HISCOX

Hiscox Cyber Readiness Report 2021

Don’t let cyber be a game of chance.

Cyber risk is too important to be left to chance.

One-in-six firms attacked in the past year said they almost went under. The threat is a complex one. But, like other business risks, it can be managed. The key is to build cyber resilience.

Find out how your firm's resilience measures up with our new maturity model at hiscoxgroup.com/cyber-maturity.

Managing the cyber threat

Businesses are devoting more resources to the cyber challenge than ever before.

Gareth Wharton
Cyber CEO, Hiscox

More firms targeted, often multiple times. This year's report underlines the scale of the cyber challenge. But it also offers good news. Despite the difficulties presented by the Covid-19 pandemic, firms have intensified their fightback by devoting more resources and focus than ever to cyber resilience. At the start of the pandemic, the majority of businesses put the simple need to carry on functioning ahead of everything else. The concern was that with IT budgets being squeezed, spending on cyber security would be cut. This report shows that was not the case. Spending on cyber has soared. Many firms have effectively moved their entire business online. As a cyber insurer, we know this has not only lifted awareness of the cyber challenge but moved the conversation about security to the forefront of decision-making.

The growing prevalence of ransomware should drive home the commercial relevance of good cyber security. Ransomware attacks are not just IT events; they are business-impacting on multiple levels. There is no doubt cyber security is a complex problem, but that doesn't mean it is unmanageable. Today the risk is too high and too tangible for businesses and individuals to leave it in the 'too difficult' bucket. There is a genuine chance that one attack will put the whole business at risk. One-in-six firms targeted in the past year said an attack had threatened the viability of their business. Simple, practical steps can lead to a level of cyber resilience whereby an attack is less likely. When one does occur, your business then has the training, tools, and financial protection to bounce back.

As an ex-CTO I was always asking 'what are our competitors doing?' and 'how do we compare?' With this year's updates, the centrepiece of the report is a new cyber readiness model that gauges respondents' strengths in six key cyber security areas across people, process and technology. It is designed to be an interactive model, so you can check and compare your business's maturity to other companies in your geography, sector and turnover band. The maturity model illustrates what cyber experts do in each area to help you plan and develop your cyber resilience.

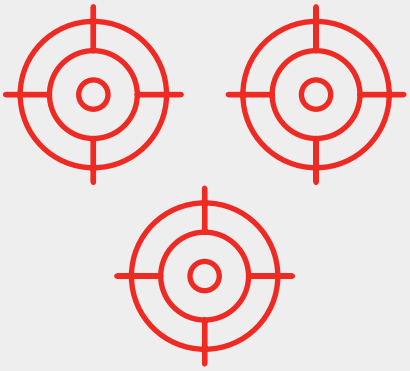
Our experience as an insurer has shown that consistent standards across all areas of security are essential if the hackers are not going find a way in. We hope it will give you a new perspective on your existing measures and perhaps highlight areas for improvement. The cyber threat is not going to go away, but, with good risk management complemented by appropriate cyber insurance, businesses can contain the impact and decrease the damage. We hope that this report contributes to firms' understanding of the cyber threat, provides a template for what best practice looks like and helps build the preparedness and resilience to deal with whatever challenge comes their way.

Executive summary

Firms focus IT spend on cyber resilience to manage increasing attacks.

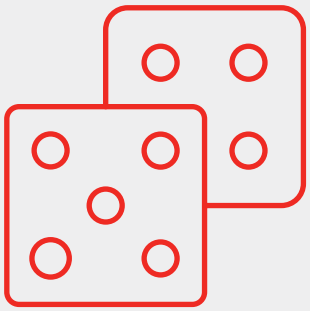
More firms targeted

The proportion of firms attacked rose from 38% to 43%. Many suffered multiple attacks.



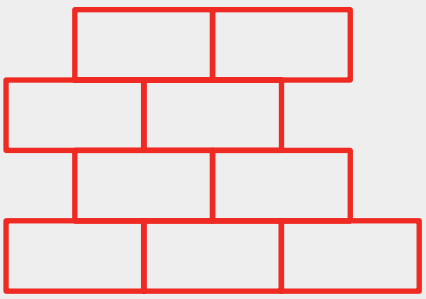
Frightening range of outcomes

Cost of attacks varies widely. One-in-six firms attacked says its survival was threatened.



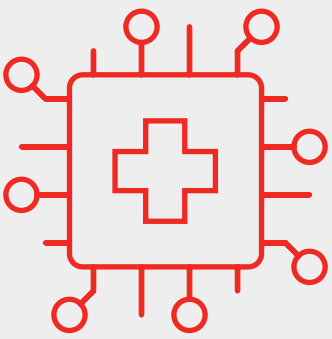
IT budgets reorient to cyber

The average firm now devotes more than a fifth (21%) of its IT budget to cyber security – a jump of 63%.



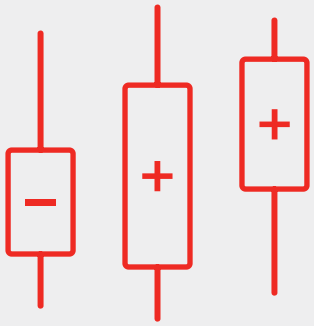
Ransomware now commonplace

Around one-in-six of those attacked was hit with a ransom and more than half (58%) paid up.



People, process, technology

Our cyber readiness model shows people scores are lower than for the other two areas.



Experts fared better

Firms qualifying as experts had fewer attacks, were less likely to pay a ransom and recovered more quickly.

