HISCOX

Hiscox Cyber Readiness Report 2019

Hiscox is a global specialist insurer, headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). Our ambition is to be a respected specialist insurer with a diverse portfolio by product and geography. Through the retail businesses in the UK, Europe, Asia and the USA, we offer a range of specialist insurance for professionals and business customers as well as homeowners. Internationally traded, bigger ticket business and reinsurance is underwritten through Hiscox London Market and Hiscox Re & ILS. Our values define our business, with a focus on people, quality, courage and excellence in execution. We pride ourselves on being true to our word and our award-winning claims service is testament to that. For more information, visit www.hiscoxgroup.com.

Rising to the cyber challenge

Our third Hiscox Cyber Readiness Report provides you with an up-to-the-minute picture of the cyber readiness of organisations, as well as a blueprint for best practice in the fight to counter the ever-evolving cyber threat.

Gareth Wharton
Cyber CEO, Hiscox

The number of firms reporting cyber incidents has risen from 45% last year to 61% in 2019.

Barely a week goes by without news of a major cyber incident being reported, and the stakes have never been higher. Data theft has become commonplace; the scale of ransom demands has risen steadily; and cumulatively the environment in which businesses must operate is increasingly hostile. The cyber threat has become the unavoidable cost of doing business today.

This is our third Hiscox Cyber Readiness Report and, for the first time, a significant majority of firms surveyed said they experienced one or more cyber attacks in the last 12 months. Both the cost and frequency of attacks have increased markedly compared with a year ago, and where hackers formerly focused mainly on larger companies, small-and-medium-sized firms are now equally vulnerable.

Regulation is going some way to improving awareness and mandating a baseline of cyber security rigour. In 2018, we saw the introduction of the EU's General Data Protection Regulation (GDPR), to which businesses have adapted, and a by-product of this has been an uptick in demand for cyber insurance. In the pages that follow, we see that more firms are taking a structured approach to the problem, with a defined role for managing cyber strategy, and we can also see more appetite to transfer some or all of the risk to an insurer by way of a standalone cyber insurance policy.

The old adage 'prevention is better than cure' springs to mind, and being aware of these threats is half the battle. From our experience as a cyber insurer, business email accounts being compromised is currently the main cause of cyber claims, followed by ransomware.

We launched our online training platform, the CyberClear Academy, a year ago in a bid to better equip our customers against these perils and already more than 2,500 companies have benefited from it. We don't rest on our laurels though, and will continue to develop other preventative measures that protect our customers and what matters to them.

The cyber risk may mutate rapidly, but progress in mitigating and managing it is also evolving. I hope this report will go some way to helping promote a better understanding of the issues and encourage the adoption of rigorous and effective measures to minimise the cyber threat.

Executive summary

Cyber readiness levels stall as attacks reach a new intensity in terms of both frequency and cost.

Key findings

Reasons for optimism despite stalling readiness scores.

More firms fail the cyber readiness test

Our quantitative model of cyber readiness shows a small decline this year in the proportion of firms achieving 'expert' scores for their cyber strategy and execution – down from 11% to 10%.

Two factors account for the fall in readiness scores

The first-time inclusion of French firms has reduced overall scores. There has also been a drop in the number of large (with 250 to 999 employees) and enterprise firms (1,000 plus) in the USA and Germany that achieve top scores.

Cyber attacks reach a new intensity

More than three out of five firms (61%) reported an attack in the last year – up from 45% the previous year. The frequency of attacks has also increased. Among the seven countries, Belgian firms are the most likely to have been attacked, US firms the least likely.

Cyber losses soar

The mean figure for losses associated with all cyber incidents among firms reporting attacks has risen from $229,000 last year to $369,000 – an increase of 61%, with medium and large firms bearing a disproportionate amount of the cost.

Supply chain incidents now commonplace

Nearly two-thirds of firms (65%) have experienced cyber-related issues in their supply chain in the past year. Three quarters of technology, media and telecoms (TMT) and transport firms have been hit.

More small firms attacked this year

While larger firms are still the most likely to suffer a cyber attack, the proportion of small firms (less than 50 employees) reporting one or more incidents is up from 33% to 47%. For medium sized firms with between 50 and 249 employees the proportion has leapt from 36% to 63%.

Loss figures impacted by large incidents

The figures above are strongly influenced by a sharp rise in the cost of the biggest single incident reported. The mean cost has jumped from $34,000 a year ago to a fraction under $200,000. For large firms, there has been an 18-fold rise to $395,000. The comparable figure for small firms is $9,000, up from $3,000 in 2018.

German firms hit hardest – for the second year running

Mean cost for all incidents experienced in Germany during the year was over $1 million for medium and large firms rising to over $1.5 million for enterprise-scale businesses.

Cyber security spending up 24%

The average spend on cyber is now $1.45 million and the pace of spending is accelerating. The total spent by the 5,400 firms in our report comes to a remarkable $7.9 billion. Two-thirds of respondents say they plan to increase their spending on cyber by 5% or more in the year ahead.

Country comparisons

Although there are variations when it comes to cyber loss experience across the seven countries surveyed, there are common themes around the prevalence of cyber attacks and the cost of recovery.

Belgium

- Most heavily attacked (71% reported a cyber incident) and most likely to report a supply chain related issue.
- Topped the list for frequency of attacks: more than a third of those targeted were attacked four times or more.
- 16% of the country's large and enterprise scale firms rank as 'experts' on our cyber readiness model – putting them at the top of the table.

France

- 81% of French firms received the lowest ranking in our cyber readiness model – just 6% qualify as 'experts'.
- Spent more on cyber security (mean cost of $2.1 million) and suffered the lowest number of cyber incidents.
- Least likely to have cyber cover – along with German firms.

Germany

- Fewer large and enterprise firms qualify as 'experts' in our cyber readiness model – down from 20% to 14%.
- Hit hardest in the past 12 months with a mean cost for all incidents of over $900,000 – more than twice the average mean cost for all seven countries.
- A German firm reported a cost for all incidents of $48 million, the highest figure among the study group.

