



# Contents

|                                   |    |
|-----------------------------------|----|
| Introduction                      | 01 |
| Hiscox and cyber                  | 02 |
| Executive summary                 | 03 |
| Country comparisons               | 04 |
| Perception vs. reality            | 06 |
| What do the experts do?           | 10 |
| Country snapshots                 | 14 |
| Top spending priorities checklist | 18 |
| Methodology                       | 19 |

# Introduction



**Gareth Wharton**  
Cyber CEO, Hiscox

One of the most telling findings in this year's report is that the cyber threat is now seen as the dominant risk to business in seven out of eight countries – ahead of the pandemic, economic downturn, skills shortages and other issues. If awareness of danger is the first step in dealing with it, that is surely an encouraging sign. On the downside, the number of firms reporting attacks has gone up, as has the severity of the attacks themselves. There can be no doubting the scale of the challenge.

While the cyber criminals have long targeted high-value companies, it is clear they are now moving down the food chain. International agencies have recently warned that more mid- and small-sized businesses are being targeted and this is borne out in this year's report.

Companies with revenues of \$100,000 to \$500,000 can now expect as many cyber attacks as those earning \$1m to \$9m annually. Yet, while big businesses have been investing ever more in building cyber defences, spending by smaller firms has fallen sharply this year. That appears to be part of a decline in overall IT spending at the lower end of the corporate spectrum. But this is not coming at a good time.

The pandemic may well have played its part here. The move to remote working has prompted many smaller businesses to adopt cloud solutions in preference to building out their own remote services. That, in turn, has encouraged more cyber criminals to exploit vulnerabilities in cloud applications and target cloud service providers too.

One good sign: there is clear evidence in this report that firms are responding to attacks with more vigour. Many more are taking decisive action. As an insurer, we are seeing this in the quality of the cyber resilience plans being presented to us. Greater awareness is driving up boardroom understanding of the issue and standards of cyber readiness with it.

We believe we have an important role to play in supporting that process. As part of that, we provide online cyber security awareness training for our clients' staff through the Hiscox CyberClear Academy. The continuing number of breaches created by simple phishing emails, highlighted in this report, shows the pressing need for continued staff awareness of the risks.

Similarly, the purpose of this report is not just to flag up the scale and nature of the cyber challenge but help firms measure up to it by identifying and adopting best practice. To that end, we invite you to visit our interactive [cyber readiness model](#) and check your company's cyber maturity against your peers. The model is intended to help a business identify its strengths and weaknesses and draw up an agenda for further action. Together with this report, we hope it helps you build stronger defences against the cyber threat and greater resilience to deal with issues as they occur.

There are signs that firms are responding more decisively to the cyber challenge.



## **When it comes to cyber insurance, Hiscox delivers expertise**

We have over 20 years' experience in privacy and cyber insurance, and in that time have underwritten hundreds of thousands of policies and managed thousands of claims worldwide. Understanding the cyber risks and challenges businesses face is paramount to our success. In 2017, Hiscox built a global, central cyber team to provide product consistency, coordinated insight and collaborative services.

## **Our new generation insurance product includes a suite of tools and services**

Beyond the classic risk transfer, Hiscox cyber insurance offers direct support and help from real experts – crisis managers, IT specialists, data protection lawyers and PR consultants. Since 2018, Hiscox has offered free employee training to all small-and mid-sized insureds around the globe through the Hiscox CyberClear Academy, which has nearly 30,000 users.

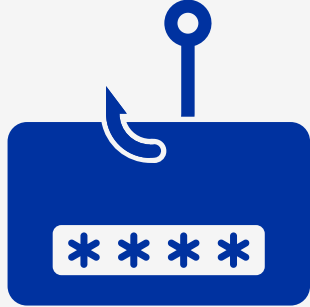
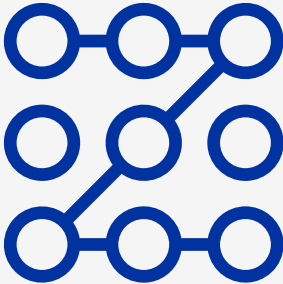

## **Sharing our expertise and building awareness**

We have built free-to-all tools like the Hiscox Cyber Exposure Calculator, which helps companies understand the financial impact of a cyber attack. In 2021, we introduced our online cyber maturity self-assessment model to help companies understand their cyber security strengths and weaknesses. They can compare their performance to over 11,000 other companies for free.

## **Keeping you informed about the cyber security landscape**

For the sixth year running, we've produced the Hiscox Cyber Readiness Report, which provides a picture of the cyber readiness of businesses, and offers a blueprint for best practice in the fight to counter an ever-evolving threat. Drawn from a representative sample of companies across eight countries by size and sector, this reflects the direct experience of those on the front line of the business battle against cyber crime.

