 2017. Initially viewed as a related, but faster-spreading, piece of ransomware, it damaged data beyond repair. It is now seen as a piece of state-sponsored malware designed to disrupt.

Time taken to return to business as usual after largest incident



Survey conducted by Forrester Consulting on behalf of Hiscox.

Assessing the broader impact

For a small number of those hit by a breach, the impact went beyond the immediate cost in dollars and cents.

Seven percent said they had lost customers as a result of a cyber attack and 5% said they had found it more difficult to attract new ones. A similar number said they had lost business partners. In 6% of cases the organisation had laid off employees.

Most difficult to quantify is the long-term impact on an organisation's reputation and standing. Some 5% of those hit by a cyber attack in the past year said the bad publicity had damaged the brand.

Multi-speed recovery

The amount of time taken to return to 'business as usual' varies widely. Analysing the biggest single incident of the past 12 months, we asked firms to estimate how long it took to manage each stage of the process – from discovery to resolution.

Around half of respondents (see above) required less than 15 hours to move from discovery through investigation to eradication of the threat. Almost as many managed to move from recovery to resolution (defined as using feedback from the incident to strengthen protocols and address legal, regulatory or other implications) in ten hours or less.

However, for a significant minority, the five-stage process took much longer. Resolving the issue is clearly the most demanding element of the process. US firms were most likely to take longer over the resolution stage – 24% took between one day and a month or more.

About this year's report

The study group for this year's Cyber Readiness Report has been materially expanded. It now includes approximately 1,000 managers and executives from Spain and The Netherlands, bringing the number of countries involved to five and increasing the number of respondents to approximately 4,100.

It has also been expanded to include non-profit and governmental organisations (making up 5% of total respondents in each case). The proportion of multinationals has been reduced from 32% to 20% and the proportion of local organisations, defined as those with operations in a single country only, lifted from 44% to 56%.

The span of job functions and responsibilities has also been broadened. C-level executives now account for 14% of respondents compared with 20% last year. The numbers who work in the organisation's IT department are down from 40% to 23%.

As with the 2017 report, all respondents have some responsibility for their organisation's cyber security decision-making – either as final arbiter, as part of the team that makes the decisions or as an influencer.

As a result of these changes, year-on-year comparisons with last year's findings have been kept to a minimum in this year's report.

The Hiscox view

The large number of organisations that have been targeted on multiple occasions in the past year gives some indication of the scale of the cyber threat. The figures here show the direct costs of cyber crime. More difficult to calculate is the extent to which this drains people and resources that could more profitably be deployed elsewhere. Fighting the cyber battle raises the costs of doing business for all concerned.

Cyber readiness model
There is room for improvement

More than half of the organisations in our survey (57%) this year claim to be 'very confident' in their cyber security readiness. But are they right to be? Have they really covered all the bases? Or are they victims of wishful thinking?

To get a true picture we asked a series of questions to assess respondents' cyber strategy and the quality of their execution. The strategy element was broken down into oversight on the one hand and resourcing on the other.

The execution part was divided into processes and technology. Scoring reflected the degree to which respondents' answers showed alignment with best practice. Each answer was marked out of five (see *Cyber readiness model methodology* – page 11)

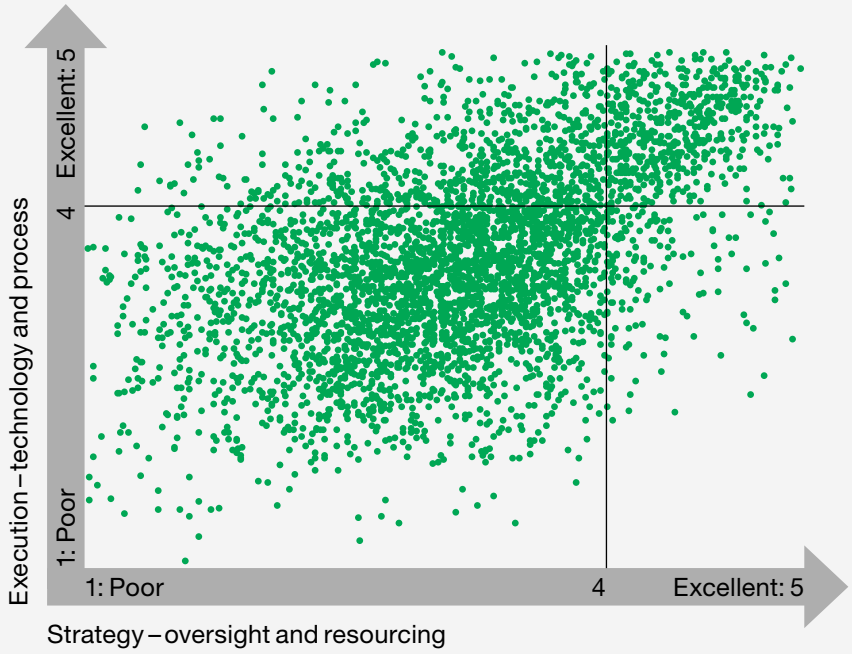
Taking those scores, each organisation was then ranked on a scale from 'cyber novice' to 'cyber expert' to establish a cyber readiness model. To achieve expert status, an organisation had to achieve an overall score of 4.0 or better in both strategy and execution. In between the novices and the experts were a substantial number of organisations that scored 4.0 on either strategy or execution – but not both. These are the 'cyber intermediates'.

Experts in the minority

The results are not reassuring. In both strategy and execution, the averages are substantially down on last year – though given the changes in the survey sample (see page 9) the two years' figures are not directly comparable. The average score in the strategy section is down from 3.65 to 3.32. In execution it is down from 3.78 to 3.49.

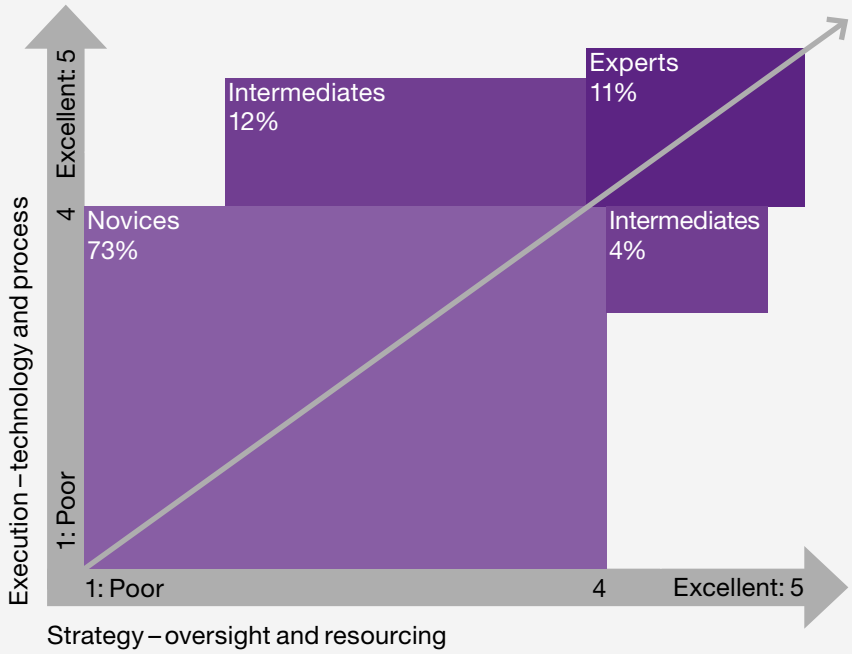
The scatter chart (above right) shows the distribution of the survey sample between novices (bottom left), experts (top right) and intermediates – either those that have scored highly in processes and technology (top left) or oversight and resourcing (bottom right), but not both. The key message is that nearly three-quarters (73%) of respondents rank as cyber novices, while just 11% rank as cyber experts.