The Netherlands

- Best improvers in our 2019 cyber readiness model – proportion with the lowest ranking down from 82% to 76%.
- 19% of firms reported a distributed-denial-of-service (DDoS) attack compared with an average of 15% across the study group.
- Worst hit by cloud outages with 27% of targeted firms reporting a problem.

Spain

- Firms responded vigorously to an incident with 18% increasing their spending on detection technologies and 22% increasing spending on prevention technologies.
- Most rigorous approach to evaluating their supply chain risks and yet 72% reported an attack in this area.
- Most likely to have a standalone cyber insurance policy: 49% compared with 41% across the study group.

UK

- The lowest cyber security budgets with less than $900,000 on average compared with an average across the study group of $1.46 million.
- Mean cost of all incidents for UK firms was below average for the survey: $243,000 compared with $369,000.
- Most likely to say they could clearly measure the business impact of cyber incidents.

US

- Lowest mean cost of incidents – $119,000 compared with $369,000 across the study group.
- Number of large and enterprise firms qualifying as 'experts' on our cyber readiness model has more than halved – down from 26% to 11%.
- 72% of US firms plan to increase their security spending – the highest proportion amongst the seven countries

The size of the problem

More businesses report being impacted by a cyber incident year-on-year, with the risk appearing to be indiscriminate when it comes to size of business or sector.

Cyber attacks intensify

The proportion of respondents reporting a cyber incident has risen from 45% last year to 61%, and the figures are higher in every category of breach.

Nearly a quarter of firms (24%) report a virus or worm infestation and 17% a ransomware attack. The number suffering a distributed denial-of-service (DDoS) attack is up from 10% to 15%.

The frequency of attacks has also increased markedly. Among firms that experienced cyber attacks, the proportion reporting four or more incidents is up from 20% to 30%.

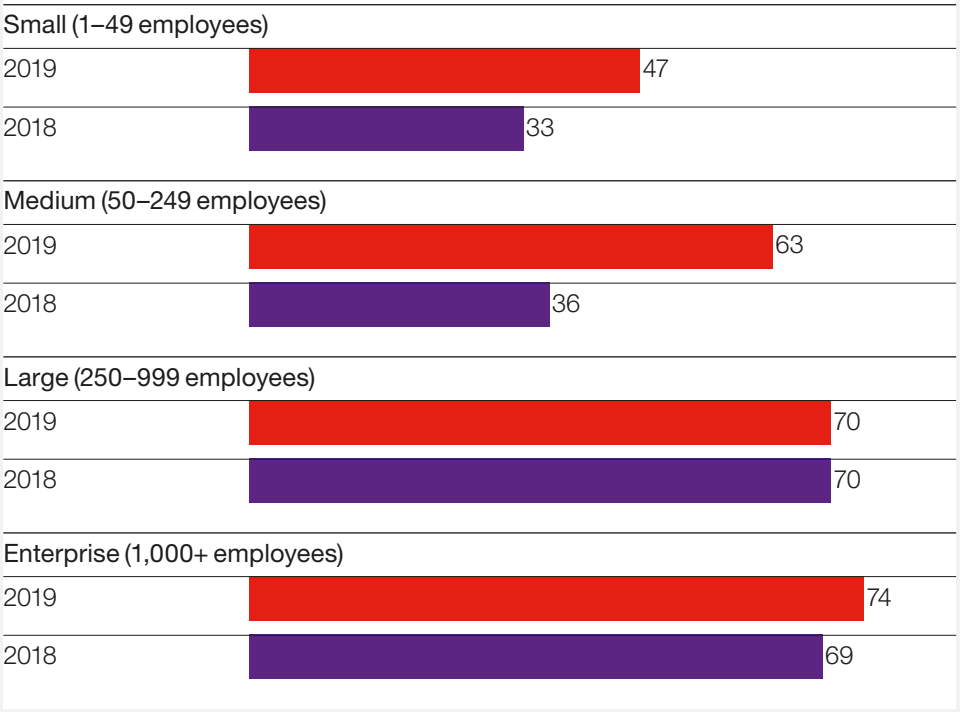
More small firms targeted this year

An increasing proportion of smaller firms are now caught up in the cyber battle. Small and medium sized firms are much more likely to have suffered multiple attacks this year, and on average the proportion of small and medium firms that have had an attack has increased 59%.

Bigger firms are more likely to have suffered repeat incidents. More than a fifth (21%) experienced five or more attacks in the year compared with an average of 16% for all respondents.

It is possible of course that larger businesses are simply better at spotting data breaches than smaller firms. However the implementation of GDPR last year has obliged larger firms – which stand to suffer big penalties for extensive breaches or failure to report an incident in a timely manner – to become more watchful and keener to report when incidents occur.

Proportion of firms targeted in 12-month period (%)



Proportion of firms reporting an attack (%)

	2019	2018
Belgium	71	–
France	67	–
Germany	61	48
The Netherlands	68	50
Spain	66	57
UK	55	40
US	53	38

2018 data not available for Belgium or France.

No industry immune

In every one of the 15 sectors tracked in this report, the proportion of firms reporting one or more attacks has risen sharply. Across all seven countries, the most heavily targeted sector was TMT, where 72% of respondents reported one or more attacks, up from 53% a year ago. Government entities came second (71% reporting an attack, up from 55%), followed by financial services (67%, up from 57%).

Is the supply chain a weak link?