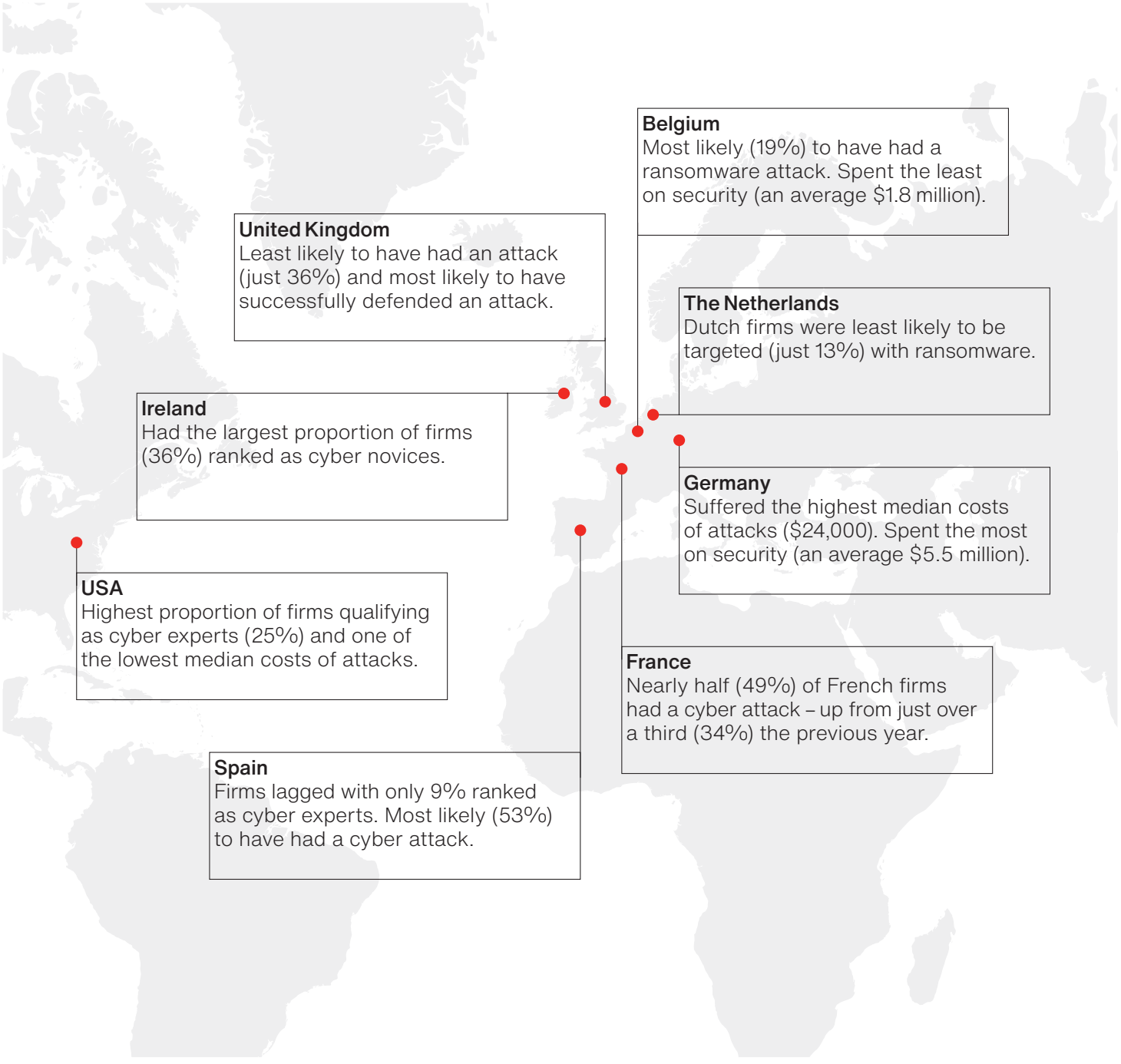
Insurance take-up slow

Take-up of standalone cover creeps up 1% to 27%; adoption highest among experts and big companies.

Big country variations

US firms top experts table, Spanish firms are most heavily targeted, Germans pay heaviest price.

Country comparisons



Belgium
Most likely (19%) to have had a ransomware attack. Spent the least on security (an average $1.8 million).

United Kingdom
Least likely to have had an attack (just 36%) and most likely to have successfully defended an attack.

The Netherlands
Dutch firms were least likely to be targeted (just 13%) with ransomware.

Ireland
Had the largest proportion of firms (36%) ranked as cyber novices.

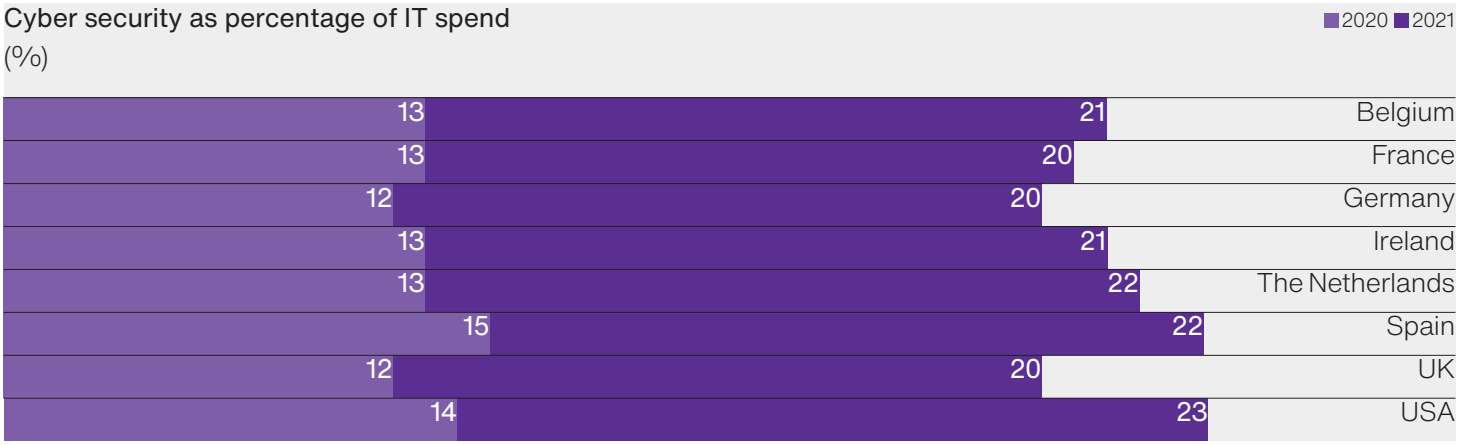
Germany
Suffered the highest median costs of attacks ($24,000). Spent the most on security (an average $5.5 million).

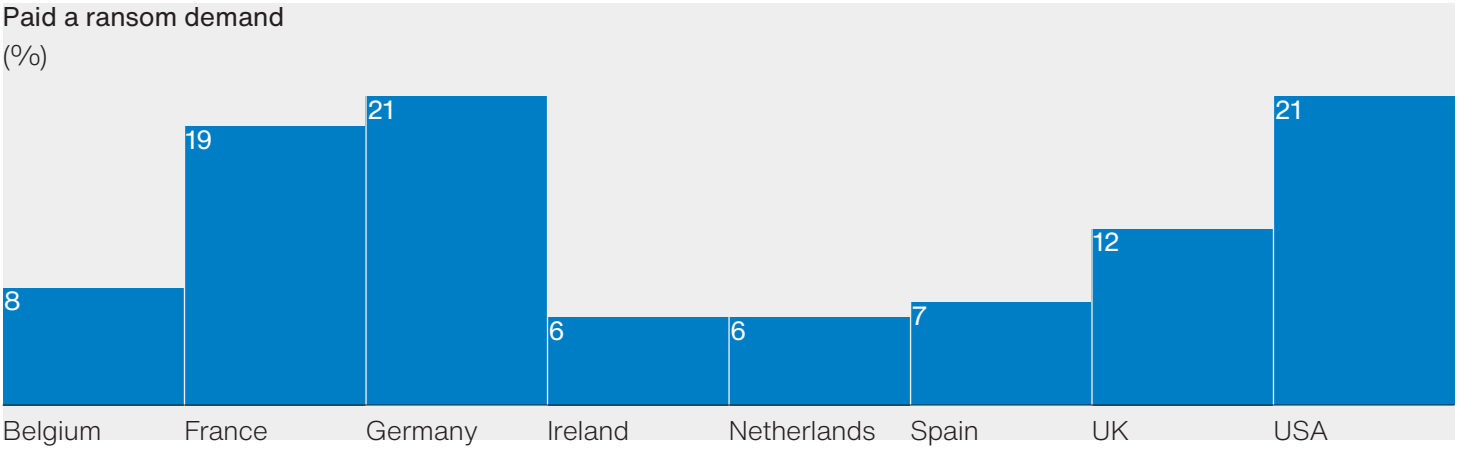
USA
Highest proportion of firms qualifying as cyber experts (25%) and one of the lowest median costs of attacks.