Cyber readiness scatter



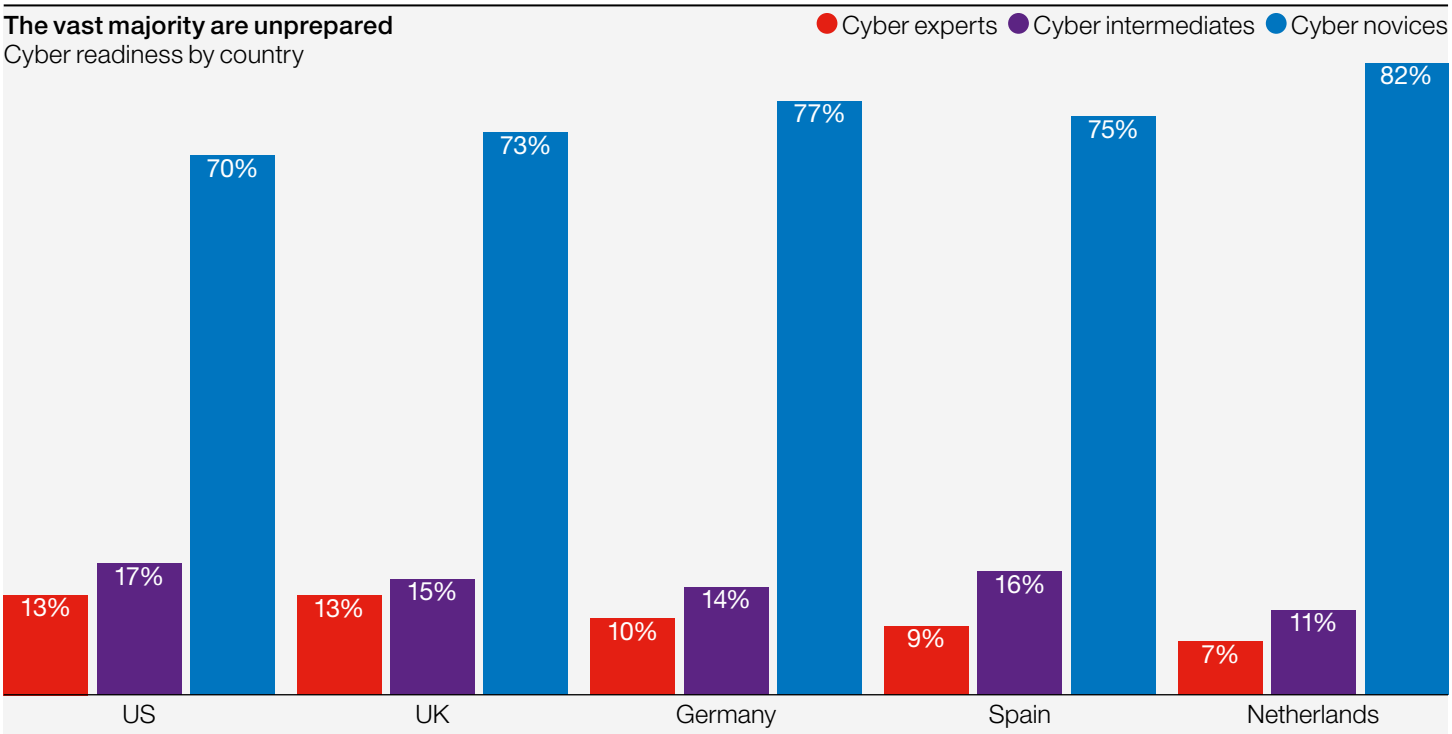
Survey conducted by Forrester Consulting on behalf of Hiscox.

Cyber readiness model



Survey conducted by Forrester Consulting on behalf of Hiscox.

The vast majority are unprepared
Cyber readiness by country



Survey conducted by Forrester Consulting on behalf of Hiscox.

Often, this is not because of under-investment in technology. As last year, this is the area where respondents have racked up the highest scores. The implication is that many organisations see the cyber threat as primarily a technology one, and are failing to support their investment in security technology with a formal strategy, sufficient resourcing and training, and sound processes.

Larger firms show the way

Not surprisingly, larger organisations are more likely to populate the top right hand corner – the cyber experts.

This may not just be a matter of resources given that, as we have seen, larger firms are more likely to be targeted. More than one in five organisations with 250 or more employees (21%) makes it into the expert category, and a further 17% rank as intermediates on one axis or the other. Multinational organisations make up a third of all the experts. Given the difference in cyber budgets, between the larger organisations in our survey sample and the smaller ones, that is to be expected.

What is more surprising is that there is little difference between the mid-sized organisations (defined here as 50 to 249 employees) and the very smallest (49 or fewer). A similar number – 7% – rank as cyber experts in each grouping, though there are slightly more cyber novices among the very smallest (79% versus 77%).

US and UK more cyber-ready

US firms emerge as the most cyber-savvy, followed closely by their UK counterparts (see chart above). While Spain comes fourth in the table, it actually boasts the second-highest number of cyber intermediates. Dutch organisations lag by some margin.

There are also wide disparities between sectors. The technology, media and telecoms sector accounts for 14% of the survey sample but provides nearly one-in-five cyber experts (19%). Manufacturing, financial services and retail/wholesale also punch above their weight as cyber experts. At the other end of the scale, professional services firms clearly have some catching-up to do. They account for 8% of the survey sample but only 4% of cyber experts.

You get what you pay for

The gulf in cyber readiness between the cyber novices and the cyber experts is mirrored in their expenditure on IT and the proportion of it they devote to cyber security (see table below). The implication of the figures is that the average cyber expert spends $2.5 million a year on cyber defence compared with $980,000 for the average cyber novice. In other words, you get what you pay for.

Just as the bigger organisations in our report make up a disproportionately large number of the cyber experts, so