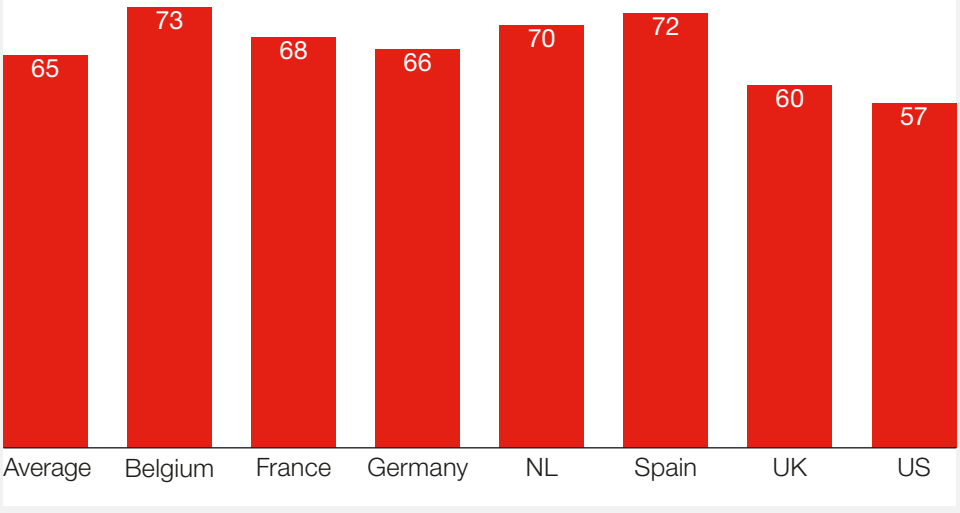
For the first time we asked a series of questions relating to the security of firms' supplier networks. Nearly two-thirds of respondents (65%) said they had experienced one or more cyber attacks as a result of a weak link in their supply chain over the past year. The figures were highest in Belgium and Spain (73% and 72% respectively). Overall, three-quarters of TMT and transport firms were targeted. Just over half of all firms in the study now include cyber KPIs in their contracts with suppliers. The figure is 65% among enterprise firms but only 39% among small firms.

Asked how often they evaluated the security of their supplier networks, nearly three quarters of firms (74%) said they did so at least once a quarter or on an ad-hoc basis. Spanish firms look the most prudent in this area: nearly half (47%) said they evaluated the cyber security of their suppliers once a month compared with 32% of respondents overall. 8% of firms said they had increased evaluation of their supply chain as a result of an incident in the past year, with the figure highest among financial services firms (12%).

Reliance on the cloud brings risk

Many more respondents this year report problems with outages from third-party cloud providers (22%, up from 13%). Dutch firms were worst hit, with more than 27% of those that suffered cyber incidents reporting cloud outages, while across the respondent pool large and enterprise firms are more likely to suffer a cloud-related incident at 27% and 22% respectively. This doubtless reflects the propensity for firms to push more of their data into the cloud as they grow.

Proportion of firms experiencing a supply chain related cyber attack (%)



Financial impact

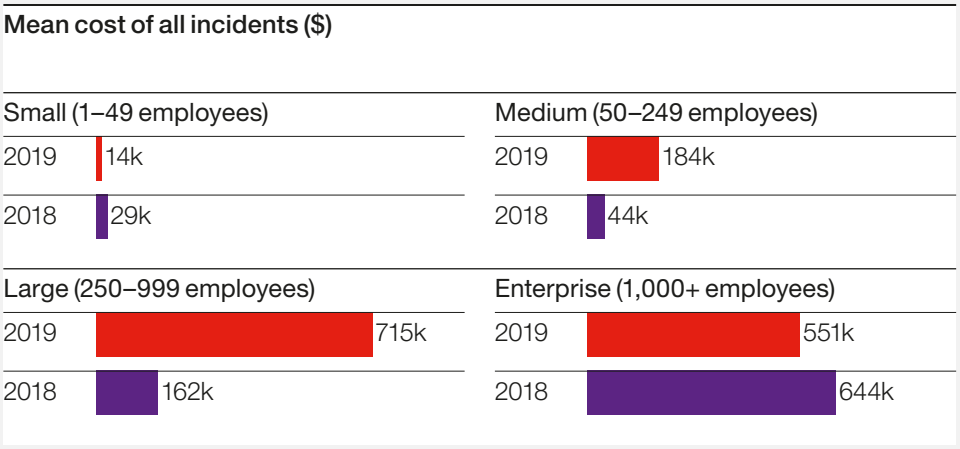
The cost of cyber crime to businesses appears to be on an aggressive upwards trajectory – up by as much as 61% in aggregate this year.

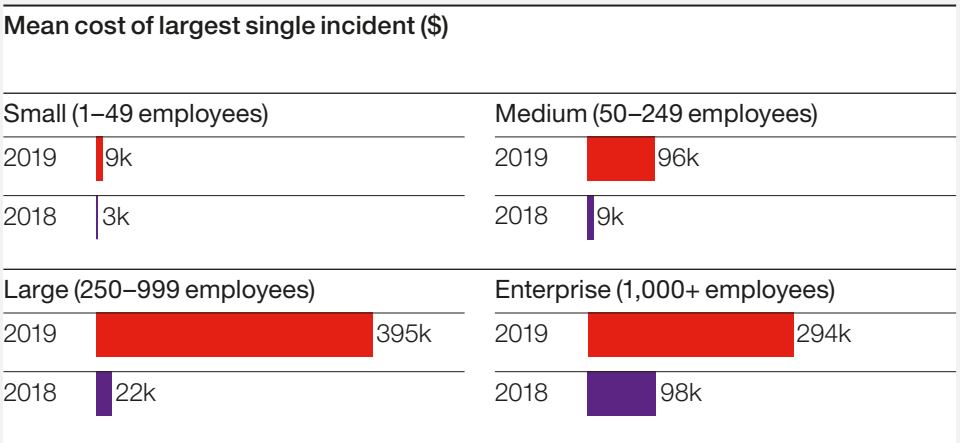
Cyber losses increase

Businesses worldwide are suffering mounting losses from cyber crime. Of the 3,300 firms in our survey that suffered attacks, around 2,250 tracked the costs to their business. Counting all incidents suffered over a 12-month period, the mean cost to those businesses rose from $229,000 to $369,000 – an increase of 61%. Assuming a similar experience among those firms that failed to track or quantify the impact of cyber attacks, the total cost for all 3,300 targeted firms was around $1.2 billion. Adjusting for the increase in both the scale of the study group this year and the numbers targeted, that is more than double the cost registered in last year's report.

Averages tell only part of the story, of course. While nearly half (47%) of small firms have suffered a cyber attack in the past 12 months (up from 33% in 2018), the mean cost of all incidents suffered has actually halved – from $29,000 to $14,000. However, the reverse is true for medium and large firms which have borne a disproportionate cost this year, often multiples of the previous year. This is the case for the UK, France, Spain and The Netherlands in particular.