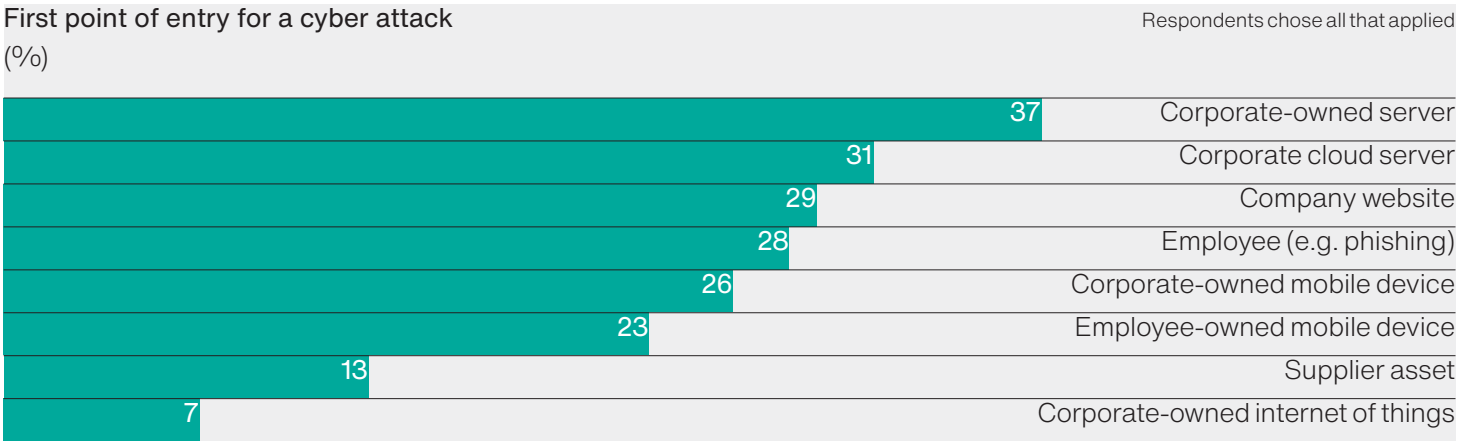
France
Nearly half (49%) of French firms had a cyber attack – up from just over a third (34%) the previous year.

Spain
Firms lagged with only 9% ranked as cyber experts. Most likely (53%) to have had a cyber attack.

By the numbers







Size of the problem

Many more firms report cyber attacks as the intensity increases in key target sectors.

There was a sizeable increase in the proportion of firms reporting one or more cyber attacks in this year's survey, with the hackers focusing their efforts on three or four sectors in particular and many more big firms.

Who is being attacked?

The proportion of respondents reporting attacks jumped from 38% in 2020 to 43%. The hackers' favourite targets were the technology, media and telecoms (TMT), financial services and energy sectors. The percentage of firms affected in these sectors was typically up from the low-to mid-40s in our 2020 study to the mid-50s (see Fig. 1).

This year, too, there were many more big firms in the firing line. As past surveys have noted, the probability of being targeted rises sharply according to size of firm. This year there was a much steeper curve – from 23% for the smallest to 61% for enterprise firms (those with 1,000-plus employees). Last year, the equivalent figures were 31% for the smallest and 51% for enterprise firms.

Overall, Spanish companies were most likely to report a cyber attack (53%). Nearly half of all French respondents (49%) reported an attack, up from 34% the previous year. By contrast, only 36% of British firms reported being targeted.

Large numbers suffer multiple attacks

More than a quarter (28%) of firms that suffered cyber attacks were targeted more than five times in the past year (see Fig. 2) Nearly half (47%) of enterprise-scale firms that were attacked found themselves fending off the hackers six times or more. A third (33%) had to do so more than 25 times. More than a fifth (22%) of French and German firms that were targeted were in the 25-plus bracket.

Fig. 1. Top five sectors reporting attacks
(%)

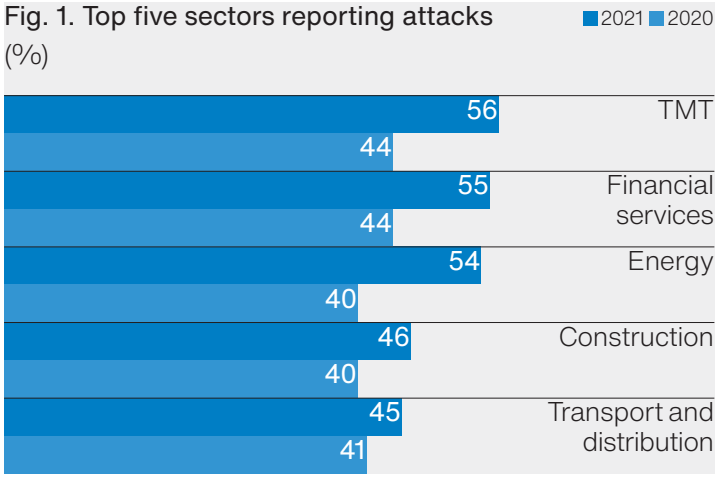


Fig. 2. Number of attacks in past year
(%)

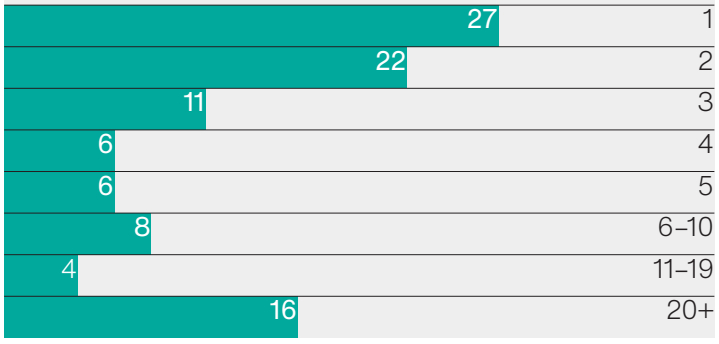
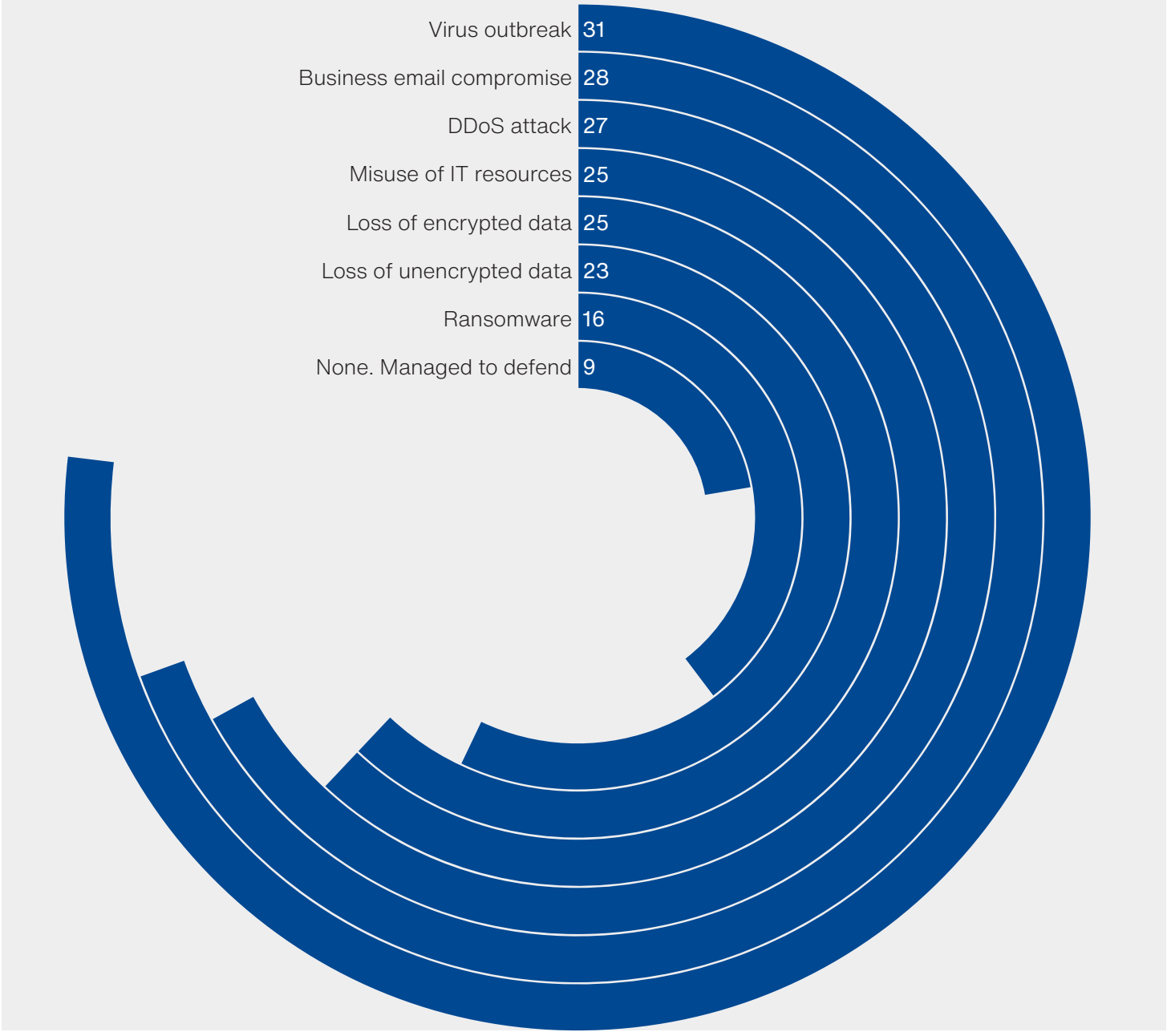


Fig. 3. Outcomes of cyber attacks

(%)

Respondents chose all that applied.