# Executive summary

|                                                                                                                                                             |                                                                                                                                                         |                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Attacks intensify</b><br/>48% of companies reported a cyber attack in the past 12 months, up from 43% last year.</p>                                  | <p><b>Perceived risk high</b><br/>Seven of eight countries rank a cyber attack as the number one threat to their business.</p>                          |                                                                   |
|                                                                           | <p><b>Bottom-line pressure</b><br/>One-in-five firms attacked say their solvency was threatened, an increase of 24% from last year.</p>                 | <p><b>Remote-working risks</b><br/>Covid caused companies to accelerate their cloud journey, leading to a big jump in attacks via cloud servers.</p> |
| <p><b>Expertise pays off</b><br/>Median attack costs, as a percentage of revenues, are two-and-a-half times higher for firms ranked as 'cyber novices'.</p> | <p><b>More cyber policies</b><br/>64% of companies now have cyber insurance as a standalone, or part of another, policy. Up from 58% two years ago.</p> | <p><b>Ransomware rises</b><br/>19% of respondents reported a ransomware attack, up from 16%. Two-thirds of the firms paid up.</p>                    |
| <p><b>Increased spending</b><br/>Respondants' mean cyber security spending is up 60% in the past year to \$5.3m, and has increased by 250% since 2019.</p>  |                                                                      | <p><b>More severe impact</b><br/>The median cost of an attack has risen 29% to just under \$17,000.</p>                                              |

# Country comparisons

| Highlights                                                                                                                                                                             |                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Belgium</b><br/>One-in-seven (14%) Belgian businesses laid off workers as a result of a cyber attack.</p>                                                                        | <p><b>France</b><br/>Two out of five firms attacked (41%) suffered payment diversion fraud – the highest proportion of any country.</p>                                                    |
| <p><b>Germany</b><br/>While German firms are least likely to have paid a ransom following an attack, they also have the highest ransom payments.</p>                                   | <p><b>Ireland</b><br/>Irish businesses paid out ransoms more regularly than the rest, with 25% paying five times or more to recover data, but ransom costs were among the lowest.</p>      |
| <p><b>The Netherlands</b><br/>Dutch firms are now the number one targets among our study group. The percentage attacked in the past 12 months has jumped from 41% to 57%.</p>          | <p><b>Spain</b><br/>Spain is the only country where the proportion of firms attacked has fallen in the past year – from 53% to 51%.</p>                                                    |
| <p><b>United Kingdom</b><br/>For the third year running, the UK has the smallest proportion of firms being attacked (42%), but the median cost of attacks has doubled to \$28,000.</p> | <p><b>United States</b><br/>US firms reporting a cyber attack have jumped sharply (+7%) in the past year, while attacks costing \$25,000 or more have also increased, from 34% to 40%.</p> |



# Country comparisons

## continued

| Experienced a cyber attack (%) |      |      |     |
|--------------------------------|------|------|-----|
|                                | 2021 | 2022 | +/- |
| Belgium                        | 42   | 43   | +1  |
| France                         | 49   | 52   | +3  |
| Germany                        | 46   | 46   | -   |
| Ireland                        | 39   | 49   | +10 |
| The Netherlands                | 41   | 57   | +16 |
| Spain                          | 53   | 51   | -2  |
| United Kingdom                 | 36   | 42   | +6  |
| United States                  | 40   | 47   | +7  |

| Median cost of all cyber attack (\$000) |      |      |     |
|-----------------------------------------|------|------|-----|
|                                         | 2021 | 2022 | +/- |
| Belgium                                 | 12   | 10   | +2  |
| France                                  | 18   | 17   | -1  |
| Germany                                 | 24   | 21   | -3  |
| Ireland                                 | 8    | 17   | +9  |
| The Netherlands                         | 12   | 18   | +6  |
| Spain                                   | 12   | 12   | -   |
| United Kingdom                          | 14   | 28   | +14 |
| United States                           | 10   | 19   | +9  |

| Experienced a ransomware attack (%) |      |      |     |
|-------------------------------------|------|------|-----|
|                                     | 2021 | 2022 | +/- |
| Belgium                             | 19   | 15   | -4  |
| France                              | 14   | 19   | +5  |
| Germany                             | 19   | 21   | +2  |
| Ireland                             | 16   | 19   | +3  |
| The Netherlands                     | 13   | 26   | +13 |
| Spain                               | 14   | 22   | +8  |
| United Kingdom                      | 13   | 16   | +3  |
| United States                       | 17   | 17   | -   |

| Victims of ransomware that paid (%) |      |      |     |
|-------------------------------------|------|------|-----|
|                                     | 2021 | 2022 | +/- |
| Belgium                             | 49   | 74   | +25 |
| France                              | 65   | 62   | -3  |
| Germany                             | 54   | 48   | -6  |
| Ireland                             | 75   | 80   | +5  |
| The Netherlands                     | 48   | 79   | +31 |
| Spain                               | 44   | 64   | +20 |
| United Kingdom                      | 58   | 63   | +5  |
| United States                       | 71   | 84   | +13 |