One of the most striking figures to emerge is the mean cost of the largest single incident. A year ago, this came out at $34,000. This year, there has been a near six-fold increase – to a fraction under $200,000. For companies in every size bracket the cost of the biggest incident is now likely to be anything from three-to-18-times what it was only a year ago. The figures tally with broader industry data that suggest a sharp rise in the scale of ransom demands, for example, over the past year.





Germany takes the hit

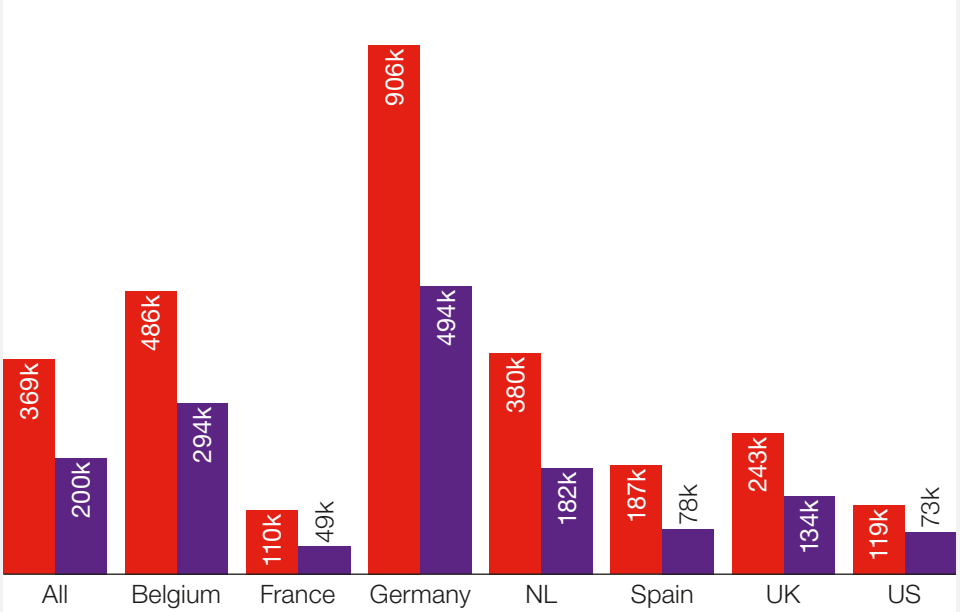
Overall, German businesses appear to have suffered worst with a mean cost for all incidents experienced in the year of over $1 million for medium and large firms and over $1.5 million for enterprise-scale businesses. It is also a German firm that reported the highest cost of all incidents – $48 million. There is a similar story when it comes to the cost of the largest single incident, with a mean figure for the largest German companies nearly ten times that of their French or Spanish counterparts – $776,000 compared with $78,000 and $82,000 respectively.

At the other end of the spectrum, US firms appear to have got off lightly. For medium and large firms the mean cost of all incidents is barely $100,000; for enterprises the figure is $213,000. This is despite a sharp drop (from 26% to 11%) in the number of large US firms that get top ranking in our cyber readiness model. One explanation is that US firms were far less exposed to the loss of customer or employee data, or to the theft of intellectual property (IP), trade secrets or research and development (R&D) in the past 12 months. For instance, twice as many French firms (16%) reported a data breach resulting in the loss of employee data as US ones (8%).

Impact spans all sectors

The average cost of all incidents has reduced in the past year in just five of the 15 sectors tracked (professional services, energy, retail and wholesale, food and drink and government related) and even there the average cost of the single largest incident has risen sharply.

Mean cost of cyber incidents ($)



Mean cost of all incidents by sector ($)

	Pharma and health	Travel and leisure	Financial services	Transport	TMT
2019	726,000	703,000	628,000	530,000	464,000
2018	103,000	148,000	400,000	157,000	349,000

Mean cost of largest single incident by sector ($)

	Pharma and health	Travel and leisure	Financial services	Transport	TMT
2019	388,000	427,000	301,000	229,000	288,000
2018	11,000	29,000	83,000	38,000	52,000

Cyber readiness model

Measuring how closely firms match up to what counts as best practice shows that in most businesses there is still some way to go when it comes to cyber preparedness.

Progress has stalled

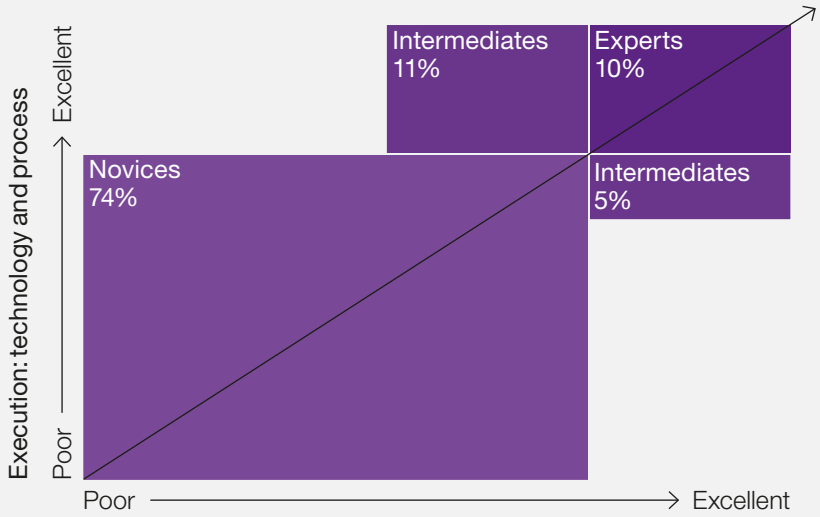
Despite increased regulation and a number of high-profile breaches, firms actually achieved lower scores in our cyber readiness model this year, with nearly three quarters (74%) failing to reach our threshold for expertise in any area.

The cyber readiness model measures how closely firms match up to what counts as best practice. Respondents are asked a series of questions covering their approach in four areas – strategy, oversight and resourcing on the one hand and technology and process on the other. They are invited to tell us how closely their way of doing things aligns with a well structured, rigorous and effective approach.

