HISCOX

Hiscox Cyber Readiness Report 2020

The fourth annual international Hiscox Cyber Readiness Report has been compiled in collaboration with research firm Forrester. The report not only provides an up-to-the-minute picture of the cyber readiness of organisations, it also offers a blueprint for best practice in the fight to counter an ever-evolving threat. It is based on a survey of executives, departmental heads, IT managers and other key professionals. Drawn from a representative sample of organisations across eight countries by size and sector, these are the people on the front line of the business battle against cyber crime.

Meeting the cyber challenge head-on

There is clear evidence of a step-change in cyber preparedness.

Gareth Wharton
Cyber CEO, Hiscox

There is one very positive message from this year's report. After two years when progress appeared to stall, there is clear evidence of a step-change in cyber preparedness. This is apparent not only in the metrics that make up our cyber readiness model but also in the enhanced levels of activity and spending underway to meet the challenge. This is not a moment too soon.

While the number of firms reporting a breach is down, the cost and intensity of criminal activity in this area appear markedly higher. The numbers that have paid a ransom following a malware infection are chilling. Nobody should doubt the scale of the problem.

The companies that are part of our report were questioned prior to the coronavirus pandemic, so the findings reflect their perspectives in more certain times. No doubt the increase in experts seen this year is an important step to protecting companies in the ever-changing cyber threat landscape.

While a high level of preparedness can be no guarantee of security, there are credible steps firms can take to minimise their vulnerability, respond effectively and recover in good order. It is about defence in depth and building resilience.

From our perspective as a cyber insurer, we believe a breach, when it comes, should not be the end of the process. It is noticeable how many of the 'cyber experts' in this report have taken out dedicated cyber cover not just to protect themselves financially but to be able to draw on the specialist expertise it brings when the chips are down. Equally, learning from the incident, and making sure it informs and improves planning and resilience to subsequent incidents, is key. As the report illustrates, this is precisely what large numbers of the experts do.

Take-up of standalone cyber cover, however, remains patchy, with more than half of firms in our report relying on more general cover. This is a conundrum. Almost certainly, they would all have cover for fire and theft, yet the report suggests they are 15 times more likely to have a cyber incident (30% in UK) compared with a fire or theft (2% in UK).

This year's report highlights the importance of changing employee behaviour, which takes the form of company-wide training to build cyber security awareness. This is another area where an insurer has a big role to play. Our online training platform, the Hiscox CyberClear Academy, provides cyber awareness training for our clients' staff, and more than 12,000 people have now completed the course. We notice that those that have done so are often quicker to notify of any breach, allowing us to help them get back up and running more swiftly and with better outcomes.

Cyber readiness comes in many forms. We hope this report, with its numerous examples of best practice, will help people better understand and respond to the challenge.

Executive summary

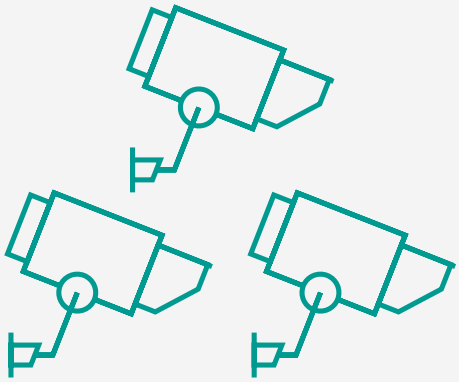
There is a new awareness of the cyber challenge.

Let's get serious

Firms that qualified as experts in our cyber readiness model nearly doubled this year – from 10% to 18%.

Security spending increases

Firms increased their cyber security spending by 39%. Expert firms spent more and plan to go on doing so.



Firms are losing more

Total cyber losses among the affected firms were $1.8 billion – up from $1.2 billion the previous year.

Cyber losses soar

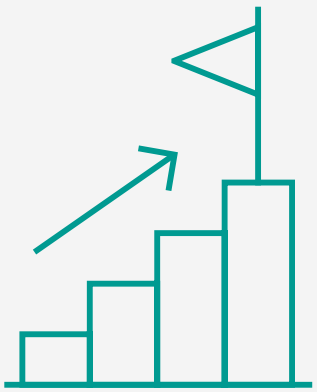
The financial impact on those affected by a cyber event rose nearly six-fold to a median of $57,000.

Cyber events drop

The number of firms affected by a cyber event this year fell considerably, from 61% to 39%.

Highest recorded loss

The highest reported annual cyber loss was $87.9 million from a financial services firm in the UK



Held to ransom

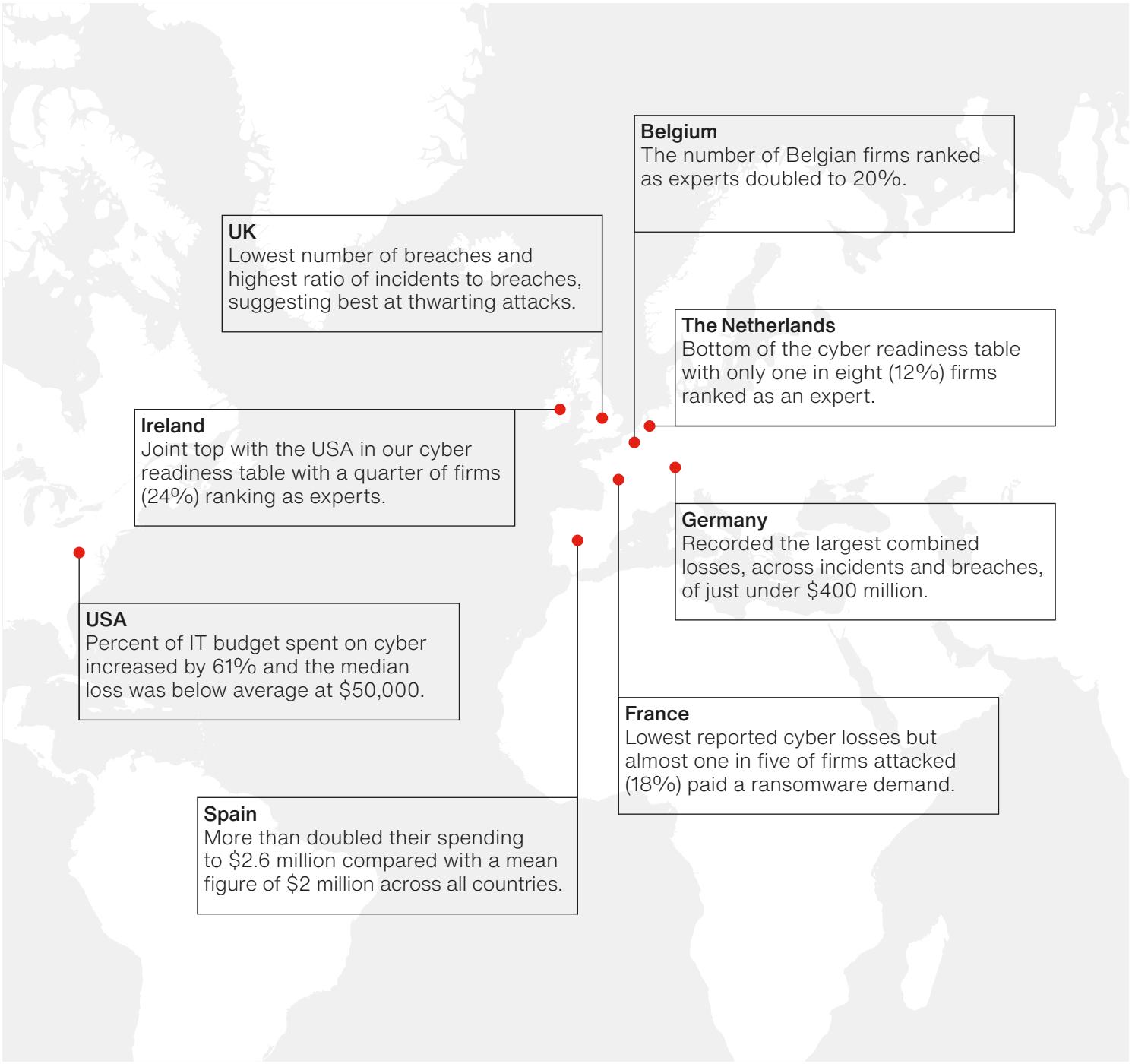
More than 6% of total respondents paid a ransom. Their combined losses came to $381 million.