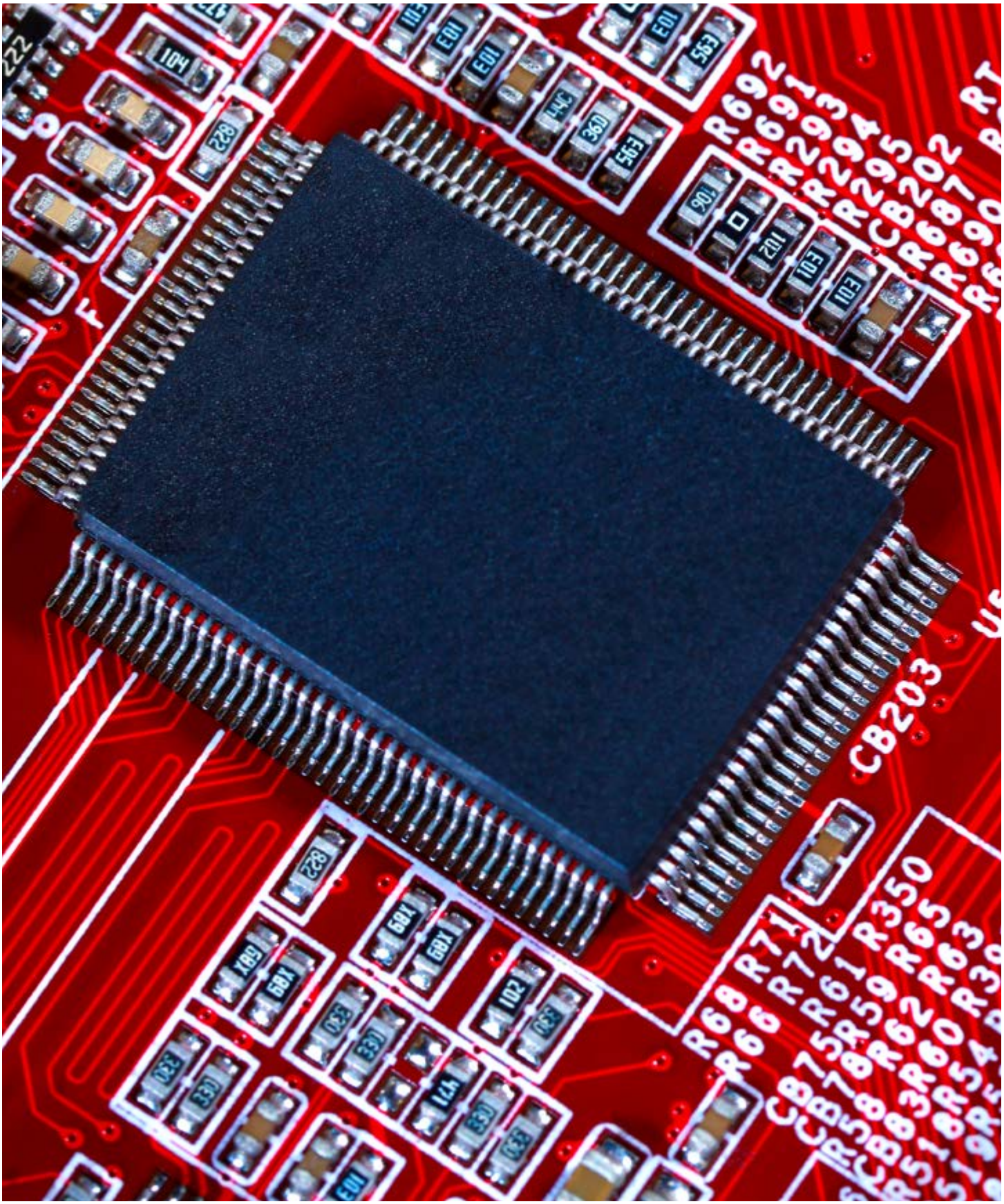
Cyber readiness model methodology

Respondents were shown a series of statements relating to cyber security strategy and execution. Each statement represents best practice in its area.

The strategy statements were broken down into two sections – oversight and resourcing. Two examples: 'Cyber security has a formal budgeting process which is integrated into all security projects and activities' and 'Cyber security competencies are regularly reviewed using established metrics according to roles and responsibilities'.

The execution statements were similarly split between processes and technology. They included: 'Security incident and event data from key servers and devices is automatically aggregated and analysed' and 'Strong authentication is integrated throughout the environment'.

Respondents were asked to indicate the extent to which each statement described their organisation's current approach. They were given a range of options from 'doesn't describe our approach at all' (which scored one) to 'exactly describes our approach' (scoring five).



Between May and July 2017, Equifax, the US credit monitoring agency, suffered a data breach that involved the theft of personal data relating to 143 million US consumers. A further 400,000 UK residents were also affected.

so the amount they spend on cyber defence dwarfs the sums spent by their smaller counterparts – not only in nominal terms but as a percentage of their overall IT budgets. While organisations with 250 people or more devote an average 12.2% of their IT budget to cyber, those with 249 or fewer devote just 9.8%.

The difference in monetary terms is enormous. The IT budget for the average larger organisation in our sample is $34.4 million, which implies spending on cyber of $4.2 million. The average IT budget of the smaller organisations is $1.3 million, implying cyber spending of just $127,000. Many firms spend more. 37% of the total survey sample spend between 11% and 25% of their IT budget on cyber security.

Financial services firms top the list of sectors for the largest spenders on cyber security, devoting an average of 11.7% of their IT budgets to this area. They are followed by the pharmaceutical and healthcare sector, at 11.3%. Government entities, led by those in Germany and Spain, are close behind.

The bad news is that the cyber experts are just as likely to report a cyber incident in the past 12 months as the cyber intermediates and the cyber novices. In fact they are substantially more likely to have experienced multiple incidents – five or more. This is not so surprising given the preponderance of larger organisations among the cyber experts (they are more tempting targets).

It is nonetheless a potent reminder that nothing buys immunity in the online world.

The Hiscox view

For smaller firms that lack the expertise for managing or fixing a breach, outsourcing can be an alternative approach. Even bigger organisations often lack the ability to field an instant response team around the clock. Outsourcing firms can add an extra layer of expertise in handling breaches however they are at best a delegation of responsibility not a complete abdication of cyber security.

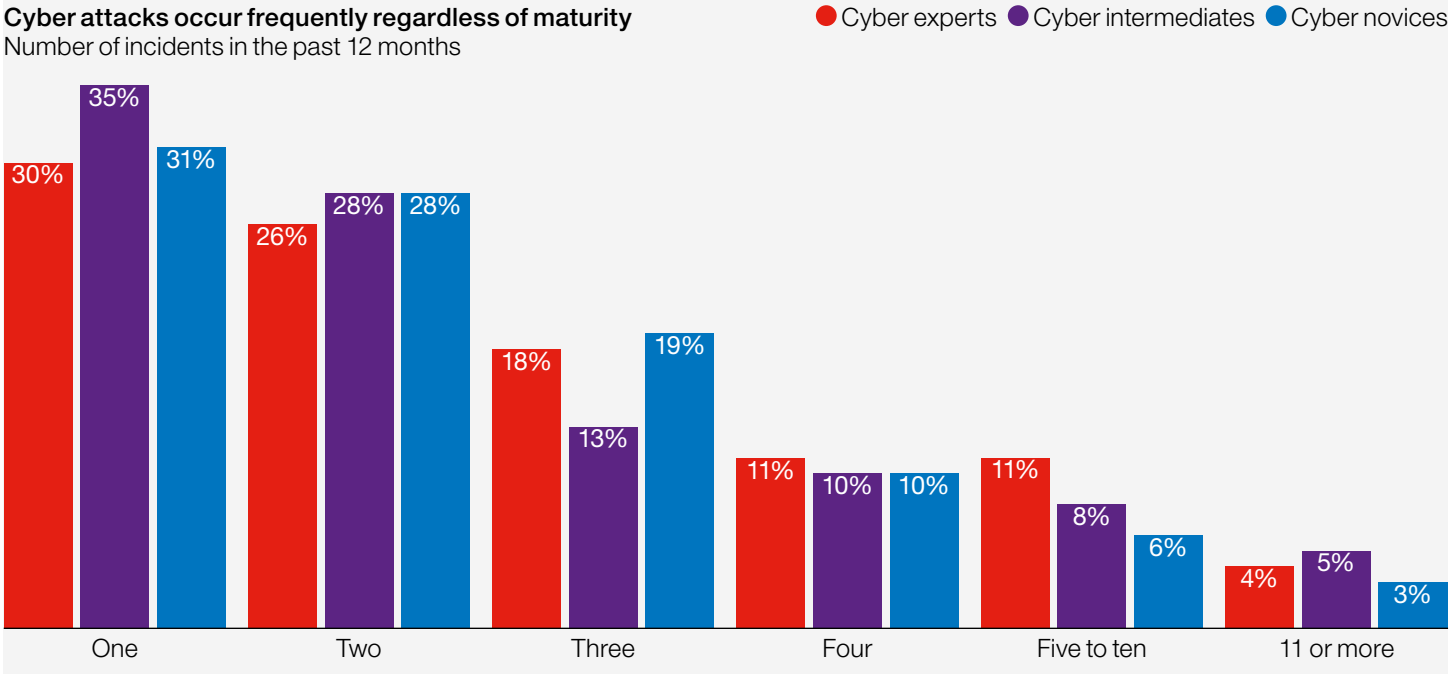
IT and cyber security budgets
By country

	Average IT budget	% devoted to cyber
UK	$13.14m	10.5%
US	$11.65m	10.6%
Spain	$10.62m	11%
Germany	$10.45m	10.4%
Netherlands	$8.35m	10%

IT and cyber security budgets
By level of expertise

	Average IT budget	% devoted to cyber
Cyber novice	$9.9m	9.9%
Cyber intermediate	$11.3m	11.4%
Cyber expert	$19.8m	12.6%

Cyber attacks occur frequently regardless of maturity
Number of incidents in the past 12 months



Survey conducted by Forrester Consulting on behalf of Hiscox.

Measuring the response
A mixture of cash and change

Significant numbers of firms are responding to the intensifying cyber challenge in two ways: by upping their game and lifting their spending.