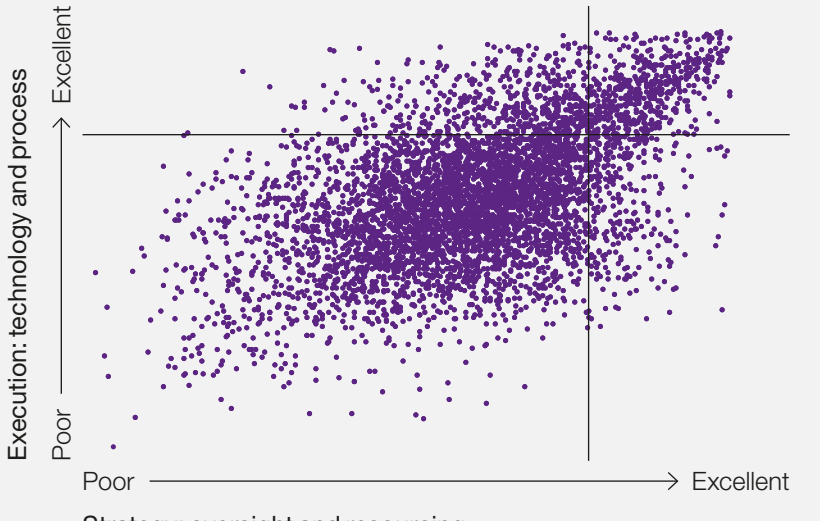
Respondents are scored on each answer and then ranked on a scale from 'cyber novice' and 'cyber intermediate' to 'cyber expert'. Firms that score four or more (out of five) on both axes qualify as experts. Those that achieve that score on one axis but not both are intermediates. Those that fall below a score of four in both departments count as novices.

Our cyber readiness scatter chart shows the results for the whole study group. Overall, the proportion of firms that made it into the expert category this year is slightly down from 11% to 10%. Intermediates make up a further 16% (same as last year) and novices constitute the remaining 74%.

Cyber readiness model



Cyber readiness scatter chart



Organisations take action

Businesses are alive to the cyber threat and responding accordingly, with evidence emerging of more decisive progress than in previous years.

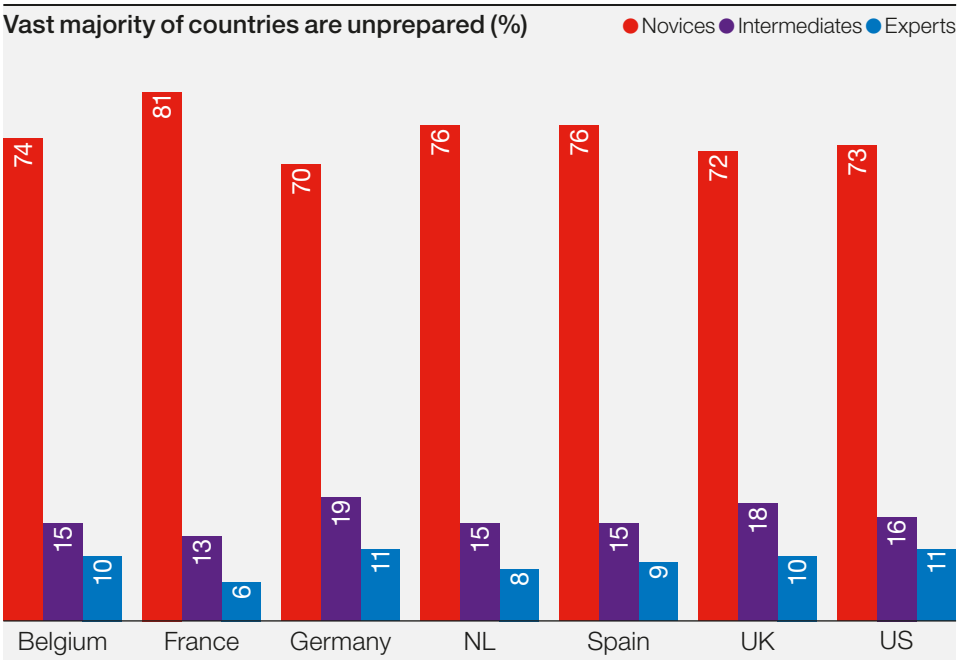
More firms now appoint a cyber head	The proportion of businesses with 'no defined role for cyber security' has halved (32% to 16%). Not all of the remaining 84% have their own head of cyber security or dedicated team in this area; 19% use an external service provider to manage their cyber security. Three-quarters of small businesses now have at least one person or a third-party supplier looking after cyber security (up from 56% a year ago). They still have some way to go before they can match bigger firms, 95% of which have a defined role for cyber security, but it is an encouraging indicator of progress.
More respond positively to incidents	More firms are responding to security incidents with concrete action. A year ago, almost half of respondents (47%) said they had changed nothing following cyber security incidents. This year, the figure has fallen by almost a third, to 32%. Among the novices, the numbers are down from 51% to 33%, and among the intermediates the figure is down from 42% to 31%.
Less complacency, more realism	Firms are less confident in the efficacy of the security measures they have put in place, and in many areas, confidence has been declining ever since our first report in 2017. This is likely to reflect not only the intensifying cyber threat but also the increase in regulation that firms are facing – both from GDPR and the New York Department of Financial Services Cyber Security Regulation (which places similar requirements on businesses that operate within New York as the GDPR does within Europe). Standing still in effect means getting worse over time.
Regulatory change prompts action	When we asked firms what, if any, changes they had made as a result of new regulations, such as GDPR, the great majority of Continental European firms (typically around 84%) had put some change into effect. Slightly fewer UK firms had done the same (80%). The figure in the USA, where GDPR may be considered a peripheral issue for domestically-focused businesses, was significantly lower, with nearly a third (32%) saying nothing had changed.
Does expertise pay off?	The average cost of all incidents for the experts is $456,000 compared with $558,000 for those judged to be intermediates. Both figures are substantially higher than for the cyber novices ($314,000), but that is explained by the heavier weighting towards smaller firms among the novices. The cost of breaches for smaller firms is generally a fraction of that suffered by big firms; the average for large and enterprise businesses is $612,000 compared with $77,000 for small and medium sized firms.