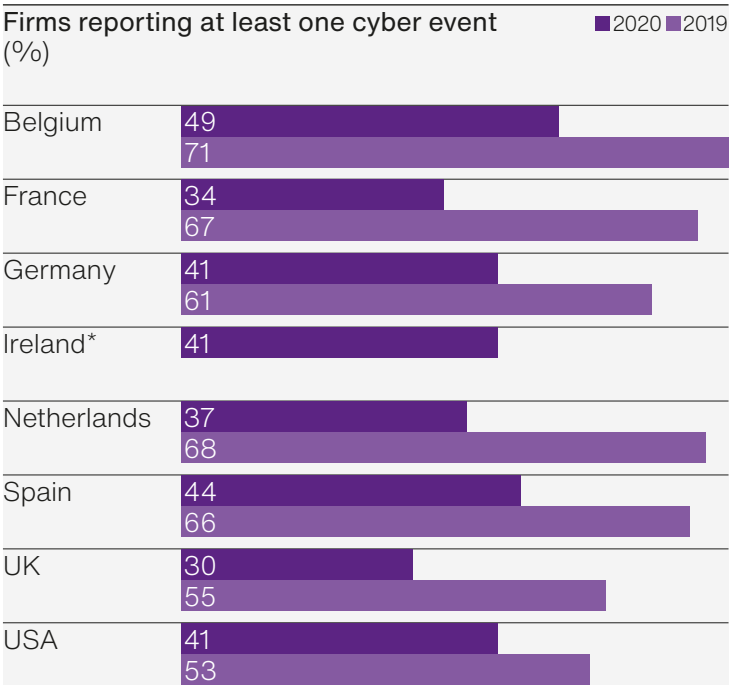
Positive signs

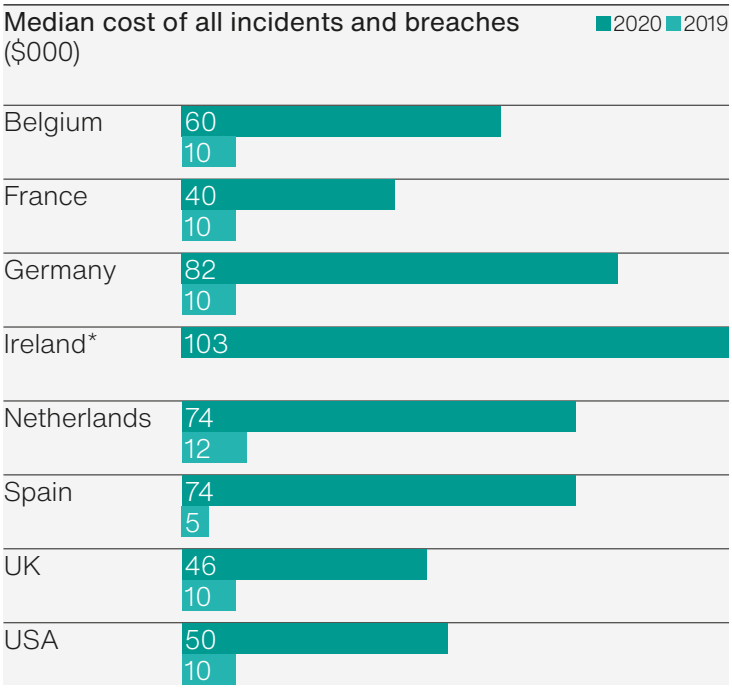
Twice as many firms responded to a breach by adding new security and spending more on employee training.