We asked all organisations to list their top security priorities for the coming year, giving them a long list of options from which to choose. The chart on page 15 (top) highlights the top ten initiatives and the percentage of respondents who selected them. It is as interesting for what does not make the top ten as what does.

Just outside the top ten is 'preparing for a cyber crisis', mentioned by 43% of respondents. 'Enhancing disaster recovery capabilities' comes a few places further down (mentioned by 42% of respondents). 'Simulating a cyber attack to test the firm's response' comes right at the bottom – mentioned by 35% of respondents.

What changes as a result of an attack?
We also asked those organisations that had suffered a cyber attack in the past 12 months what they had changed as a result. Remarkably, nearly half (47%) said 'nothing'. The remainder had made a number of changes. Increased spending on prevention and detection technologies heads the list – mentioned by 13% of respondents.

One in eight (12%) said they had introduced additional security and audit requirements and a similar number said security and/or privacy were now regularly evaluated. In 9% of cases, the breach had prompted the organisation to purchase or enhance a cyber insurance policy and the same number had increased spending on threat intelligence capabilities. Some 7% had switched their IT auditors.

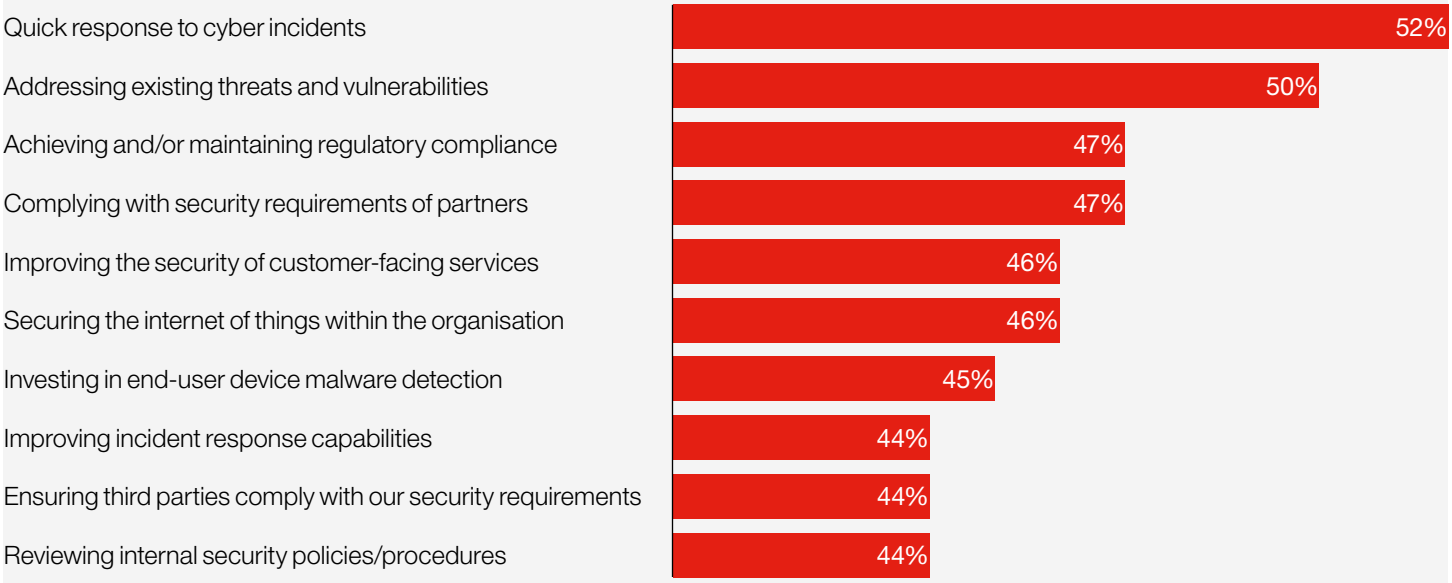
Spending rise led by the cyber experts
The majority of respondents (nearly three out of five – 59%) are increasing their cyber security budgets for the coming year. New security technology heads the list, with 57% of organisations increasing their spending here – despite the fact that this is the area in which our respondents are already best prepared (see *Cyber readiness model* – page 10).

Spanish firms are the most enthusiastic spenders on technology: 60% of them plan to lift spending in this area. A third of respondents (34%) intend to increase employee awareness training and more than a quarter (26%) will bring in more cyber security staff. But in both instances, rather more respondents are planning to cut spending (36% and 33% respectively). Similarly, a small number of respondents plan to reduce their security outsourcing budget.

In every area of spending, it is the cyber experts that are most likely to increase their budgets. One example: 55% of cyber experts plan to lift their spending on training compared with only 29% of cyber novices. Given that the cyber experts already devote a larger percentage of their IT budget to cyber security (see page 13), it would appear that the gap between them and the rest is set to widen rather than shrink in the year ahead.

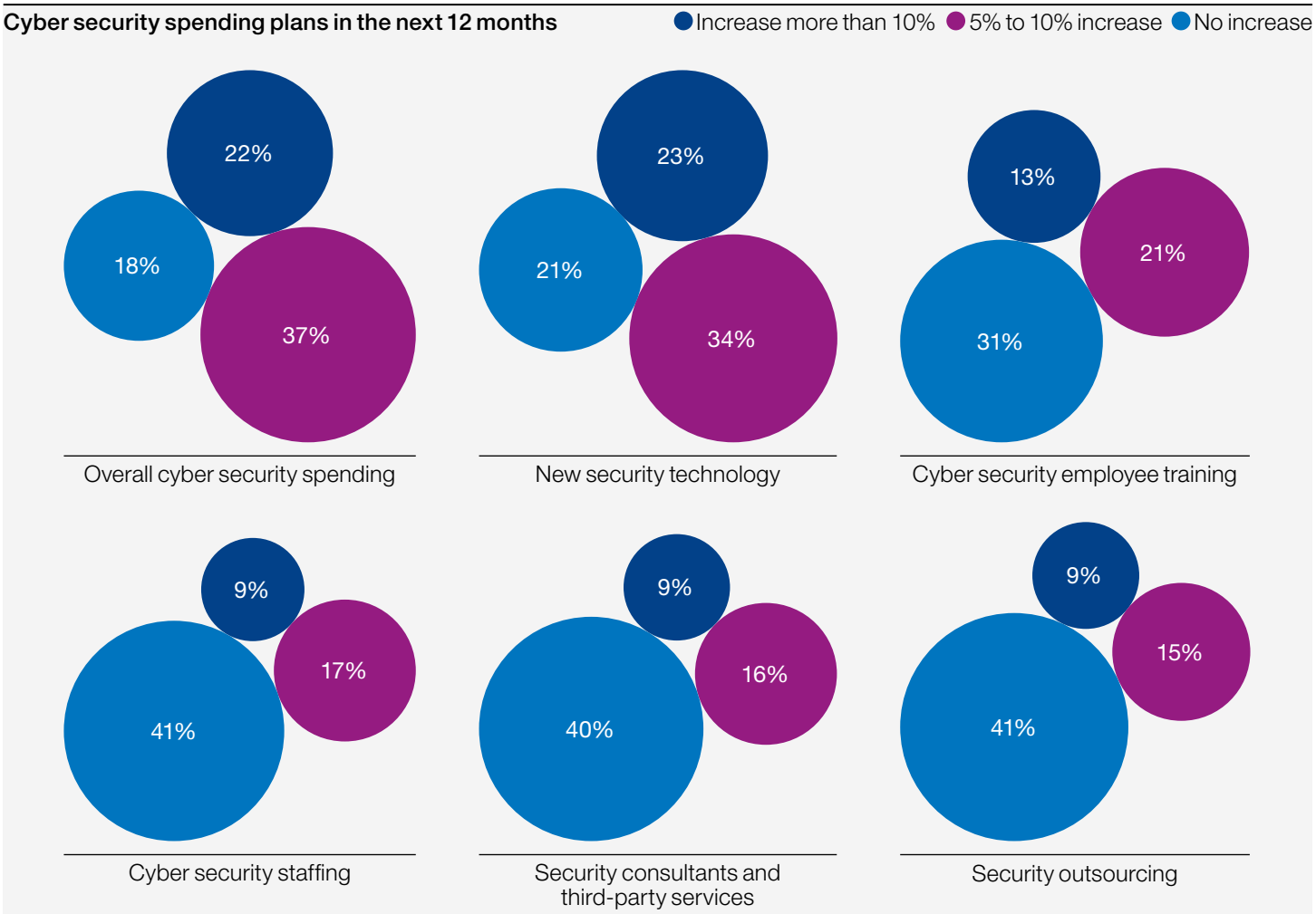
The Hiscox view
Spending on technology is often the easy part. To be effective, you have to move on all fronts together. That means people, processes and technology. Simply spending on technology is not enough without a fully structured, rigorous set of processes combined with people who are fully aware of the issues. It is especially disappointing that so few people appear to simulate a cyber attack and practise what to do when their systems go down.