Cyber readiness by country

More than four-fifths of French firms (81%) are in the novice category. Along with The Netherlands, France has the smallest proportion of large and enterprise firms that rank as experts, at 9%. Overall, US, German and Belgian firms score highest – with around a 10% overweighting towards experts. However, there has been a dramatic decline in the number of large and enterprise firms in both the USA and Germany that qualify for expert status. In Germany, the proportion is down from 20% to 14%; in the USA it is down from 26% to 11%.

The USA and German figures are the main reason for an overall fall in the number of experts among large and enterprise companies this year – from 21% to 12%. Nearly three-quarters of them (73%) now rank as novices. That compares with 61% a year ago. Given the resources at their disposal and the much higher security budgets they deploy, this comes as something of a surprise.

Vast majority of countries are unprepared (%)



Proportion with no defined role for cyber security (%)

	2019	2018
All countries	16	32
Belgium	12	–
France	12	–
Germany	15	31
The Netherlands	12	36
Spain	14	26
UK	20	33
US	20	32

2018 data not available for Belgium or France.

As a specialist insurer, we have been offering cyber cover for over 20 years – giving us a unique insight into what constitutes good and bad when it comes to recognising and responding to the cyber threat. That experience, combined with the insight gained from this research, gives us an informed view on where businesses go wrong – and how they can do better.

What constitutes good and bad?

- ✓ Executive buy-in – cyber security is a priority for the board or proprietor
- ✓ Clear strategy set by multiple stakeholders within the business
- ✓ Dedicated head of cyber or team
- ✓ Adequate cyber budget – on average, experts spend over $1 million more on cyber than novices
- ✓ Regular evaluation of supply chain, security KPIs in supply contracts
- ✓ Process – ability to track, document, measure impact
- ✓ Cyber awareness training throughout the workforce
- ✓ Proactive testing – through simulated attacks
- ✓ Regular phishing experiments
- ✓ Readiness to learn, respond, and make changes after an incident
- ✓ Cyber insurance policy in place

- ✗ Cyber security dealt with on ad-hoc basis – no clear line of responsibility
- ✗ No formal cyber strategy, no dedicated cyber budget
- ✗ Over-reliance on technology, light on people
- ✗ Slow response to incidents
- ✗ Occasional, often patchy, employee awareness training
- ✗ No evaluation of supply chain vulnerabilities
- ✗ No simulation of cyber attacks or employee responses
- ✗ Reliance on general property insurance

Cyber security spending

Prevention is better than cure and this year has seen a notable increase in expenditure on cyber security measures – with many anticipating this trend will continue in the year ahead.

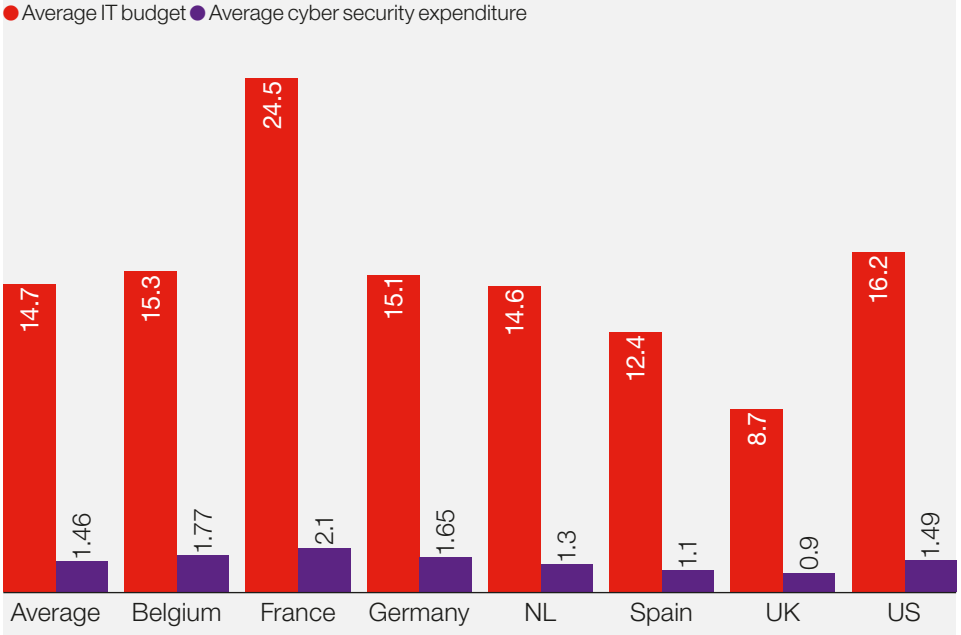
The pace is accelerating

Across the study group, there has been a marked rise in overall spending on IT – up from an average $11.2 million last year to $14.7 million this year. This is largely explained by the first-time inclusion of France, where the average IT budget is $24.5 million. The percentage of IT budgets spent on cyber is marginally lower than before – accounting for 9.9% of the total IT spend compared with 10.5% the previous year – but by value it is up nearly a quarter (24%), to $1.46 million.

The inclusion of Belgium and France this year has also skewed the numbers to the high side. The average spend on cyber security by Belgian companies is $1.77 million and for French companies it is $2.1 million. Both figures are well above the average for all seven countries.

Multiplied across the whole study group of 5,400 firms, the total spend on cyber security comes to a staggering $7.9 billion over the year. After adjusting for the increased size of the study group this year, it represents a rise of just under 20% on the equivalent 2018 figure, with spending heavily weighted to the biggest firms.

IT budget and expenditure on cyber security ($m)



Figures rounded to the nearest $100,000

Average annual spend on cyber security ($)

Number of employees	Average annual spend
1–9	7,000
20–49	37,000
50–99	115,000
100–249	436,000
250–499	930,000
500–999	1,018,000
1,000–4,999	2,336,000
5,000–19,999	4,009,000
20,000+	10,643,000

Shift in spending for the year ahead

Around two-thirds of respondents (67%) say their spending on cyber security will increase in the year ahead, up from 59% a year ago. While higher spending on technology is still a target for 50% of respondents, the numbers planning to spend more on employee training, cyber security staffing and consultants or third-party services are notably higher, suggesting a shift in emphasis towards people and processes.