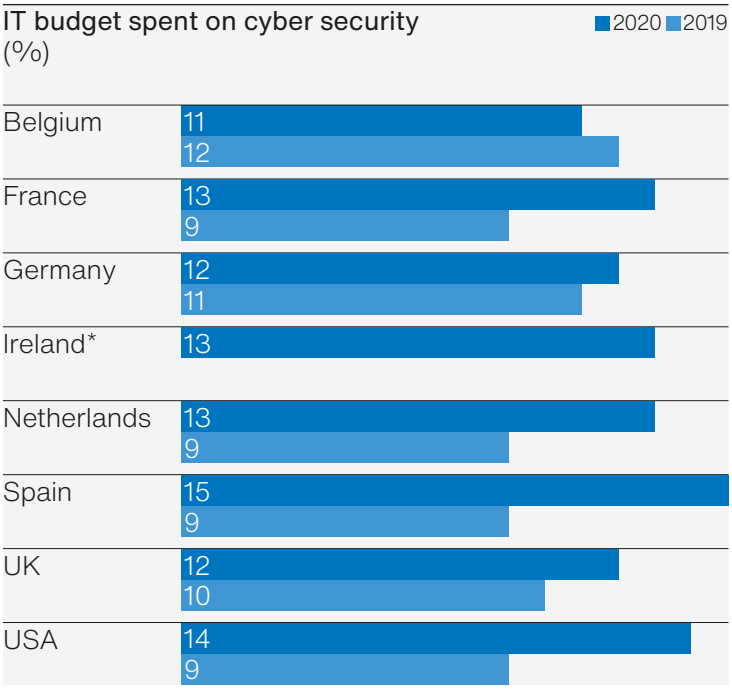
Country comparisons

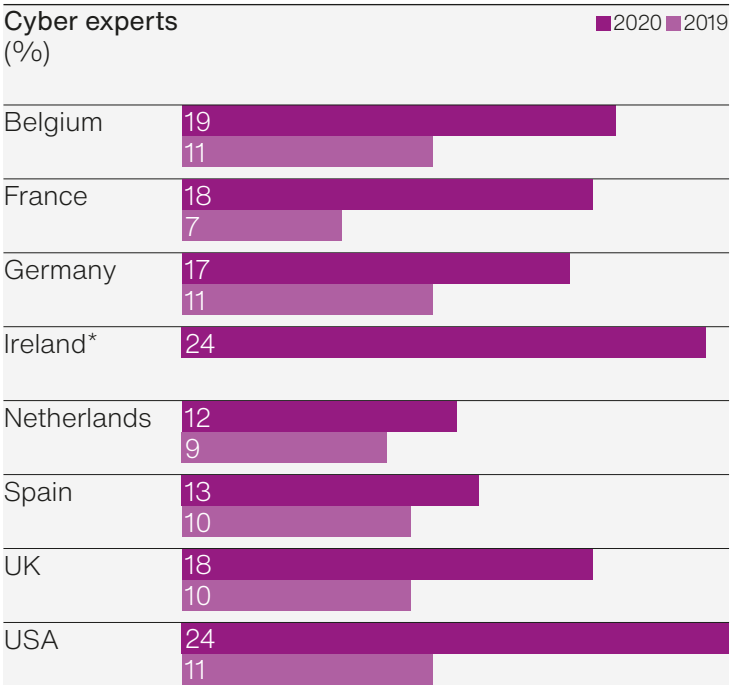
Cyber event costs and security investment increase around the world.











*Data only available for 2020.

The size of the problem

While a smaller number of firms experienced cyber events in the past year, the costs spiralled.

Fewer targets, bigger losses

The proportion of firms reporting a cyber security event in the past 12 months is down this year from 61% to 39%. That is the good news. The bad news is that the financial impact is many times greater than before.

One or more cyber events reported

For the first time, we asked firms to quantify separately the number of cyber incidents and breaches they had experienced, opening the way for more detailed analysis of firms' resilience. An incident is defined as any event that does not succeed in compromising the confidentiality, integrity or availability of information. A breach is any event that successfully compromises the confidentiality, integrity or availability of information, resulting in a material loss.

Among those reporting a cyber event of one kind or another, the median number of incidents was 50. The median number of breaches was 15. Belgian and German firms were the top targets, with median figures for incidents of 100 and 80 respectively. For breaches, the positions were reversed, suggesting German firms were a lot less successful at keeping hackers at bay. Taking all respondents, not just those who reported a cyber event or were 'don't knows', the median firm experienced 20 incidents and six breaches.

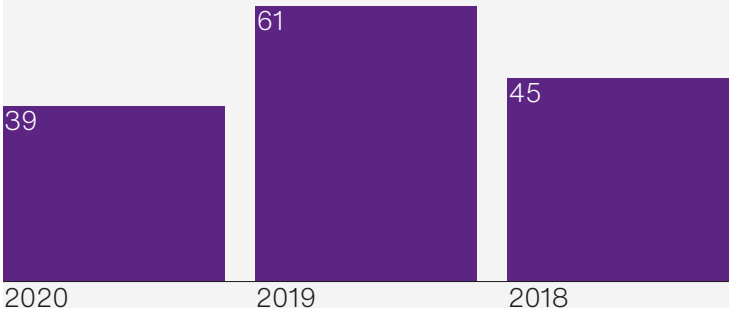
Emergence of 'super targets'

The numbers were strongly influenced by a relatively small contingent of firms in each of the eight countries that reported 500 or more events. They emerged because of a change in our questionnaire this year, allowing respondents to provide an open-ended response to the number of cyber events they had experienced.

It would be reasonable to assume they are all enterprise-scale businesses. They are not. There are super targets in each of our five size brackets. A surprising number are among the smallest.

There are many possible reasons for these figures. In many sectors, the majority of micro-firms have nobody managing cyber security. The smallest transport and distribution firms look particularly vulnerable with 59% saying they have no such role, either internal or external.

One or more cyber events reported
(%)



Equally, dependence on a managed service provider (MSP) may backfire when that MSP is itself attacked. Some firms could simply be over-counting by including spam emails.

A lack of effective counter-measures among some smaller companies provides one explanation. Analysis of the data suggests firms with fewer than 12 computers, and where anti-virus or anti-spyware was not deployed consistently across the organisation, were particularly likely to be super targets.

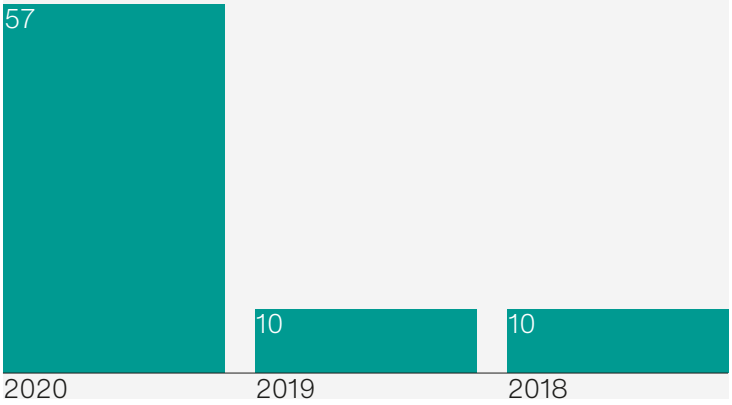
For all that, the biggest companies were more likely to be targeted than smaller ones. More than half of all enterprise firms (51%) – those with 1,000-plus employees – said they had at least one cyber incident. They also reported by far the most cyber incidents (a median 100) and breaches (80). They were almost certainly targeted more than the rest but they may also have been better at spotting attacks.

Failure to spend adequately on cyber security appears to be one common thread here. In the great majority of sectors it was big firms with more than 700 computers that devoted less than 8% of their IT budget to cyber security that became super targets.

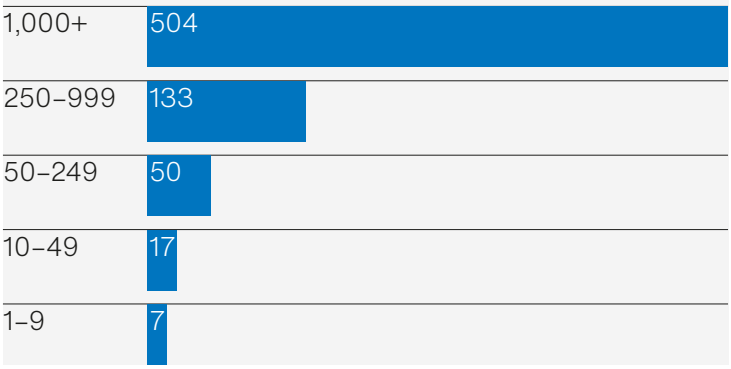
$1.8bn

Total costs spent by our sample due to cyber events in the past 12 months.