Key security initiatives planned in the next 12 months
Percentage ranking the initiative a high priority



Survey conducted by Forrester Consulting on behalf of Hiscox.

Cyber security spending plans in the next 12 months



Survey conducted by Forrester Consulting on behalf of Hiscox.

What makes an expert?
Awareness, engagement, rigour...

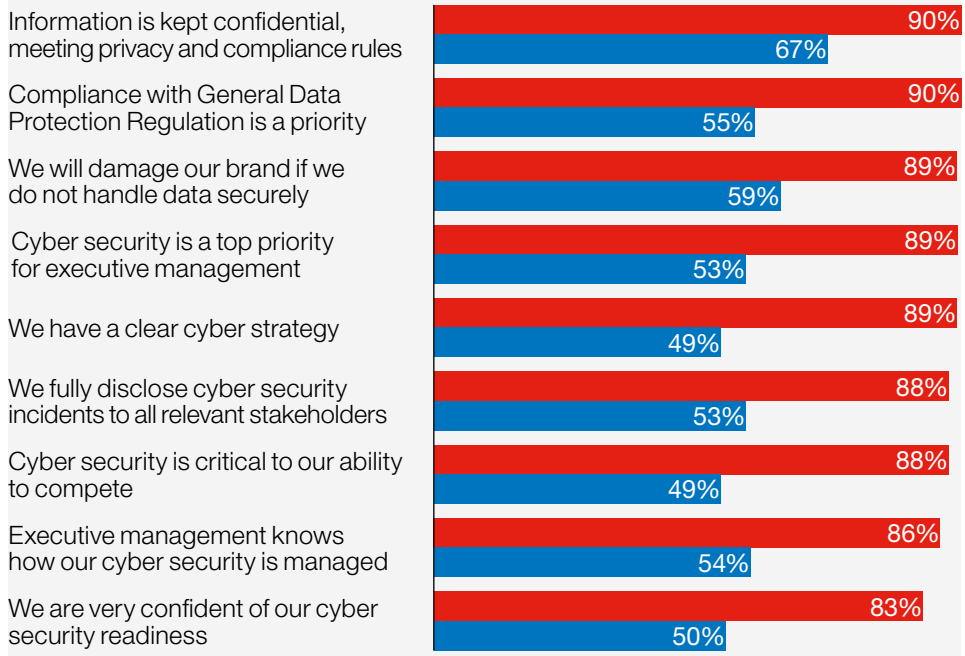
The cyber security experts in our report form a distinct minority. That should perhaps not surprise. For the purposes of our analysis, the bar was set deliberately high. As discussed in the previous section, organisations had to achieve a score of 4.0 or better (out of five) in all four metrics to qualify as cyber experts. But behind the quantitative analysis there is a range of behaviours that, taken together, helps to define what cyber security readiness looks like. So what divides the cyber experts from the cyber novices? Here are some key factors.

Awareness. Awareness of the cyber challenge is clearly a good starting point. To gauge their awareness, respondents were asked how strongly they agreed with a number of statements. They ranged from the fairly basic – 'We ensure information is kept confidential, available, and with integrity, meeting all necessary privacy and compliance rules' – to the more ambitious – 'We are very confident with our cyber security readiness'.

What is striking is the gulf between the responses of the cyber experts on the one hand and the cyber novices on the other. None of these statements can be considered contentious. Take for instance: 'We will damage our brand if we do not handle client and partner data securely'. It might be expected that those in business would take that as a given. But while nearly nine out of ten cyber experts (89%) agreed or strongly agreed with this statement, only 59% of cyber novices felt able to do the same. By contrast, there is strong buy-in to all the statements in the table from the great majority of cyber experts.

Strategy. Nine out of ten cyber experts (89%) have a clearly defined cyber security strategy – compared with less than half (49%) of cyber novices. Cyber experts are likely to have put in place a formal budgeting process, which is integrated into all security projects and activities. In nine out of ten cases (89%), the decision structures and processes are clearly defined. More than four out of five (83%) cyber experts identify the compliance requirements through a combination of active research, automated alerts and information from content providers.

Experts have a higher level of agreement
Those agreeing



Survey conducted by Forrester Consulting on behalf of Hiscox.

Engagement. Cyber experts get support from the top and engage a broader range of stakeholders when setting their organisation's cyber security strategy. Experts are more than twice as likely to agree that 'there is formal support for cyber security from business leaders and executives on an ongoing basis' (86% versus 38% for cyber novices). In addition, more than two-thirds (68%) of cyber experts involved the board and executive management in setting strategy, while only 52% of cyber novices did so.

By country, it is German organisations that are most likely to have board-level involvement in the strategy-setting process (64% of them). UK and US organisations are most likely to involve IT (57% each). US organisations lead in giving operations a say (25%).

Asked which of 11 different functions were involved in setting strategy, the cyber experts generally ticked off significantly more boxes than the cyber novices. Four-fifths (82%) of cyber experts engaged the IT department in the strategy-setting process, nearly twice the number of cyber novices who did the same (44%). There is a similar picture in operations (mentioned by 32% of cyber experts but only 15% of cyber novices) and e-commerce (22% of cyber experts but only 9% of cyber novices).

Organisation and professionalism. All but a few cyber experts have one or more roles dedicated to combating the cyber threat. Just over half (52%) have a dedicated leader or executive responsible for cyber security and just under half (46%) say they have a dedicated team to back that leader up. That is around twice the comparable numbers for cyber novices.

Just over four-fifths of cyber experts say they can clearly measure the business impact of incidents that disrupt their business. They also document and track cyber security centrally on an ongoing basis and around three quarters of them (76%) make cyber security data available to all stakeholders on a 'near real-time basis'.

The cyber experts are also more proactive. More than seven out of ten (72%) say they have conducted phishing experiments to understand employee behaviour and preparedness for attacks. The equivalent figure for cyber novices is 37%.

As might be expected, the cyber experts score high for their deployment of security technologies – ranging from antivirus/antispyware through to intrusion detection systems. But most combine that with a rigorous approach to authentication and they actively enforce message encryption policies. The best monitor and track the performance of spam blocking services and have systems in place to track violations and generate alerts.

Training and evaluation. All but a tiny proportion of the cyber experts (97%) incorporate security training and awareness throughout the workforce. Nine out of ten (90%) review the cyber security competence of their employees on a regular basis, using established metrics. And cyber security competence forms part of the regular performance evaluation. More than four-fifths of the cyber experts say 'increased employee training has reduced the number of incidents that disrupt our business'. The equivalent figure among the cyber novices is just 44%.

Willingness to respond. The cyber experts mark themselves apart from the cyber novices by their readiness to make changes in response to a cyber security incident. Nearly three-quarters (72%) of those that experienced an incident in the past year beefed up their security in one way or another – and only 28% of them sat on their hands. By contrast, more than half of those organisations classed as cyber novices (51%) failed to act.

Investment. The expert organisations devote a greater proportion of their IT budget to cyber than the novices – a mean 12.6% compared with 9.9% – and will go on doing so. As the chart below shows, far more of the experts intend to lift their spending in the coming 12 months – across every area from staffing, training and technology to outsourcing and consultancy.