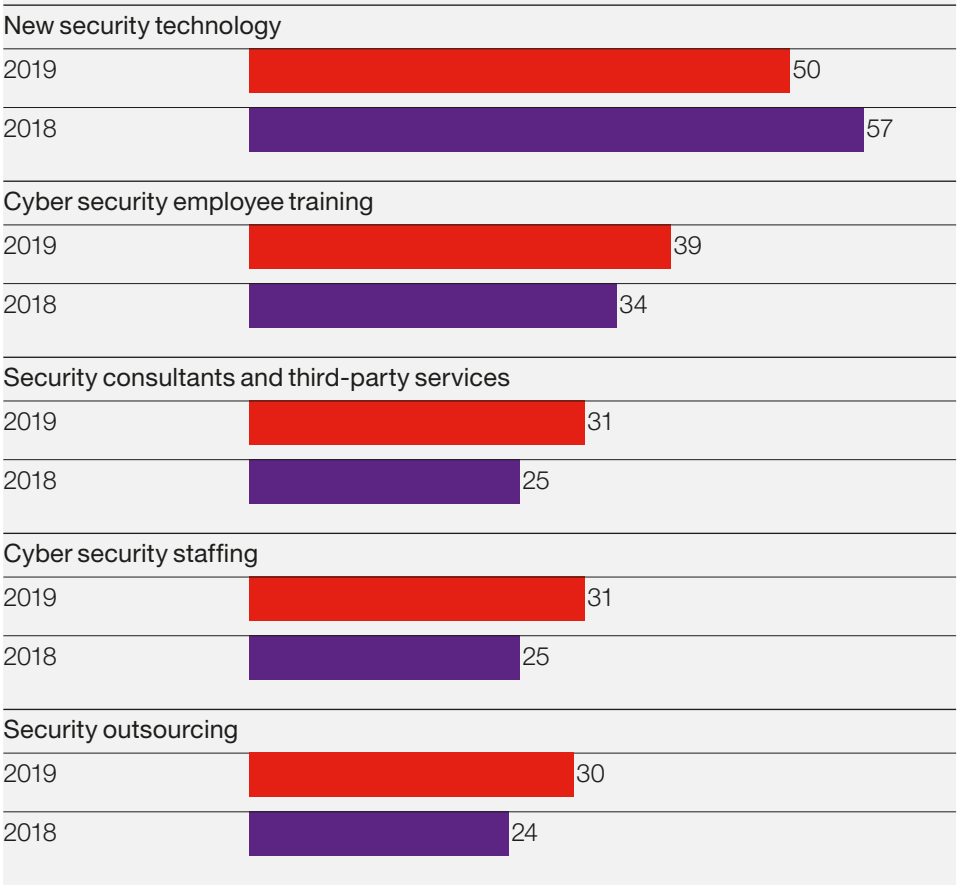
This is borne out by the priorities firms have set themselves for the year ahead. Taking those action areas most frequently mentioned as a 'high' or 'critical' priority gives a good indication of where this year's spending will be directed. Many are process-oriented.

US firms are most likely to be planning increased cyber security budgets, with 72% saying they intend to increase spending here. Ironically, it is those firms that already spend the most – essentially the larger firms in the study – that are planning the biggest budget increases.

Plan to increase spending on cyber security (%)

Small (1–49 employees)	60
Medium (50–249 employees)	67
Large (250–999 employees)	73
Enterprise (1,000+ employees)	75

Technology and people spending priorities for the year ahead (%)



Cyber insurance

Growing awareness of the cyber risk is contributing to an increased appetite for cyber insurance, as more businesses say they have invested, or plan to invest, in cyber insurance.

What is cyber insurance?

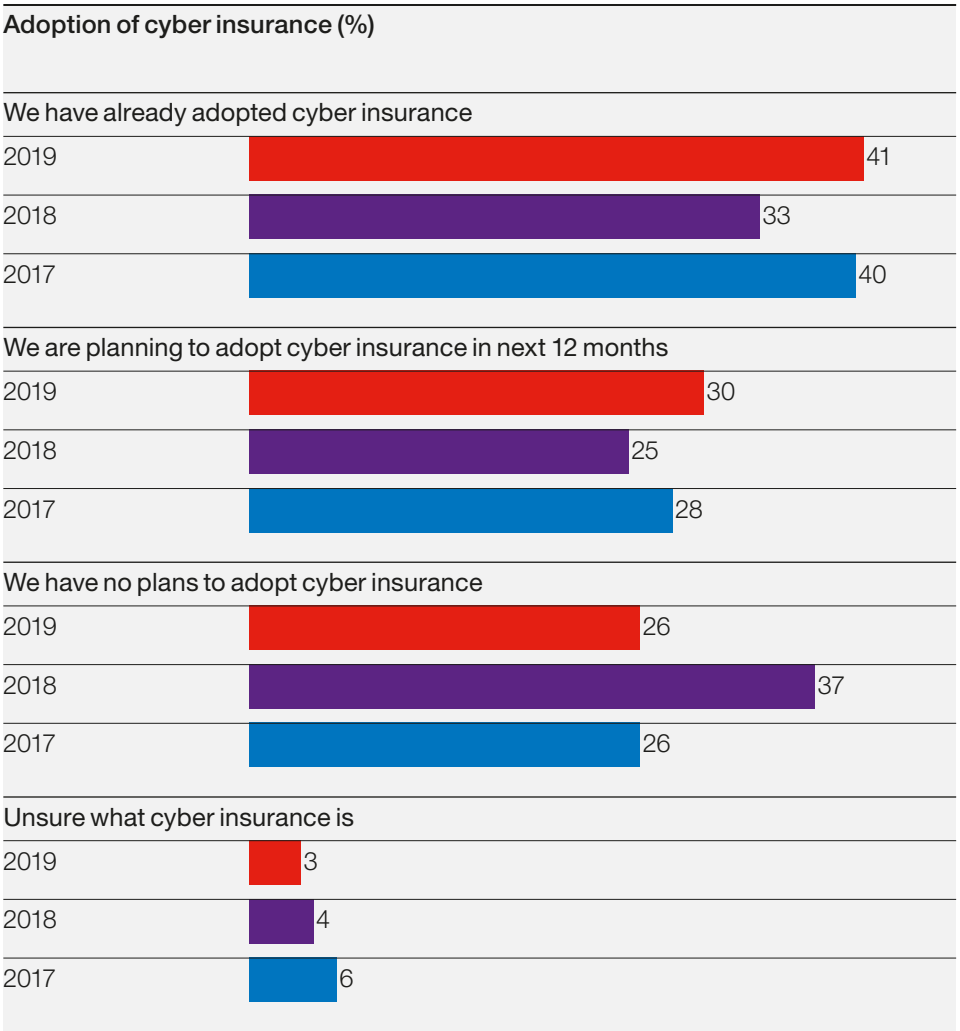
A cyber attack can require a range of expert services including lawyers to notify data protection regulators and defend claims, IT professionals to investigate breaches and restore IT systems, and PR consultants to manage communications with the media and wider world. Cyber insurance provides cover for all of these costs as well as financial losses suffered, whether through lost business or third-party claims.