Median cost of all cyber events
($000)



Median cost of all incidents and breaches
By number of employees ($000)



The most heavily targeted sectors were financial services, manufacturing and technology, media and telecoms (TMT) – with 44% of firms in each sector reporting at least one incident or breach. Ironically, these were the three sectors that emerged best on our cyber readiness model, but firms are often forced into becoming experts when they are heavily targeted industries.

Large number of 'don't knows'
Worryingly, 11% of overall respondents said they did not know how many times they had been targeted. That was up from 4% the previous year. Surprisingly, too, the largest percentage of 'don't knows' (15%) was among enterprise firms with more than 1,000 employees.

It is worth noting that the fall in the overall percentage of firms reporting a cyber event may reflect the increased weighting in this year's sample to micro businesses. Some 63% of businesses with fewer than ten employees said they had suffered no cyber incidents or breaches. But almost half (49%) had no defined role for cyber security – suggesting they could well have blind spots.

Costs accelerate to $1.8 billion
This year's figures illustrate the price to be paid for an online presence today. The median cost to the 1,971 companies that suffered cyber incidents and breaches, over the past 12 months, was $57,000. That represents a near six-fold increase on the previous year's $10,000.

Median cost of all cyber events

Totting up the cost of all cyber events reported by our sample brings the combined cost to $1.8 billion. That compares with $1.2 billion on the previous year, when the number of businesses attacked was more than a third higher.

Who was most vulnerable?
In short, it was the bigger companies that paid the highest price for an online presence. This should be no surprise as they were also the most heavily targeted.

Cost of all incidents and breaches

Behind the median figures, the financial impact varied enormously between countries, sectors and companies. The highest recorded total loss for any one company was $87.9 million (a UK financial services firm) while the highest loss from any one event was $15.8 million (a UK professional services firm). That compares with a median cost for the largest single incident of $4,200.

Largest incident or breach

Irish and German firms suffered the biggest median losses, but the pain was widely spread. Among firms that experienced attacks, the median losses for energy firms rose more than thirty-fold while several other sectors had to deal with losses many multiples of the previous year. The figures suggest cyber criminals increasingly see energy and manufacturing firms as lucrative targets.

Sectors bearing the most pain

The Hiscox view

We have seen a shift in the hackers' behaviour in the last six to 12 months as they focus more on industries such as energy and manufacturing. We believe there are three reasons for this. Firstly, reliance on automation (i.e. managed by computers). Secondly low maturity in cyber resilience (e.g. poor back-ups, limited disaster recovery planning or testing). Finally, low tolerance to what is often a high-impact outage. This offers rich pickings for ransomware attacks.

Ransomware: a lucrative business

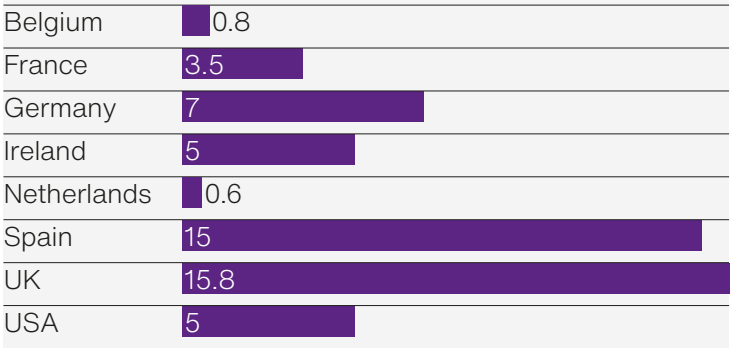
This year's data provide a chilling insight into the cost and frequency of malware and ransomware attacks. We asked respondents to detail the types of incidents and breaches they had experienced.

Most common types of breach

Enterprise-scale businesses were more likely to report breaches across multiple categories than smaller firms. This may be because they were more lucrative targets or were simply better at identifying attacks.

The most dramatic figures concern malware and ransomware infections. 350 firms reported paying a ransom following a malware or ransomware attack (16% of all firms attacked).

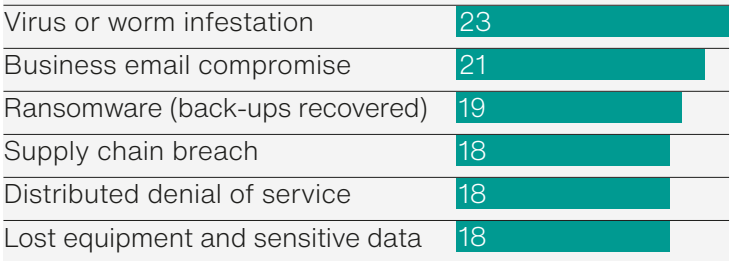
Largest incident or breach
($m)



Sectors bearing the most pain
Median losses ($)

	2020	2019
Energy	337,000	10,000
Manufacturing	100,000	12,000
Financial services	166,000	30,000
TMT	76,000	10,000
Pharmaceuticals	60,000	10,000

Most common types of breach
(%)



350

Firms in our sample that reported paying a ransom after a ransomware or malware attack.

Malware and ransomware infections
Incidents and breaches

	Malware with no ransomware	Malware with ransomware
Number of attacks	173	411
Mean losses	$492k	$927k
Largest annual loss for one company	$10.1m	$50.6m
Largest single loss	$1.5m	$7m
Total losses	$85m	$381m

Whether a ransom was paid or not, the mean losses for all firms subjected to a ransomware attack were nearly twice as much as those that only had to grapple with malware on its own – $927,000 compared with $492,000. The highest losses for any one company, which could have included costs other than ransomware, was five times higher, at $50.6 million.

Malware and ransomware infections

The figures drive home the importance of good detection and back-ups. Among firms reporting any form of cyber event, USA and France had the largest percentage paying a ransom (18% compared with an average of 16%). The good news is not all ransomware attacks were successful. Large numbers of firms reported recovering their data from a back-up or rebuilding it without resorting to paying of ransom (19% and 17% respectively).

The Hiscox view

We are seeing hackers' ransomware techniques evolve. Typically in larger attacks there are two distinct phases after the initial infection. The first phase is lateral movement. This is where attackers look for valuable assets (e.g. finance data) and assess the size of the target to set the ransom amount. The second phase is ransomware attack. This often happens at the weekend when there is less chance to react and when hackers can cause the most damage. There can typically be a period of one to three weeks between these two phases. Companies with good detection capabilities can stop the attack in this time and therefore suffer shorter outages, lower overall costs and less impact to business.

Longer-term impacts

The softer impacts of a cyber breach are often not mentioned or are simply too hard to quantify. Their gravity should not be doubted. Significantly more respondents this year mentioned either increased difficulty in attracting new customers (15% of firms that had been targeted, up from 5% before), the actual loss of customers (11% compared with 5% before) or the loss of business partners (12% compared with 4%).