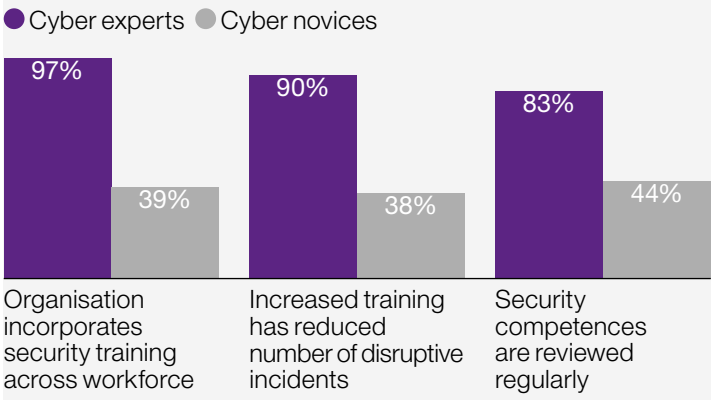
Insurance. 60% of the cyber experts in this study have taken out cyber insurance and a further 31% of them say they plan to do so. By contrast, barely a quarter (26%) of the cyber novices say they have cyber cover – though a further quarter (24%) plan to take out cover in the next 12 months. However, nearly half of the novices either say they have no plans to take out cyber insurance (44%) or say they are 'not sure what cyber insurance is' (5%). See: *Insurance: larger organisations lead the way* – page 18).

Disclosure. Nearly nine out of ten cyber experts say they fully disclose when a cyber security incident has occurred – both to internal and external stakeholders. By contrast, barely half of the novices feel able to say the same. Given that nearly three-quarters (73%) of respondents this year fall into the novice category, that means that around a third of all the 4,100 companies surveyed for this report have a questionable approach to disclosure.

The Hiscox view

It is striking that the majority of experts take on board the lessons of any incident and respond forcefully through stepping up their capabilities. That may involve spending but it can also mean improving internal processes. And, clearly, in a significant number of cases it involves the purchase of cyber insurance.

Experts are better at training and evaluation



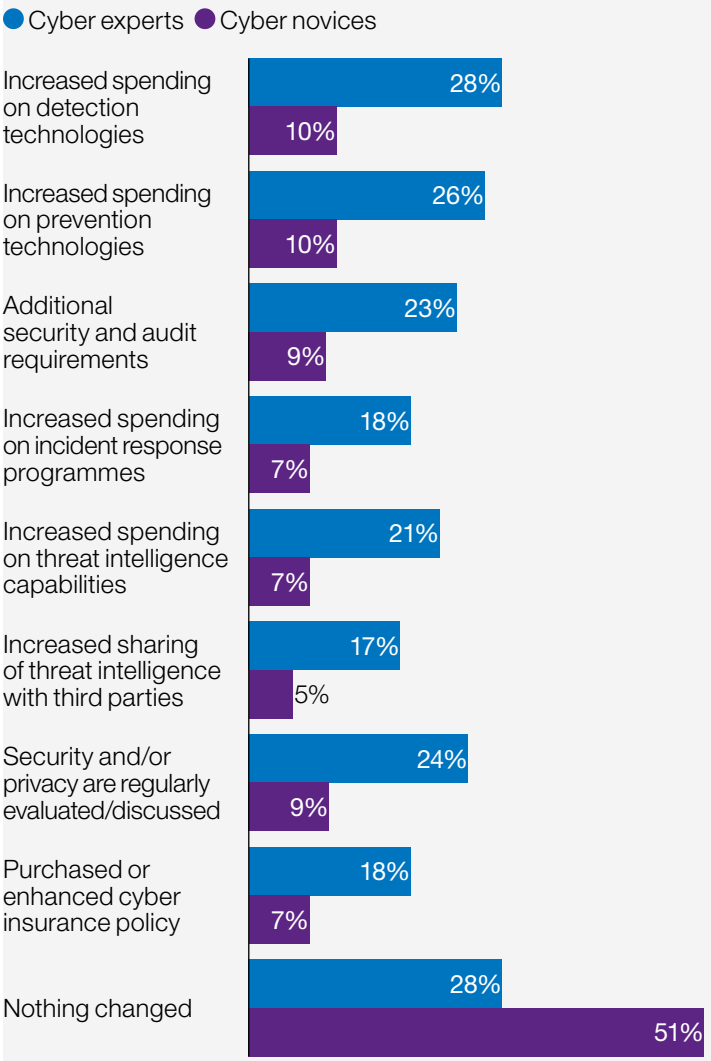
Survey conducted by Forrester Consulting on behalf of Hiscox.

Experts spend more than novices

Percentage planning to increase spending in next 12 months

Survey conducted by Forrester Consulting on behalf of Hiscox.

Experts are more likely to make changes after an incident



Survey conducted by Forrester Consulting on behalf of Hiscox.

Insurance
Larger organisations lead the way

One of the defining characteristics of the cyber experts identified in this report is their take-up of standalone cyber insurance. Three out of five (60%) cyber experts say they have cyber cover and a further 31% say they plan to take out cover in the coming 12 months. For comparison, across the full survey sample, one-third of respondents (33%) say they have standalone cyber cover while a quarter (25%) say they intend to adopt it in the coming year.

The report shows that smaller companies still have some way to go to catch up with their bigger counterparts. More than half (57%) of organisations with 250 employees or more say they have cyber insurance – and for the very biggest organisations with 20,000-plus people, the figure is higher still, at 64%. Among organisations with fewer than 250 employees, the proportion drops to under a quarter (23%).

There is a sharp divide between big and small among those who say they have no plans to adopt cyber insurance. More than half (52%) of US smaller businesses say they have no intention of taking out cyber cover. That contrasts with just 9% of larger US organisations. Smaller firms in Germany and The Netherlands also appear quite resistant to cyber insurance – with 50% and 49% of them respectively saying they have no plans to take out cover.

Financial services firms are the most likely to have cyber insurance cover. Just under half (48%) say they have a standalone cyber policy. At the other end of the spectrum, nearly half of food and drink organisations (46%) and 43% of professional services firms say they have no plans to take out cyber cover.

Waiting on the GDPR

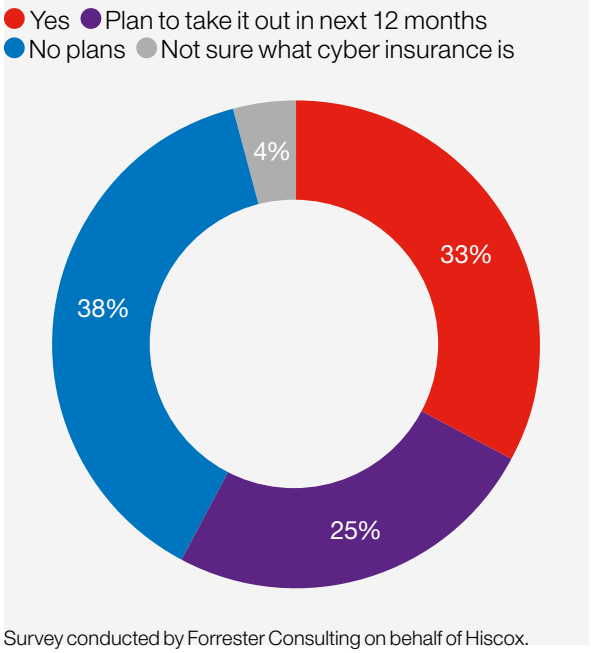
The big question is whether cyber insurance take-up in Europe will get a boost this year in the shape of the EU's General Data Protection Regulation (GDPR).

The US market has been helped by the progressive introduction of mandatory breach notification. From May this year, any organisation operating in Europe will be subject to the GDPR, the first significant overhaul in data protection across most of Europe for 15 years.