The Hiscox view

The prominence of larger firms among the multiple targets begs a question: are they just better at picking up attacks? It is also noticeable that firms that qualified as either cyber intermediates or experts in our cyber readiness model were more likely to report multiple attacks. In 2020, we saw businesses of all sizes moving online and moving staff to remote working. Open remote desktop protocol (RDP) ports were responsible for 61% of Hiscox ransomware claims in 2020. These are some of the reasons for multiple attacks.

Firms had to deal with a wide range of attacks

Three-in-ten targeted firms (31%) had to deal with a (non-ransomware) virus infection, 28% with payment diversion fraud arising from business email compromise and 27% with a DDoS attack (see Fig. 3). German, French and US firms were most likely to suffer these outcomes.

A remarkable 39% of US firms had to deal with IT resource misuse – such as hosting malware or having the infrastructure hijacked to mine cryptocurrency – compared with just 25% overall.

Looking for the open window

Leave a door unlocked or a window on the latch and the burglars will find it. Asked to name the first point of entry for the hackers, 37% of respondents mentioned their corporate-owned servers. Cloud-based servers came second (mentioned by 31%), followed by company websites (29%) and employee error such as phishing or spoofing (28%). The previous year, phishing was the clear number one issue, mentioned by 45% of respondents. This year's survey offers respondents a greater range of answers.

But there are some big variations by sector. While professional services, construction and financial services firms were particularly likely to cite the corporate server as the point of entry, businesses dealing with the public, particularly retail/wholesale and energy, were more likely to have suffered a breach via the company website. Company owned mobile devices, mentioned by just over a quarter of all firms attacked (26%), appear to be areas of particular vulnerability for more mobile industries such as transport/distribution and travel/leisure (mentioned by 32% and 30% respectively).

Small businesses in the 10-to-49 employee range appear especially susceptible to server vulnerability or credential compromise (mentioned by 41% vs 37% average) but it is striking that enterprise firms also feature heavily in each area. The data suggests that investment in a sophisticated website may be counter-productive: the biggest companies in our study group are much more likely to have suffered an attack via the website (such as a DDoS attack).

Companies ranked as experts appear to have experienced the same vulnerabilities. Remarkably, 44% of the experts mentioned their corporate owned server as a first point of entry for the hackers, compared with 37% for the study group as a whole. The company website is also mentioned by 36% of experts.

German firms have some work to do in nearly all these areas. For instance, 44% and 41% said a corporate owned server or cloud server (either involving direct vulnerability of the server or credential compromise) provided the first point of entry for the hackers. US firms also appear to have been particularly vulnerable in most of these areas.

Fig. 4. Range of cyber attack costs
By number of employees
($000)

Financial costs

A wide range of outcomes gives the cyber threat added menace. It is easy to overlook the full import of data relating to cyber attack costs. If one only looks at average or median figures, the financial impact may appear containable. But behind those figures is a range of outcomes that should send a chill down any CEO's spine. The striking thing to note from the chart (see Fig. 4), is the sheer range and unpredictability of incident outcomes for every size grouping in our study.

Taking all cyber attacks experienced over the past 12 months, the chart shows both the median cost and the cost for the 95th percentile of each size grouping.

While the median costs may look manageable, it is worth remembering what the median represents. It is the midway point. While half of those targeted will have suffered cyber costs up to that figure, the other half will have suffered more costly breaches. What the chart shows is that those costs can be two, three or even four orders of magnitude higher.

Small firms feel the pain

Smaller firms were prominent among those suffering the largest losses relative to size of business. For micro firms with under ten employees, the median cost of all attacks this year was just over $8,000. But at the 95th percentile and beyond there were firms suffering losses of $308,000. Some encountered still worse outcomes. One German business services firm experienced breaches costing the equivalent of $474,000 per employee.

At the opposite extreme, half of enterprise-scale firms managed to contain their cyber attack costs at under $24,000. But, at the 95th percentile, they were experiencing losses nearly 40 times that level. The impact of this cannot be overstated. One-in-six of all firms attacked this year (17%) said the impact was serious enough to 'materially threaten the solvency or viability of the company'.

German firms again stand out for the severity of attacks. They accounted for more than a third of the total financial impact ($47.9 million) with half of that arising in two sectors: retail/wholesale and pharma/healthcare. German firms also topped the table for the median cost of all cyber attacks ($23,700) and the single largest attack ($5.1 million). At the opposite end of the spectrum, Irish firms suffered median costs of just $8,300.

The data on costs come from the 1,709 firms that tracked the cost of cyber attacks. Encouragingly, the numbers that measure the impact are creeping up. More firms say they can now 'clearly measure the business impact of security incidents that disrupt their business' – 60%, up from 54% last year and 51% the year before.

Happily, the hackers do not always have things their way. Some 9% of respondents (and 11% of experts) said they managed to repel or remediate all the attacks thrown at them before they caused damage. UK firms were best at this (13%), US firms the worst (just 6%). But it is worth noting that there are still significant costs involved in a successful defence or remediation. Overall, the median cost was only marginally less than for a successful breach. There is no free lunch.

Brand reputation on the line

The effect of a serious breach goes well beyond the immediate financial costs. Nearly a quarter of firms that were attacked (23%) cited bad publicity and its impact on the company's brand and its reputation. That is a sharp increase on the 14% who said the same last year. Not surprisingly, enterprise-scale firms, many of which have global brands, were most likely to report a reputational impact.

$7.3m

Total amount paid by 241 companies that paid a ransom.

Firms dealing with the public topped the list of those affected (28% of travel and leisure firms and 25% of food and drinks businesses). Increased cost associated with notifying customers was similarly mentioned by 23% of respondents. It may be relevant that one of the top tasks the experts have set themselves this year is 'improving the security of customer facing services and applications'.

More than one-in-ten firms targeted (11%) paid 'a substantial fine that had a significant impact on the financial health of the business'. In the USA, the figure was 18%, suggesting tough regulations in key states involving penalties for privacy breaches, like the California Consumer Privacy Act (CCPA),are having an impact. The number saying they lost customers jumped from 11% to 19%. Nearly as many (18%) said they had greater difficulty attracting new customers, up from 15% the previous year.

Ransomware: just over half pay up

Around a sixth of firms (16%) reporting cyber attacks had to deal with a ransomware demand. Belgian and German firms were most likely to be targeted (19%), Dutch firms least likely (13%).

Just over half of those targeted (58%) paid a ransom – either to recover data or to prevent publication of sensitive information. The most fruitful territory for the ransom specialists was the USA, where 71% of those targeted paid up (the proportion in Ireland was higher, at 75%, but on a sample of just 20 firms, it's not statistically significant). Spanish firms were least likely to pay up – just 44% of them did so.