Nearly one in five French firms (19%) reported greater difficulty in attracting customers after an incident or breach. Sixteen percent of Belgian firms lost business partners (compared with a mean 12%).

Overall, 15% of firms that were targeted said they had reevaluated the cyber security of their supply chain (up from 8% the previous year) or been subjected to increased evaluation by their own customers (15% compared with 10%). Bad publicity, affecting the brand or the company's reputation, was mentioned by 14% of respondents (up from 5% before). One in eight (13%) said they had experienced a reduction in business performance indicators such as their share price (up from 5% the previous year).

How to summarise this year's findings? While the number of companies hit by cyber events fell, the frequency and severity for those affected showed a sharp increase. Though some of that is clearly down to the additional costs of ransomware, this is a trend that should concern everyone involved in cyber security.

Cyber readiness model

There was a welcome uptick in the number of firms qualifying as experts in our cyber readiness test.

Big firms lead the way

The proportion of businesses qualifying as experts in our cyber readiness model has nearly doubled in a year – from 10% to 18%. By the same token, the number falling into the novice category has dropped from 74% to 64%. This comes after a small fall in the readiness scores the previous year, suggesting then that progress had ground to a halt.

Cyber readiness distribution

The first time inclusion of Irish businesses has helped to lift the mean score. Irish firms align with US ones at the top of the readiness table with 24% qualifying as experts and are most likely to have either a dedicated head of cyber security or a dedicated team (89%).

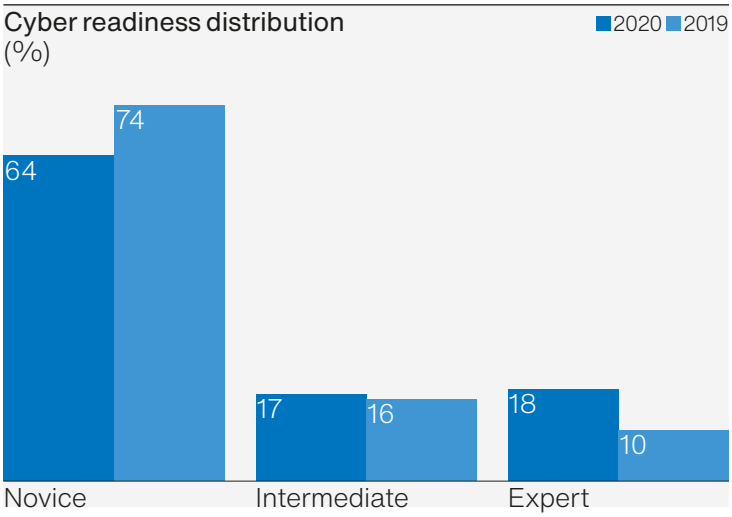
This may reflect the large number of global financial and technology businesses that have chosen to use Ireland as a European hub, though the country's weighting to these sectors is not markedly out of line with the mean.

Every country has contributed to the improvement. France, behind the curve in the two previous reports, saw its proportion of experts triple (from 6% to 18%) a reward perhaps for exceptional levels of cyber-related spending over the past two years.

Size still key

Cyber readiness is clearly an area where size matters. Big businesses have big resources. There is a clear correlation between the numbers employed in the security function and a firm's readiness score. For instance, firms employing more than 50 people in their security team constitute only 11% of the sample, but represent 19% of experts. Among businesses with 1,000-plus employees, 29% boast security teams of this size.

Big firms spend an order of magnitude more than their smaller counterparts. While the average micro business spent $13,000 on cyber security in the past year, firms with 1,000-plus employees spent on average $8 million. On the whole, spending appears to buy expertise. Firms ranking as experts spent on average $4.2 million on cyber security in the past year, compared with the average novice spend of $1.3 million.



Though there was an increase in smaller businesses in the report this year, the overall readiness score has still improved. That is largely down to a doubling (or more) in the numbers of medium, large and enterprise firms ranked as experts compared with last year.

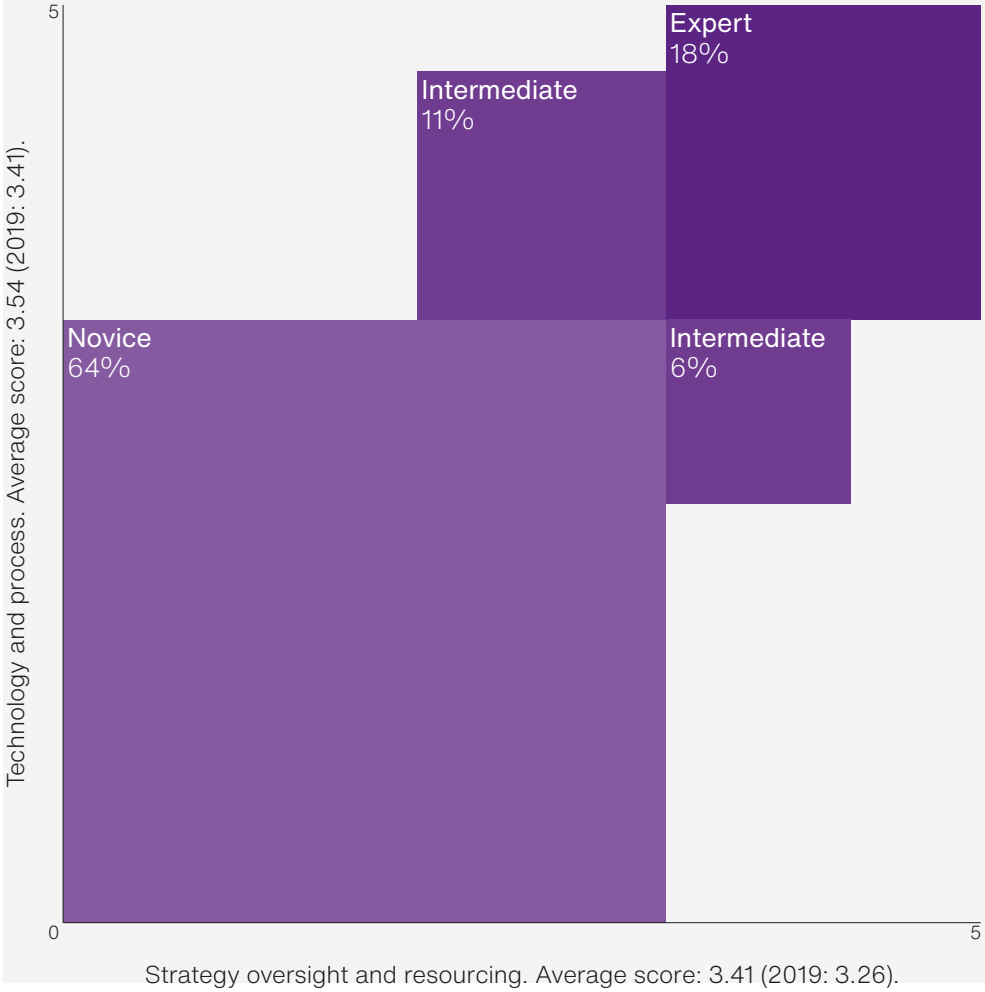
By contrast, nearly four out of five micro businesses with between one and nine employees (79%) ranked as novices. Across all respondents, the number saying their firm had 'no defined role' for cyber security increased from 16% to 20% (nearly half of micro businesses had no such role). The proportion using external service providers remained constant, at 19%.