GDPR not only makes breach notification mandatory but lifts the ceiling for fines for breaches to penal levels – potentially €20 million or 4% of an organisation's worldwide turnover. This could be a watershed moment. The GDPR has a catch-all element to it; even if an organisation is not domiciled in Europe, it will be covered by the legislation if it has any kind of operation there.

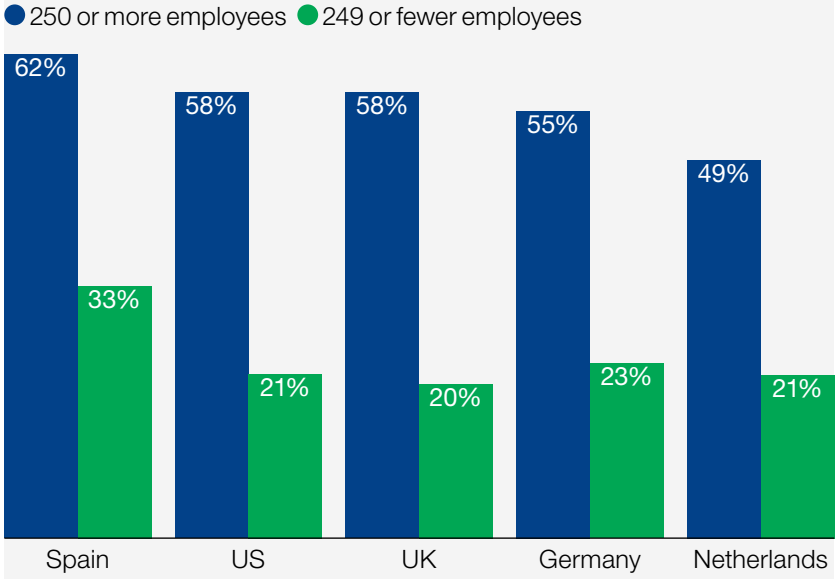
While most organisations in this report appear to have taken the GDPR's wide-ranging impact on board, a significant number have not. Overall, 62% of respondents say 'ensuring compliance with GDPR is a top priority', yet that leaves 38% for whom it is not

Do you currently have cyber insurance?



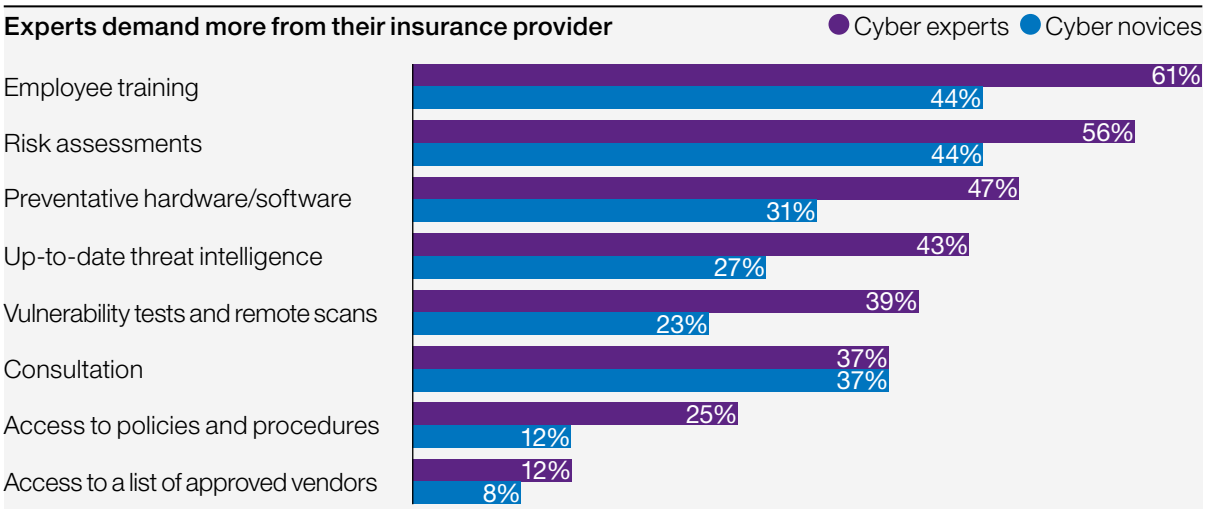
Survey conducted by Forrester Consulting on behalf of Hiscox.

Cyber insurance by organisation size
Percentage covered



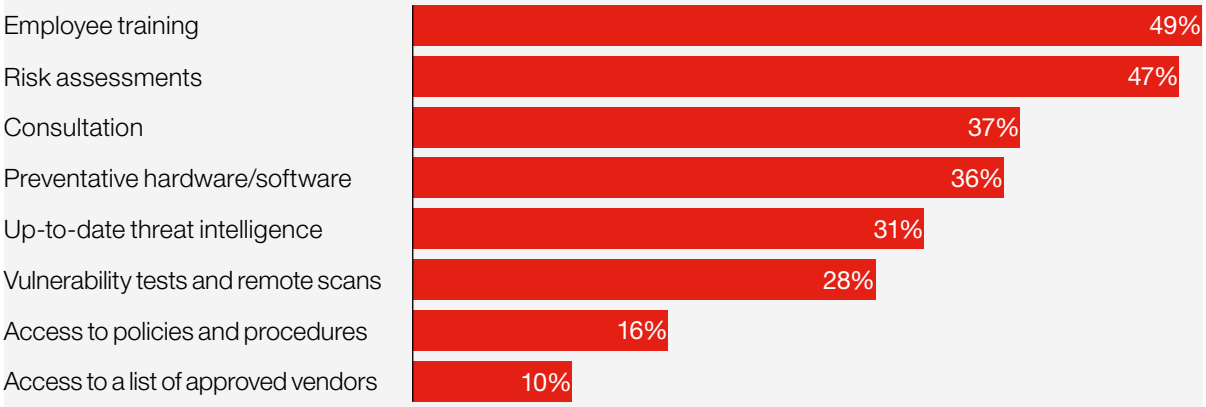
Survey conducted by Forrester Consulting on behalf of Hiscox.

Experts demand more from their insurance provider



Survey conducted by Forrester Consulting on behalf of Hiscox.

Additional services sought from insurer



Survey conducted by Forrester Consulting on behalf of Hiscox.

a pressing issue. The figure among cyber experts is 90%. Interestingly, 60% of US respondents also see compliance as a priority – suggesting the measure's extra-territorial implications are recognised.

Among those already covered or planning to take out cover, the top two reasons for doing so are the cost of a potential breach/the desire for peace of mind and the fact that cyber insurance policies offer 'additional expertise that I do not have'. More than a third (34%) cite the attraction of additional expertise as a reason for taking out cover.

And what reasons do respondents give for not taking out cover? Some 46% say 'cyber insurance is not relevant for me' while 27% think it is 'too expensive'. Nearly one in five (19%) says cyber policies are 'so complicated, I don't understand what the insurance would cover me for'. The results suggest the insurance industry still has some work to do.

Interestingly, C-level executives appear more resistant to the idea of cyber insurance than those they manage. Only 28% say they have taken out cyber cover and 44% say they have no plans to do so.

Additional services a big attraction

The opportunity to draw on additional services is clearly one of the attractions of insurance. Nearly half (49%) of those with cover or planning to take out cover say they either use or are planning to use the insurer's employee training. Nearly half (47%) will turn to their insurer for risk assessments. The ability to get consultative advice is also mentioned by 37% of respondents.

Once again, it is the cyber experts who appear the most conscious of what is on offer. They expect much more from their insurer. Training, risk assessments and preventative hardware and software top the list of services.