Rising uptake of cyber policies

Uptake and understanding of dedicated cyber insurance is on the rise as 41% now say their firm has cyber insurance, up from 33% a year ago. A further 30% say they are planning to adopt cyber insurance in the next 12 months, up from 25% a year ago.

The proportion who say they are 'not sure what cyber insurance is' has halved since our 2017 report from 6% to just 3%. However, some confusion remains among small firms, where 6% continue to say they are not sure what cyber insurance is.

Unsurprisingly, uptake is highest among those firms that qualify as experts on our cyber readiness model, where 59% have cyber cover and larger businesses are much more likely to have cyber insurance than small ones. More than half of enterprise scale firms say they have cyber cover compared with just 27% of small firms with under 50 employees.



Research methodology

The findings contained in this report have been drawn from a representative sample of firms by size and sector, involving those on the front line of the battle against cyber crime.

Respondent level (%)	
Director	51
Vice president	24
Manager	13
C-level executive	12

While all surveyed are engaged with their organisation's cyber security effort, 70% are either the final decision-makers or part of the decision-making team.

Scope of the report

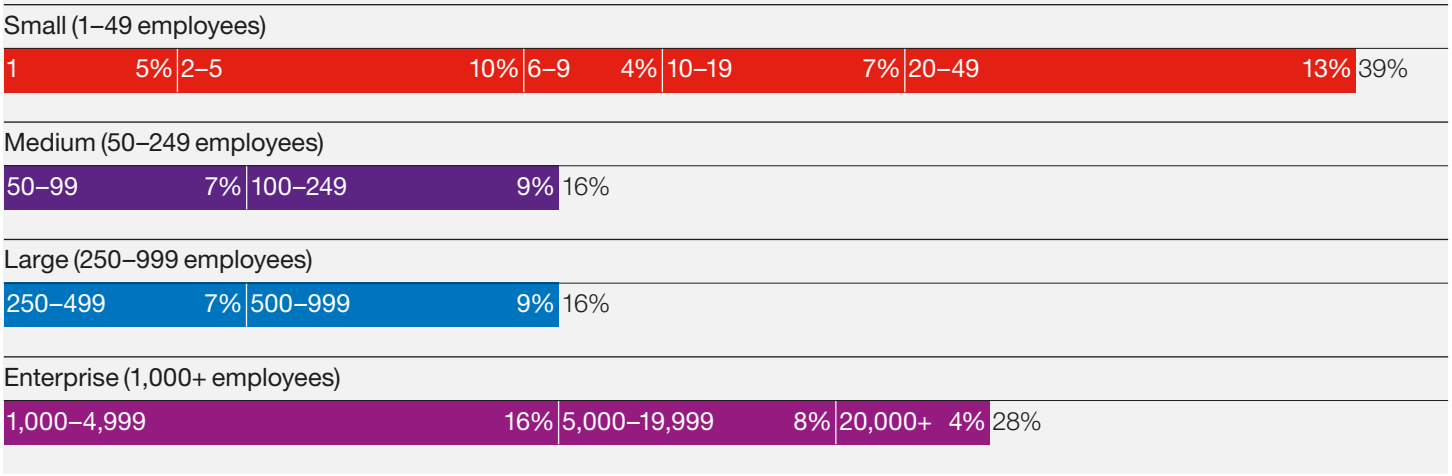
Hiscox commissioned Forrester Consulting to assess organisations' cyber readiness. In total 5,392 professionals involved with their organisation's cyber security strategy were contacted (1,000 plus each from the UK, USA and Germany, and 500 each from Belgium, France, Spain and The Netherlands). Thirty-nine percent of respondents were from organisations with fewer than 50 employees (small firms), 16% from medium sized firms employing 50-249 people, 16% from large firms employing 250-999 personnel and the remaining 28% from enterprises with 1,000 or more employees. Respondents completed the online survey between 22 October and 7 December 2018.

Changes for this edition

A number of changes have been made both to expand the scope of this year's report and make it more statistically meaningful at the small company level in particular. The study group now comprises seven countries – with the addition this year of Belgium and France. The number of respondents has increased from 4,100 to approximately 5,400, making the Hiscox Cyber Readiness Report one of the broadest of its kind.

The weightings between small (defined as under 50 employees), medium (50 –249), large (250–999) and enterprise (1,000 plus) have also been changed. Small firms now account for 40% of the study group, compared with 33% a year ago. Within that grouping, firms with five or fewer employees make up 5% of the total. The weighting towards enterprise firms has also been increased, from 17% to 27%. The middle ground of medium and large firms now makes up 33% of the total compared with 50% a year ago. There is one other change. This year's questions on IT budget, cyber security spend and resourcing were put only to those who were either the final decision makers or part of the decision making team in these areas.

Breakdown of respondents by business size



Sector in which respondents work (%)	
Technology, media and communications	16
Professional services	11
Manufacturing	9
Retail and wholesale	8
Business services	8
Financial services	8
Construction	7
Pharmaceutical and healthcare	7
Transport and distribution	5
Travel and leisure	5
Food and drink	5
Energy	3
Property	3
Government	3
Non-profit	2

Department in which respondents work (%)	
IT and technology	22
Operations	11
Finance	10
Marketing and communications	8
Sales	7
Risk management	6
Product management	6
Human resources	6
Procurement	5
General counsel	5
Ecommerce	5
Executive management	4
Owner	3

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

19882 04/19