2x

Number of businesses qualifying as experts has almost doubled in a year.

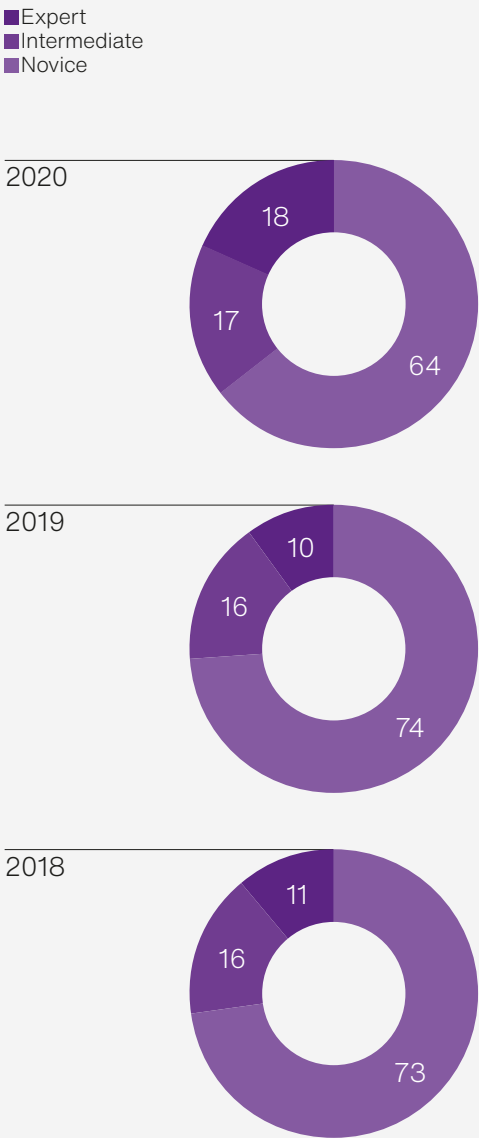
Cyber readiness model

Our cyber readiness model measures firms' alignment with best practice in four areas: strategy oversight and resourcing on one axis and technology and process on the other. Businesses that score four out of five on both axes are considered experts. Those that achieve that score on one axis only are intermediates. Those that do neither count as novices.



Cyber readiness year-on-year

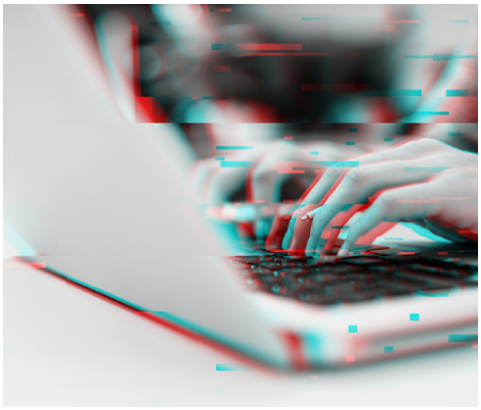
(%)



What can the experts teach us?

Do the basics well
Identify every device in the organisation. Back data up off-site and learn from each incident or breach. Experts are more likely to up their game following a breach through regular security evaluation, ensuring additional security and audit requirements are in place and increasing crisis management.

Follow a framework
Make sure that all the virtual doors and windows are shut. A framework such as the one created by the US National Institute of Standards and Technology built around five imperatives – identify, protect, detect, respond and recover – provides a useful checklist. On average, experts pursue twice as many initiatives in all five areas as novices.



Don't penny pinch
Cyber experts direct a larger proportion of their IT budgets to cyber security and more of them plan to lift spending in every cyber-related area in the year ahead. In simple terms: the more people a company devotes to cyber security, the more likely it is to rank as an expert.

Invest in training
Novices suffered more breaches resulting from successful phishing and malware attacks. Regular training to drive awareness throughout the workforce is vital. This is only partly an issue of resources. Nearly three quarters of the micro businesses ranked as experts intend to prioritise the roll-out of effective employee training in the coming year.

Get management involved
Nine out of ten experts agree that cyber security is a top priority for executive management. Only half of novices feel able to say the same. When it comes to priorities for the coming year, only a quarter of micro firms ranked as novices recognised the need to enhance executive management engagement in cyber security policies.

Build resilience
No business will ever be completely secure. But all can build resilience by preparing for a breach, testing for it and having the capability to respond quickly and effectively. A standalone cyber insurance policy helps build that resilience through certainty of cover and specialist expertise such as risk assessment, crisis management and training.

How some smaller firms got it right

There was a marked increase in the number of small and micro firms ranked as experts. Who were they and what did they get right? One in six of them (16%) were digitally savvy TMT companies, while retail and wholesale and construction were also well represented (11% and 10% respectively). Most appear to have achieved their expert status by taking cyber security seriously. Analysis shows they all took these three actions:

- engaged actively in cyber awareness training;
- deployed anti-virus or anti-malware systems consistently across the organisation;
- took decisions based on clearly defined business needs or cyber security tolerances.

Best prepared sectors

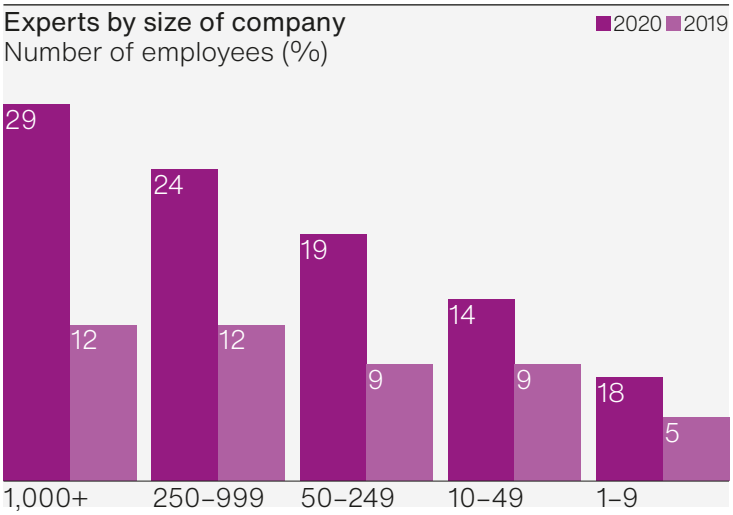
Overall, financial services and TMT firms were again in the top three (with 24% and 23% respectively ranking as experts) but they were joined this year by manufacturing (24%). Professional services, which saw losses rise nearly tenfold, emerged well below the average with only 14% of respondents ranked as experts. The explanation may lie in the fact the sector has a higher weighting to micro businesses than most. The food and drinks sector came bottom of the list, with only 7% of firms ranking as experts.