The 241 companies that did pay a ransom handed over a combined $7.3 million. The median amount paid in ransom was $11,900 and the largest single payment was $94,900, paid by a German entity. A French firm was only a few Dollars behind. A quarter of the companies paying a ransom were TMT firms.

Fig. 5. Methods of entry for ransomware attacks
(%)

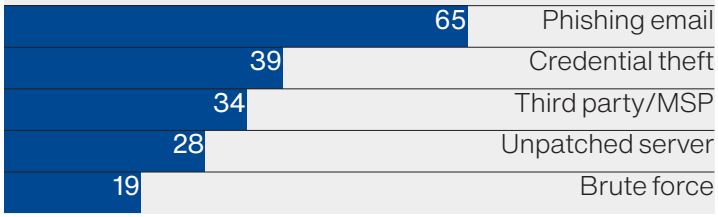
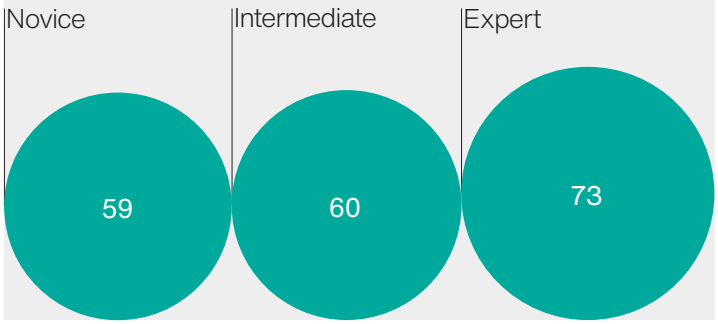


Fig. 6. Back to normal within a week
(%)



The Hiscox view

There's no doubt ransomware is the scourge of doing business online. Businesses of all sizes regularly fall prey to ransomware gangs. However, as our research shows, experts fare best when attacks happen. They had less ransomware attacks, fewer fell victim to phishing emails, and when they were hit recovered more quickly. At Hiscox we take ransomware incredibly seriously. It is important that an insurer's proposal forms are aimed at promoting good protection against ransomware, thereby encouraging customers to improve and maintain their cyber resilience.

The amount of ransom paid was only part of the story. For the first time we asked respondents to gauge the costs involved in recovering from both the largest single ransomware attack and all ransomware attacks in the last 12 months. The results were quite shocking: typically, recovery came close to doubling the financial impact, accounting for 45% of the total costs (ransom and recovery combined).

More than 60% of the firms paying ransoms were clustered in three countries: USA (21%), Germany (21%) and France (19%). Germany shared top spot with Belgium for the number of firms reporting one or more ransomware attacks (19%).

Small firms fall prey to phishing

Phishing emails were the number one way in for the extortionists. Almost two-thirds (65%) of ransomware victims mentioned this method of entry – still more in The Netherlands and Germany (76% and 74% respectively). Smaller companies fell prey to phishing more often than the rest. Some 74% of firms with fewer than ten employees targeted with ransomware mentioned this point of entry. That compares with just 65% among the biggest firms in our study (see Fig. 5).

Credential theft and third-party supplier (or managed service provider) were the next two most cited pathways, mentioned by 39% and 34% of victims. US firms appear to have been particularly vulnerable to entry via a third-party supplier/MSP, unpatched server or credential theft.

Having found a lucrative target the hackers often return for more. Just under 200 firms found themselves paying the extortionists more than once. Some 76 firms paid between three and five times, while 14 paid five times or more. One-in-four firms (27%) paid three times or more to recover data and one-in-five (22%) paid three times or more to prevent publishing of sensitive data.

How well did the experts fare?

Generally, very well. They were less likely to have to deal with ransom demands (13% of them compared with 16% for novices and 17% for intermediates) or fall victim to phishing emails (56% of them compared with an average 65% across all companies targeted with ransomware).

They were also less likely to have paid a ransom, suggesting they often had the expertise to deflect a ransomware attack or remediate afterwards. Just over half of targeted experts (54%) paid up compared with two-thirds (68%) of novices. The experts were also likely to recover more quickly (see Fig. 6).

However, taking into account all cyber attacks, the experts suffered as big a cost hit as the novices and intermediates combined, despite making up only 20% of our study group. This, however, is the large company effect. Just over half of all cyber experts are enterprise firms and they constitute the biggest targets, suffering the biggest breaches.

However, the experts were not always on their game: they were more likely to let ransomware attacks in via an unpatched server (mentioned by 38% of experts compared with 28% on average) or brute force server credentials where the hackers simply run through number sequences or popular passwords (25% compared with 19% on average).

Cyber readiness model

Firms are strong in a number of technology areas but weaker on personnel.

As cyber risks evolve, so too must the way in which we measure preparedness and resilience. For the first time since the inception of this report, we've revaluated what it means for a business to be an expert in cyber security. Our new model is a maturity assessment of not just preparedness, but also whether a business is resilient at managing attempts and attacks.

Our cyber readiness model has two dimensions. Each question is designed to quantify a firm's capabilities across six operational areas within cyber security (termed 'domains') in relation to a particular 'function', such as people, processes, or technology. The combined view across the two dimensions provides a composite picture of cyber maturity (see Fig. 7).

As part of the process, it highlights specific areas of strength or weakness. Many are surprisingly consistent across countries and industries – underscoring lessons that many businesses need to take on board.

Only one-in-five firms (20%) qualifies as an expert (a slight advance on the model used in previous years). Half of firms sit in the middle bracket of intermediates. Novices make up the remaining 30%.

USA leads the way

US firms emerge best with the highest proportion of experts (25%) and the lowest proportion of novices (27%), although they lag their German and French counterparts on overall average scores. Interestingly, the strong showing of US firms is reflected in the lowest median cost of attacks. Spanish firms are some way adrift, with only 9% of firms emerging as experts and 35% ranked as novices. They rank bottom of the table in all company size groupings.

The UK is something of an enigma. While ranking second to the USA for the proportion of experts (23%), its micro businesses (1-9 employees) fare worst of all eight countries – with 62% coming out as novices. The smallest firms in Spain and Ireland were also marked down, with 58% ranked as novices.

In terms of sectors, TMT has the highest proportion of experts (25%), overtaking financial services and manufacturing which led last year (see Fig. 8). It may be no coincidence that the top three industries (TMT along with energy and financial services) are also the three most heavily targeted. At the other end of the scale, professional services, travel/leisure and business services have the highest proportions of novices (41%, 41% and 39% respectively).

Not surprisingly, the distribution of experts is heavily weighted to larger firms, though there is little difference in readiness scores between firms in the large (250-999 employee) bracket and enterprise firms with 1,000-plus. The highest proportion of experts is to be found among US enterprise-scale and large businesses (36% and 35% respectively). UK enterprise businesses come next (33%). Globally, more than half (53%) of firms with under ten employees come out as novices as do a third of those in the 10-49 employee bracket.