Confusion still reigns

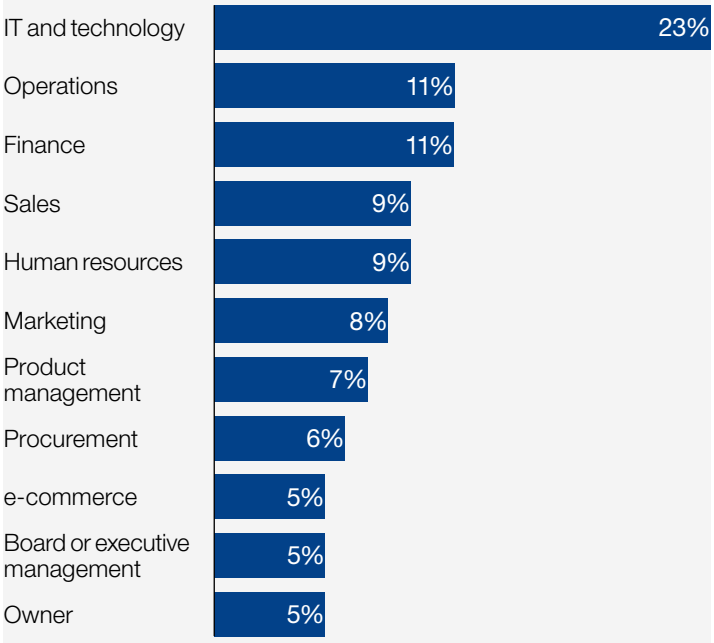
Large numbers of respondents believe their general business insurance policy covers them for various cyber incidents. For example, nearly two-thirds (64%) of all respondents think it covers them in whole or in part for a data breach resulting in loss of customer data and 57% think it covers them for DDOS (distributed denial of service).

The Hiscox view

The figures for those either insured already or planning to take out cyber cover look high. But there is no doubt this is one of the fastest-growing areas of the insurance market. We are seeing penetration spread rapidly from the US to the UK and mainland Europe, and from larger customers to smaller ones.

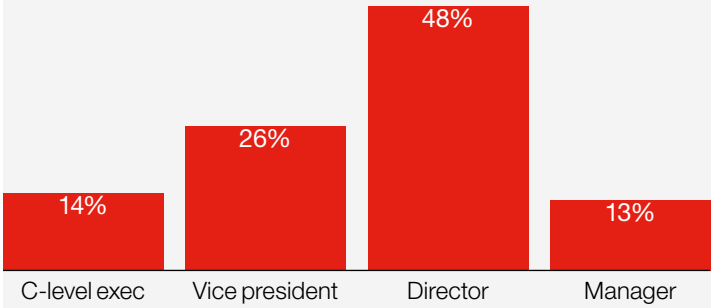
Research methodology

Departments in which respondents work



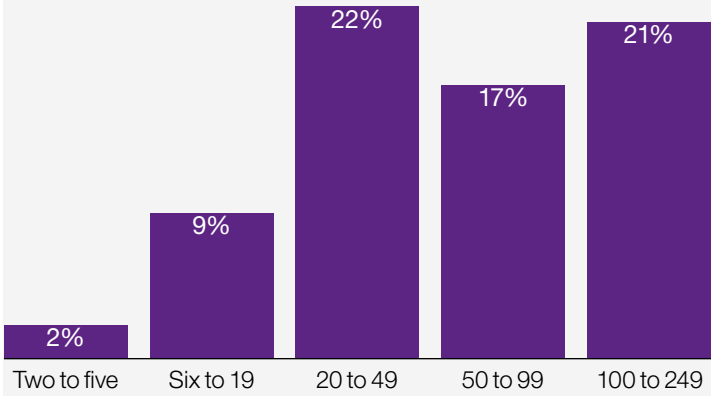
Hiscox commissioned Forrester Consulting to assess organisations' cyber readiness. In total 4,103 professionals responsible for their organisation's cyber security strategy were contacted (1,000 plus each from the UK, US and Germany, and 500 each from Spain and The Netherlands). Seventy percent of respondents were from organisations with fewer than 250 employees (small firms), and the remaining 30% from organisations with 250 or more employees (large firms). Respondents completed the online survey between 12 October and 10 November 2017.

Respondent level

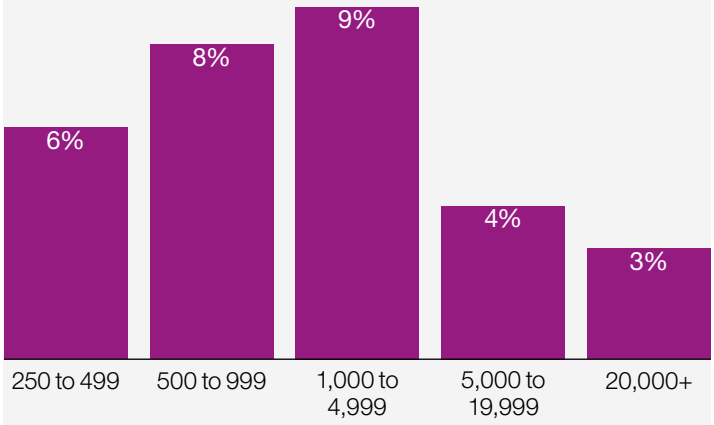


Size of business

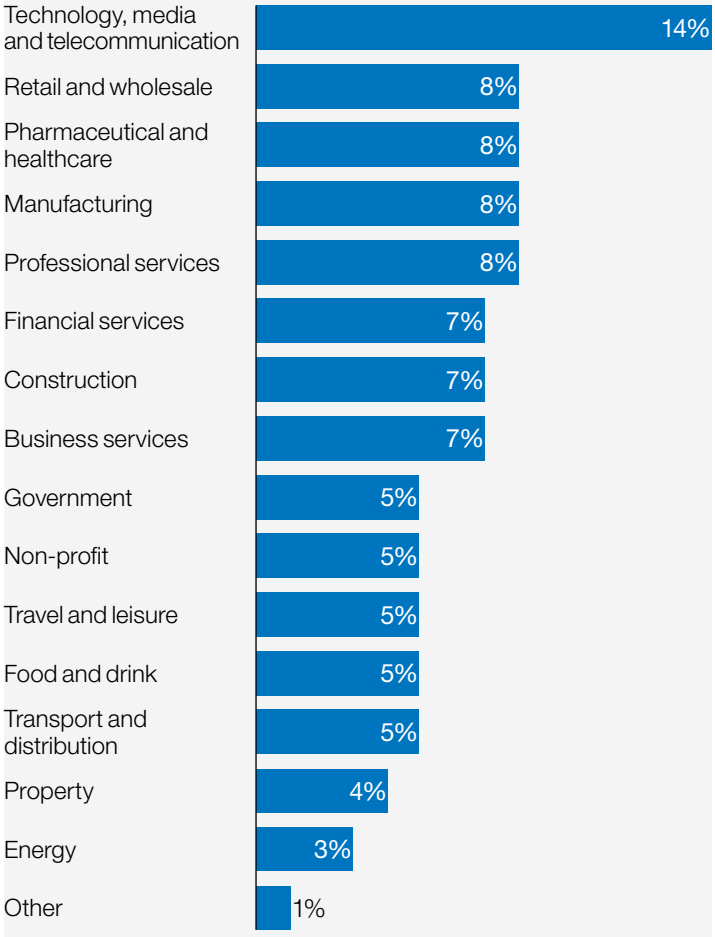
Fewer than 250 employees (70% of total)



More than 250 employees (30% of total)



Sector



Hiscox, the international specialist insurer, is headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). There are three main underwriting divisions in the Group – Hiscox Retail (which includes Hiscox UK & Europe, Hiscox Guernsey, Hiscox USA and subsidiary brand, DirectAsia), Hiscox London Market and Hiscox Re & ILS. Through its retail businesses in the UK, Europe and the US, Hiscox offers a range of specialist insurance for professionals and business customers, as well as homeowners. Hiscox underwrites internationally traded, bigger ticket business and reinsurance through Hiscox London Market and Hiscox Re & ILS. For more information please visit www.hiscoxgroup.com.

Report design by somethingbrighter.com

Hiscox Ltd

4th Floor
Wessex House
45 Reid Street
Hamilton HM 12
Bermuda

T +44 (0)20 7448 6000
E enquiries@hiscox.com
hiscoxgroup.com

18423 02/18