Did the experts fare better?

In general terms, the better prepared firms did much better than the novices. The latter were three times more likely to suffer a breach than the experts, with a median figure of 30 per firm compared with nine for the experts.

Experts by size of company

Many large and enterprise firms are among the experts but still experience high incident to breach ratios since bigger businesses offer more entry points, bigger gains to cyber criminals and are likely better at spotting breaches. Two in every five enterprise businesses rank as experts. while 60% of firms with fewer than 100 employees rank as novices.



One of the more striking findings is that almost one in five (19%) of the novices that suffered a cyber event found themselves paying a ransom. Smaller, more vulnerable firms are likely to be in the firing line and the less well prepared are clearly paying the price.

The Hiscox view

We commonly see two types of ransomware attack. The first is targeted attacks. These are focused on larger organisations (so called 'big game ransomware') where a hacker group will specifically target key individuals with highly personalised phishing scams. The second is mass scanning. This is where hackers will look for key weaknesses in servers exposed on the internet (e.g. remote access and VPN servers). In these cases, the attacks are mostly indiscriminate, and the attackers will infect any company they find vulnerable.

Building resilience

A host of indicators this year suggest the bulk of firms are taking the cyber threat more seriously than before.

Surge in spending

The report shows a dramatic and broad-based rise in cyber security spending over the past year – with an average spend among our respondents of $2.1 million, up from $1.5 million the previous year. That is a rise of 39%. It reflects both an increase in overall IT budgets and a 30% jump in the proportion devoted to cyber (9.9% to 12.9%). Enterprise-scale firms led the way.

French firms were once again the biggest spenders, lifting their cyber budgets from $2.1 million on average to $3.1 million. Spanish and US firms were close behind, at $2.6 million and $2.4 million respectively. The UK, historically a laggard in past studies, started to catch up – with average spend on cyber of $1.5 million compared with just under $900,000 the previous year.

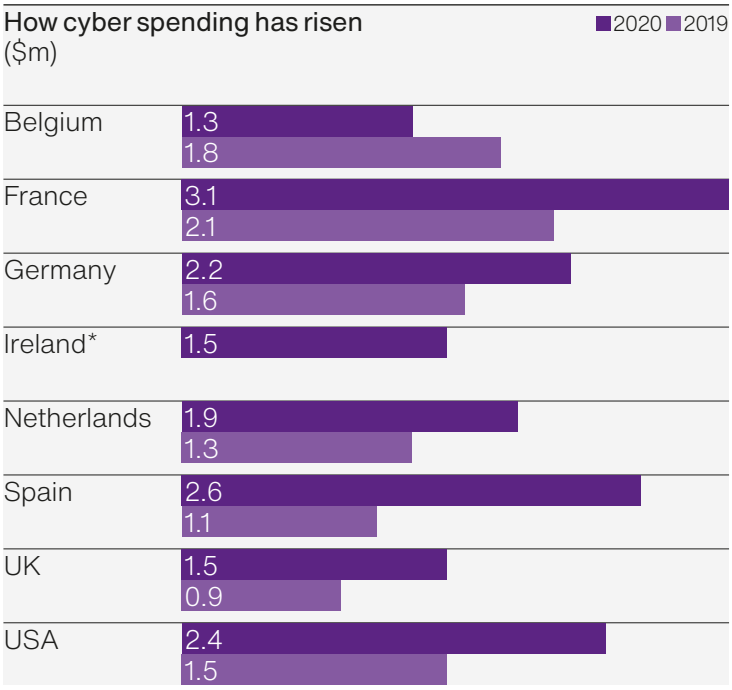
Just over three-quarters of respondents provided figures for their cyber security spending. Assuming they were representative of the total respondents, the total spend on cyber in the past year was a staggering $11.4 billion. That compares with $7.9 billion a year ago on a 3% smaller sample. Nearly three-quarters of firms (72%) intend to lift their cyber spending in the coming year by 5% or more. That is up from two-thirds (67%) a year ago.

How cyber spending has risen

The gap between the 'have's' and the 'have not's' is vast. The average micro business with less than ten employees spent around $13,000 on cyber security. The average enterprise firm spent $8 million. On average, the cyber experts plan to increase their budgets by just over 15% while the novices lift theirs by just under 12%. This suggests the gap between the best and the worst is set to widen.

Does high spending equate to cyber readiness?

The answer is not clear cut. On the one hand, firms that spent double-digit percentages of their IT budget were less likely to have experienced an incident or breach than those spending less than 5%. However, the big spenders, who were often larger firms, suffered higher average costs arising from breaches. Size brings more customers, higher notification costs and bigger ransoms.



*Data only available for 2020.

Identifying spending priorities in 2020
(%)

	Experts	Novices
Achieving or maintaining regulatory compliance	82	44
Addressing existing threat or vulnerabilities	81	44
Complying with security requirements placed on us by business partners	80	42
Ensuring business partners or third parties comply with our security requirements	79	40
Improving the security of customer-facing services or apps	78	40

It is also worth asking whether firms are directing their spending to the right areas. There has clearly been a shift of emphasis over three years. The proportion of respondents planning to increase spending on new cyber security technology has progressively fallen over that time from 57% in 2018 to 46% in 2020 while the number intending to invest more in employee awareness training has risen from 34% to 40%. More than a third (35%) plan to increase cyber security staffing, up from 26% two years ago.

Identifying spending priorities in 2020

Broader awareness

Once again, we asked respondents what their top priorities were for the year ahead, using the National Institute of Standards and Technology (NIST) cyber security framework: identify, protect, detect, respond and recover. Looking at the last three years there has been little change in the initiatives deemed most pressing. But the number of firms ticking them off has grown year-on-year, suggesting an increasing awareness of the need for a broad-based and active approach to cyber security.

Spending growth in each NIST category

Enthusiasm for these initiatives increases both by size of company and by maturity on our readiness model, The experts clearly have longer 'to do' lists. Four out of every five mentioned these top priorities for the coming year. They also put more emphasis on conducting cyber security assessments and on securing the internet of things.