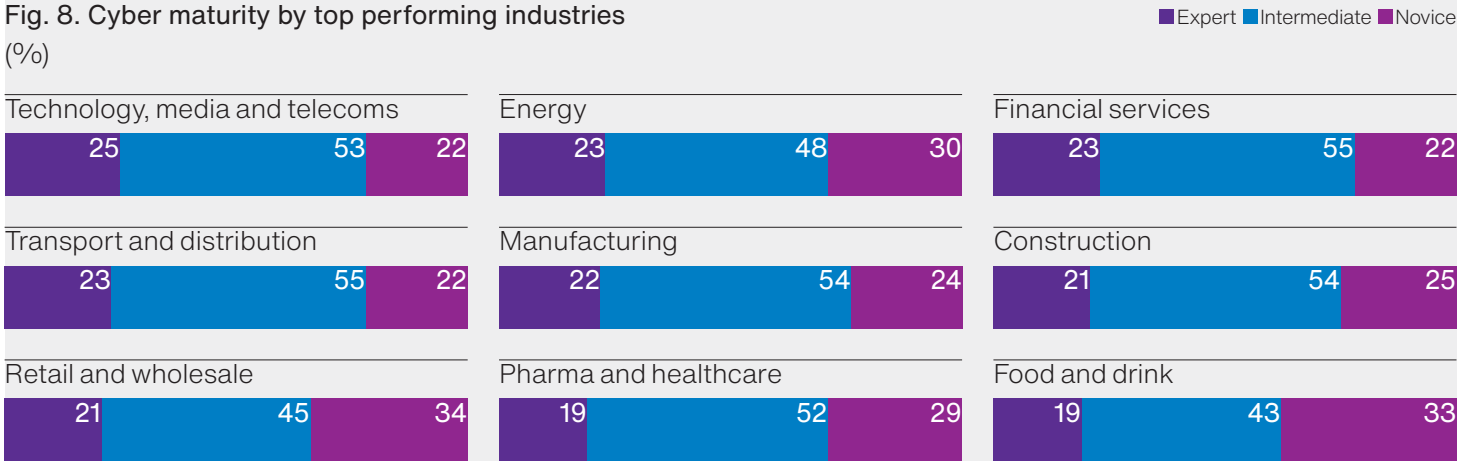
Fig. 7. Cyber maturity model

Our maturity model assesses a firm's maturity across six different areas of capability (domains) using the COBIT® measurement framework and the SABSA® security architecture. The six domains make up all the elements required to install, run, manage and govern an effective security system. Each domain is measured against one of three functions – people, process, and technology. The scoring system marks firms out of five, and any score over four qualifies the firm as a 'cyber expert'. Between 2.51 and 3.9, they qualify as 'cyber intermediates'. Below 2.5, they rank as 'cyber novices'.

	People	Process	Technology	Total average
Business resilience management	3.12	3.13	3.10	3.12
Cryptography and key management	2.93	2.90	2.94	2.93
Identity and access management	3.05	2.95	2.94	2.97
Security information and event management	2.93	3.10	2.99	2.99
Threat and vulnerability management	3.00	3.12	3.28	3.13
Trust management	3.07	3.05	3.09	3.07
Total average	3.02	3.04	3.06	3.03

Fig. 8. Cyber maturity by top performing industries

(%)



64%

Respondents who are 'very confident' of their cyber security readiness.

What the model tells us

Using overall cyber readiness scores (see Fig. 10), the model highlights a dramatic gulf between the experts and the rest with an average of 4.36 for the experts and just 1.72 for the novices. When it comes to analysing where firms' strengths and weaknesses lie, the breakdown between domains and functions is instructive.

Domains

Two domains stand out as relative strengths: threat and vulnerability management and business resilience management (where firms scored an average 3.13 and 3.12 respectively). German firms had the best scores here, with French and US firms close behind. Spanish firms scored the lowest – as they did in all domains. Scores rise in line with size of company though, and they level off once the 250 employee mark is reached.

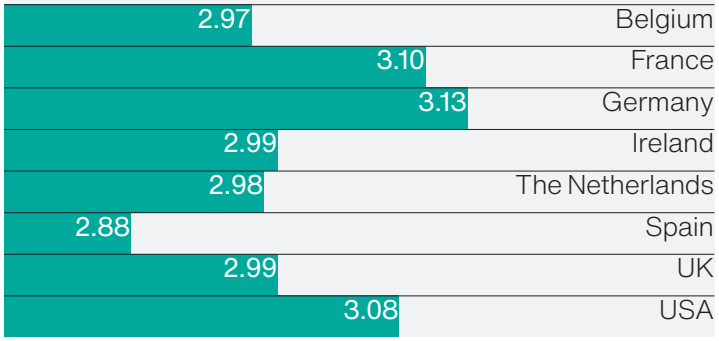
Taking all six domains together, there were three stand out sectors. TMT scored highest, as might be expected, but financial services and transport/distribution were only narrowly behind. Professional services fared worst.

Numerous firms were let down by poor scores in cryptography and key management (travel and leisure, business services and professional services in particular) and to a lesser extent identity and access management. This is a concern. Cryptography is foundational to every modern IT system and central to every other control.

Functions

On the function side, the model scores firms' cyber security operations in three areas – people, process and technology. Broadly, the lowest scores are in the first of these areas, suggesting many firms have work to do to recruit and train suitably qualified and experienced people.

Fig. 9. Composite readiness scores



As is to be expected, levels of expertise generally increase in line with the size of business. The smallest firms, with fewer than ten employees, are a long way adrift but many lack the ability to employ a specialist in this area.

Once again, it is German and French firms setting the standard, with the US not far behind. Spanish firms prop up the table, with a particularly low score in technology (see Fig. 9). As with the domains, the TMT sector comes top, though both financial services and transport and distribution score more highly for process.

Interestingly, given a year in which the numbers hit by cyber attacks has risen, a greater proportion of respondents say they are 'very confident of their cyber security readiness' – 64% up from 62% the previous year and 57% the year before that. A great gulf remains between the experts, 84% of whom express confidence in their readiness, and the novices (just 43%).

The Hiscox view

Not surprisingly, some more established cyber security practices score higher. For example, backups and disaster recovery within 'business resilience management' and practices such as firewalling an anti-virus in 'threat and vulnerability management'. Scores also highlight a general weakness in 'cryptography and key management', where even the experts tend to do poorly. This is a common problem. Among the most complicated areas to master, cryptography suffers a noted skills shortage.

Fig. 10. Cyber readiness scores

Cyber novices	People	Process	Technology	Total average
Business resilience management	1.83	1.86	1.75	1.81
Cryptography and key management	1.58	1.54	1.52	1.55
Identity and access management	1.80	1.71	1.63	1.69
Security information and event management	1.57	1.90	1.61	1.65
Threat and vulnerability management	1.65	1.85	2.24	1.91
Trust management	1.76	1.71	1.72	1.73
Total average	1.70	1.76	1.74	1.72

Cyber experts	People	Process	Technology	Total average
Business resilience management	4.44	4.43	4.43	4.43
Cryptography and key management	4.29	4.25	4.34	4.29
Identity and access management	4.37	4.29	4.38	4.34
Security information and event management	4.32	4.34	4.38	4.35
Threat and vulnerability management	4.34	4.36	4.29	4.33
Trust management	4.37	4.37	4.46	4.41
Total average	4.35	4.34	4.38	4.36

What the experts can teach us

Share the risk

It is impossible to guarantee total security. But having the ability to respond quickly and effectively, and draw on outside expertise when the chips are down, locks in resilience. This is what the experts do. Nearly half (47%) said they have a standalone cyber policy, up from 45% last year. Among novices, only 11% now say the same, down from 18% last year.

Make someone responsible

Many firms are too small to be able to justify an in-house cyber specialist but that is no reason for failing to give someone responsibility for cyber security or appointing an external service provider to do the job. Nearly half (48%) of firms with under ten employees and 45% of novices said they had no defined role for cyber security.

Deal with key vulnerabilities

Seven-in-ten experts see the move to remote working as increasing their vulnerability to attack. Only 40% of the novices agree with them. The experts' number one priority for this coming year is to address existing threats and vulnerabilities. That is mentioned by nearly three-quarters of experts (74%). They are telling us something here.