A new urgency

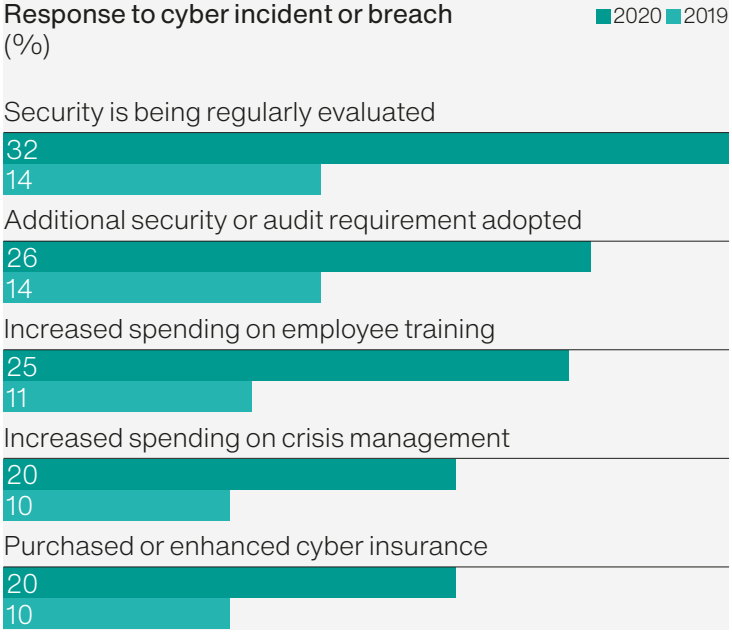
There is another indicator of a new determination to tackle the cyber threat. This can be seen in the way firms have responded to either a cyber incident or a breach in the past 12 months. Suddenly, businesses are acting with a new urgency. Typically, around twice as many firms say they have taken extra measures to combat the hackers as last year.

Response to cyber incident or breach

Spending growth in each NIST category
(%)

	2020	2019	2018
Identify	50	46	44
Protect	50	45	44
Detect	50	47	45
Respond	44	39	39
Recover	46	43	41

Response to cyber incident or breach
(%)



Experts ahead on cyber insurance

The proportion of respondents that have purchased cyber insurance cover as a result of a previous cyber incident or breach (not necessarily in the past year) has risen over the past three surveys from 9% to 20%.

This year, we amended the questionnaire to ask respondents if they have a standalone cyber policy (as opposed to relying on the cyber cover within a more general policy). Just over a quarter of firms (26%) said they had a standalone cyber policy and a further 18% said they planned either to purchase standalone cover or add it as coverage to their policies.

Do you have cyber insurance?

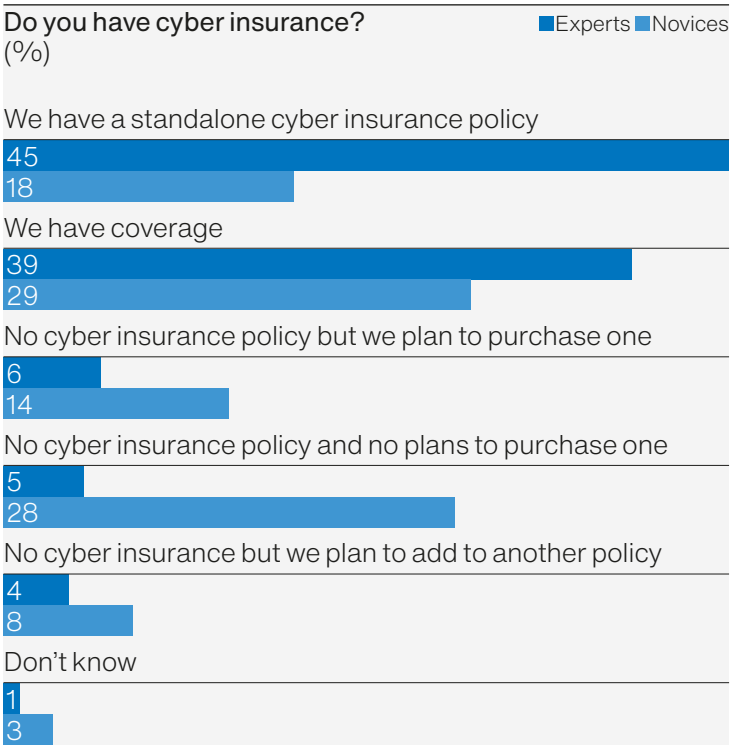
This is an area where the experts are clearly ahead of the game. Nearly half (45%) say they have a standalone cyber policy and 70% intend either to buy or enhance their cyber cover.

Adoption of standalone cyber cover rises steadily in line with size in our survey – from just 12% among micro businesses to 42% at the enterprise level. Apart from the very largest firms, most businesses rely on a more general policy, which may or may not cover them in the event of a serious breach.

Uptake of standalone cyber policies varies markedly between countries. Ireland comes top of the list, with 38% of firms saying they have specialist cyber cover. The USA (33%) and Belgium (30%) come close behind, while The UK (22%) and France (23%) sits at the bottom of the list.

The Hiscox view

As a cyber insurer, it is only natural that we would promote standalone cyber insurance. But it is important to point out that standalone cyber insurance is dedicated to getting businesses back up and running quickly after a cyber attack. Cyber insurance provides a range of services like IT forensic response, crisis communication, legal advice and, if necessary, credit card monitoring. Coverage in other policies rarely provides all these specialised services, and, in some cases, may not respond at all.



About this report

Hiscox commissioned Forrester Consulting to assess organisations' cyber readiness. In total 5,569 professionals responsible for their organisation's cyber security strategy were surveyed (1,000-plus each from the USA, UK and Germany; more than 500 each from Belgium, France, Spain and The Netherlands; and 300-plus from the Republic of Ireland). Respondents completed the online survey between December 2019 and February 2020.

The proportion of smaller businesses (fewer than 250 employees) has increased from 56% to 60%. Firms with up to nine employees account for 29% of the survey compared with 20% last year. Sole traders make-up 10% of the total, up from 5%. Large (between 250 and 999 employees) and enterprise companies (1,000-plus) continue to make-up a combined 40% of respondents.

We have adopted median rather than mean or average figures and restated prior-year figures in the same terms. Given the extreme variation in the underlying figures between the smallest and largest firms, this provides a more accurate representation of the respondents as a whole.

The full make-up of respondents is detailed below.

Level	%	Number of employees	%
C-level executive	31	1,000+	25
Vice president	21	250–999	15
Director	39	50–249	15
Manager	9	10–49	15
		1–9	29
Sector	**%**	**Department**	**%**
Business services	7	Executive management	13
Energy	4	eCommerce	2
Construction	8	Finance	8
Financial services	9	General counsel	3
Food and drink	4	Human resources	4
Government and non-profit	7	IT and technology	21
Manufacturing	8	Marketing and communications	3
Pharma and healthcare	9	Operations	10
Professional services	9	Owner	21
Property	4	Procurement	3
Retail and wholesale	9	Product management	4
TMT	16	Risk management	3
Transport and distribution	4	Sales	5
Travel and leisure	4		

Hiscox Ltd

Chesney House
96 Pitts Bay Road
Pembroke HM 08
Bermuda

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

hiscoxgroup.com/cyber-readiness

20647 5/20