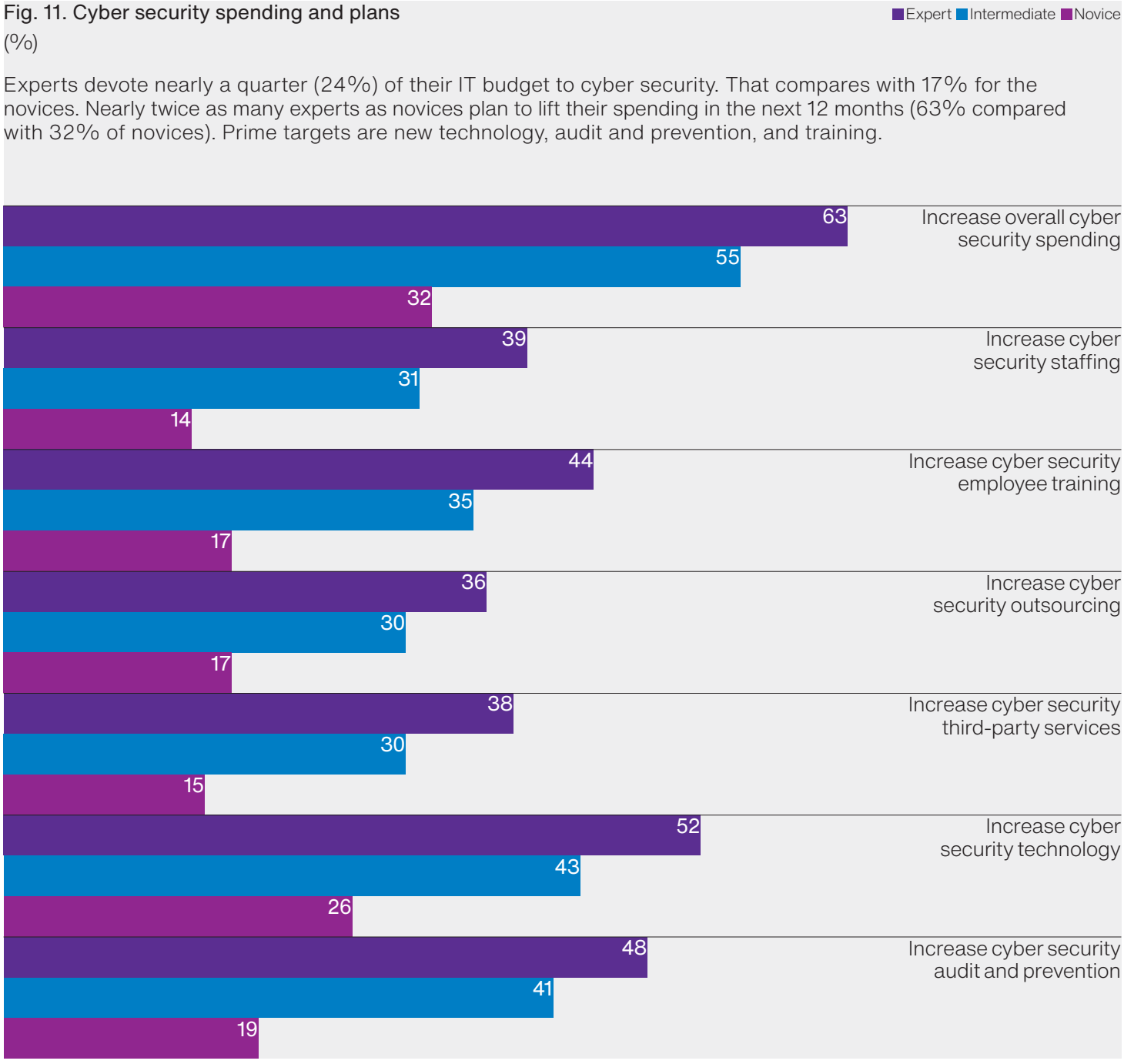
Back-up, preferably off-site

The experts were more likely to repel all attacks before they did damage. One-in-seven (14%) said ransomware attacks had no financial impact. One reason was they were more likely to be in a position to recover their data. Nearly two-fifths (39%) of them did so three or more times last year. Doing the basics, such as backing up all data and preferably off-site, is vital.

Fig. 11. Cyber security spending and plans

(%)

Experts devote nearly a quarter (24%) of their IT budget to cyber security. That compares with 17% for the novices. Nearly twice as many experts as novices plan to lift their spending in the next 12 months (63% compared with 32% of novices). Prime targets are new technology, audit and prevention, and training.



Building resilience

Cyber security spending now claims a much bigger share of IT spend as firms step up their counter measures.

Businesses have radically reoriented their IT budgets in the past year. While mean spending on IT is little changed overall, the proportion devoted to cyber security has increased by a remarkable 63%. The average firm now devotes more than a fifth (21%) of its IT budget to cyber – up from 13% the previous year. This marks a big change in attitudes.

Given the heavy weighting towards small firms, the overall rise in cyber spending across our study group is a more modest 25% – from $11.4 billion to $14.3 billion or 23% after adjusting for the increase in the number of respondents from 4,313 to 4,412.

On average, German firms spent the most on cyber security at $5.5 million, an increase of 155% on the previous year – perhaps a recognition of their apparent vulnerability exposed elsewhere in this report. Belgian firms spent the least ($1.8 million).

Across the different sectors, energy firms were the top spenders with an average spend on cyber security of $13.4 million. Financial services came next ($5.6 million on average), followed by manufacturing ($5.4 million). Travel firms spent the least ($711,000), but that may reflect the fact that many went into hibernation with the onset of the pandemic.

The fastest growth has come from opposite ends of the corporate spectrum, the very smallest and the very biggest (see Fig. 13). Firms with between 10 and 49 people have also lifted spending more than tenfold – to $395,000. At the opposite extreme, enterprise firms are now spending an average of $13 million, up from $4.2 million two years ago. But in terms of spending per employee they are still a long way behind the rest, suggesting the biggest firms have the capacity to lift spending still further.

The surge in spending looks set to continue, albeit at a slightly less exuberant pace. At the individual company level, the planned spending increase for the year ahead averages 51%. That compares with 72% the previous year, which proved to be pretty accurate.

Fig. 12. Mean cyber spending per firm

($m)

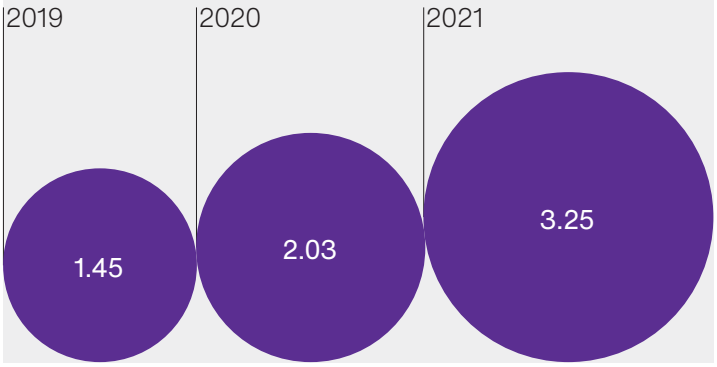


Fig. 13. Mean cyber spending
By number of employees

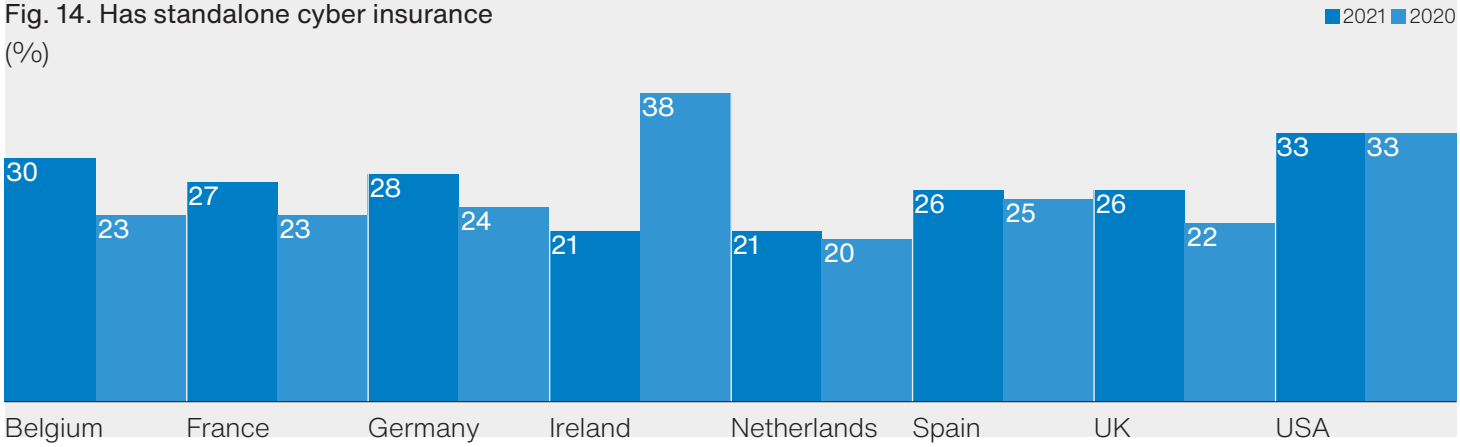
($)

	2021	2020
1–9	123,700	13,299
10–49	395,075	79,422
50–249	318,339	248,472
250–999	1,927,095	862,818
1,000+	13,063,690	8,029,026

The Hiscox view

In 2020, businesses were forced to work remotely overnight, move their physical presences online and engage with customers in a completely different channel. This digital transformation created some new business opportunities, but also left IT teams running change programs without any previous experience or in-house expertise. A benefit to the sudden shift online was recognising the importance of building cyber resilience and thus and increase in cyber security spend. Attacks, impacts and cyber security focus do, however, differ by industry, so some will be better prepared at managing dramatic changes in the future.

Fig. 14. Has standalone cyber insurance



Where is the money being spent?

Two-in-five firms (40%) say they plan to lift spending on cyber technology by between 5% and 10% while 36% say the same in regard to cyber security audit and prevention. For all that, the number of businesses mentioning increased spending on staffing and training is down (from 35% to 27% in staffing and from 40% to 32% in training). This seems unfortunate given the relative weaknesses in the people segment of our cyber readiness model.

It is also noticeable that fewer firms are taking decisive action following a breach this year. Among those who have been attacked, the proportion saying security and/or privacy are regularly evaluated is down from 32% to 19%, while the number putting in additional cyber security/audit requirements is down from 26% to 20%.

A mixed picture for cyber insurance

Adoption of cyber insurance is creeping up – both through standalone policies (27% now have one, up from 26%) or another policy (34% compared with 32% last year). The number of firms planning to purchase a standalone policy has risen marginally, from 11% to 12%, while the proportion planning to add cyber insurance coverage to an existing policy as remained static, at 7%. The numbers saying they do not have cover and do not plan to purchase it have gone down (18% compared with 21% last year).

Adoption of a standalone policy is highest among firms of 250 or more employees (36% for firms with 250-999 employees and 38% for enterprise firms). Getting through to the smallest firms remains challenging: nearly half of those with under ten employees (44%) say they have no intention of buying insurance cover. Given the evidence elsewhere in this survey that smaller firms are vulnerable to phishing attacks and credential theft – and the potential for crippling losses well beyond the median – this is disturbing.

US firms continue to lead in this area (see Fig. 14). A third (33%) have standalone cover; Belgian firms come second in the table at 30%. Irish, Spanish and German firms are most likely to say they are covered as part of another policy (43%, 37% and 36% respectively).

Two sectors stand out: financial services and TMT. Among the former, 39% have a standalone cyber policy while 37% have coverage as part of another policy. In TMT, the equivalent figures are 34% and 37%. Manufacturing firms are most likely to rely on another policy (42%).

46%

Average increase in percentage of staff who are working remotely due to Covid-19.

Gulf in perception on Covid-19 impact

Given the publicity accorded to Covid-related phishing and the shift to home working, it may surprise that understanding of the added threat posed by the pandemic is patchy. Less than half of respondents (47%) say their organisation 'has been more vulnerable to cyber attack since the start of the pandemic' – though the figure rises to around 59% among firms with 250 or more employees. There is a clear gulf in perception among the smallest firms where less than a third (30%) recognise their increased vulnerability.

Overall, levels of remote working have risen sharply. The average business in our study group has increased the percentage of its workforce working remotely from 14% to 60%. Two-in-five (41%) say they have increased the number of staff working remotely, while 29% have upped their use of cloud-based technologies and 32% are employing more collaborative technologies. In each case, the percentage rises in line with the size of business.

There is more concern on the specific issue of home working. Nearly three-in-five firms (58%) agree that 'because more employees are working from home, my organisation is more vulnerable to cyber attacks'. Again, the perception is more widespread among the bigger firms (verging on 69% for firms with 250 employees or more).

The bigger firms are also more likely to have acted to limit their increased vulnerability: more than two-thirds of both enterprise firms and those with over 250 employees say they have reinforced their cyber defences (68% and 67% respectively). For the smallest firms, with up to nine employees, the equivalent figure is just 35%. The figures suggest there is still a wide swath of firms, and not just the smaller ones, that have yet to take on board the added vulnerability remote working entails.

Fig. 15. Increased cyber security due to Covid-19
By number of employees
(%)

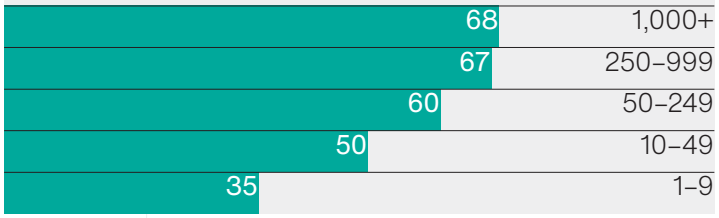


Fig. 16. Changes due to Covid-19
(%)

Increased number of staff working remotely	41
Paused hiring	33
Increased use of collaboration technologies	32
Reduced operating costs	31
Increased use of cloud-based technologies	29
Expanded online payments	27
Accelerated digital transformation plans	27
Expanded existing e-commerce channels	20
Reduced volume of IT changes	18
Added new e-commerce channels	18
Consolidated or reduced number of suppliers	15

Respondents chose all that applied.

The fifth annual Hiscox Cyber Readiness Report has been compiled in collaboration with Forrester Consulting. The report provides an up-to-the-minute picture of the cyber readiness of organisations, and 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 6,042 organisations across eight countries by size and sector (1,000 plus each from the USA, UK, France and Germany; more than 500 each from Belgium, Spain and The Netherlands; and 300 plus from the Republic of Ireland), these are the people on the front line of the business battle against cyber crime. Respondents completed the online survey between 5 November 2020 and 8 January 2021.

Respondents (%)	
C-level executive	50
Vice president	13
Director	22
Manager	16

Respondent sector (%)	
Business services	8
Energy	4
Construction	8
Financial services	8
Food and drink	4
Government and non-profit	5
Manufacturing	8
Pharma and healthcare	8
Professional services	8
Property	4
Retail and wholesale	9
Technology, media and telecoms	16
Transport and distribution	5
Travel and leisure	4

Respondent number of employees (%)	
1,000+	25
250–999	15
50–249	15
10–49	16
1–9	29

Respondent department (%)	
Executive management	14
e-commerce	2
Finance	9
General counsel	2
Human resources	6
IT and technology	21
Marketing and communications	3
Operations	11
Owner	21
Procurement	2
Product management	3
Risk management	3
Sales	5

Hiscox Ltd

Chesney House
96 Pitts Bay Road
Pembroke HM 08
Bermuda

+1 441 278 8300
enquiries@hiscox.com
hiscoxgroup.com/cyber-readiness

21486 04/21