| Cyber insurance uptake (%) |      |      |     |
|----------------------------|------|------|-----|
|                            | 2021 | 2022 | +/- |
| Belgium                    | 58   | 59   | +1  |
| France                     | 57   | 61   | +4  |
| Germany                    | 64   | 67   | +3  |
| Ireland                    | 64   | 69   | +5  |
| The Netherlands            | 55   | 58   | +3  |
| Spain                      | 63   | 66   | +3  |
| United Kingdom             | 61   | 62   | +1  |
| United States              | 65   | 65   | -   |

| Proportion of IT budget for cyber security (%) |      |      |     |
|------------------------------------------------|------|------|-----|
|                                                | 2021 | 2022 | +/- |
| Belgium                                        | 21   | 24   | +3  |
| France                                         | 20   | 22   | +2  |
| Germany                                        | 21   | 24   | +3  |
| Ireland                                        | 21   | 22   | +1  |
| The Netherlands                                | 22   | 24   | +2  |
| Spain                                          | 22   | 24   | +2  |
| United Kingdom                                 | 20   | 22   | +2  |
| United States                                  | 23   | 24   | +1  |

## Perception vs. reality

Once bitten, twice shy: it seems there is nothing like a brush with the hackers to focus the mind. Firms that have suffered an attack in the past year are much more likely to classify the threat of cyber attack as 'high risk' than those that have not.

The cyber threat is now widely viewed as the number one risk to the business. From a country perspective, only Irish firms relegated the cyber threat to the number two spot, behind pandemics. But there is a huge gulf in perception between those who have actually suffered an attack and those who have not. More than half of cyber attack victims (55%) see cyber as an area of high risk. Among non-victims the figure is just 36%. Keeping data secure, regardless of cyber risk, seems to be important for all – 72% of companies agree they'll damage their brand if they don't handle client and partner data securely.

This gulf in perception is mirrored in the numbers who say risks have gone up in the past year. More than two-in-five (41%) of those attacked say their risk exposure has increased. Among those not attacked the figures is closer to one in five (23%).

There are some exceptions. Respondents in the food and drink industry, which was more heavily attacked this year, rank pandemics, skills shortages and heightened competition as more high risk challenges.

One other indicator of risk perception is the amount firms in different sectors spend on cyber security. Business services firms are far and away the biggest spenders at an average \$34m. That is more than six times the average. The travel and leisure industry spends the least.

### Experts and insureds see the risks

The majority of firms that qualify as cyber experts show similarly heightened awareness of the danger, as do nearly half (49%) of those that have cyber insurance cover (for a full understanding of how our model works in evaluating the people, processes and technology needed for effective cyber security go to [www.hiscoxgroup.com/cyber-maturity](http://www.hiscoxgroup.com/cyber-maturity)). Nearly twice as many experts as novices consider their exposure to cyber attack high or very high: 58% compared with 32%. This is despite the fact they have built better defences.

It is notable that nearly four out of every five firms that have no cyber cover, and say they do not plan to get it, did not experience an attack in the past year. More than half (51%) are novices. They have yet to undergo the perception shift common among cyber attack victims.

Confidence to deal with attacks effectively is greatest among large companies and those that have been attacked. Smaller firms have some catching up to do.

Overall, more than three out of five respondents (62%) agree that their business is more vulnerable to attack with more employees working from home. Among firms with more than 250 employees the figure is 69%. Among experts it is 76% but only 49% on average for novices.

### And what is the reality?

There is some correlation between perceived risk exposure and the incidence of cyber attacks. As mentioned above, firms that qualify as experts are more likely to see the cyber threat as high risk. They are right to do so. They receive the hackers' attention more often than the others, probably because they are more tempting targets given their relative size.

It would appear that the move to remote working has shifted the focus of attacks. The main way in for the hackers is corporate servers, and there has been a big jump in the numbers reporting entry via cloud server. This aligns with the warning from international agencies that bad actors are increasingly targeting cloud infrastructure.

How does the perception of the cyber threat match up with the chance of being attacked?



# Perception vs. reality

## continued

Though there's a fairly even perception of different types of attack, the reality illustrates where companies should focus. The top two types of attack – IT resource misuse (32%) and payment diversion fraud (31%) – seem to present more of a risk than ransomware (19%). The implication is that firms may not be paying sufficient attention to staving off the first two.

### Hackers broaden their attack pool

The average number of cyber attacks per company has risen only moderately this year (179 to 190). For enterprise firms, it has actually fallen slightly, though the largest (revenues of more than \$5 billion) report an average of more than 1,100 attacks. At most other size groupings it has actually increased as the hackers have directed more of their attention to mid- and small-sized businesses.

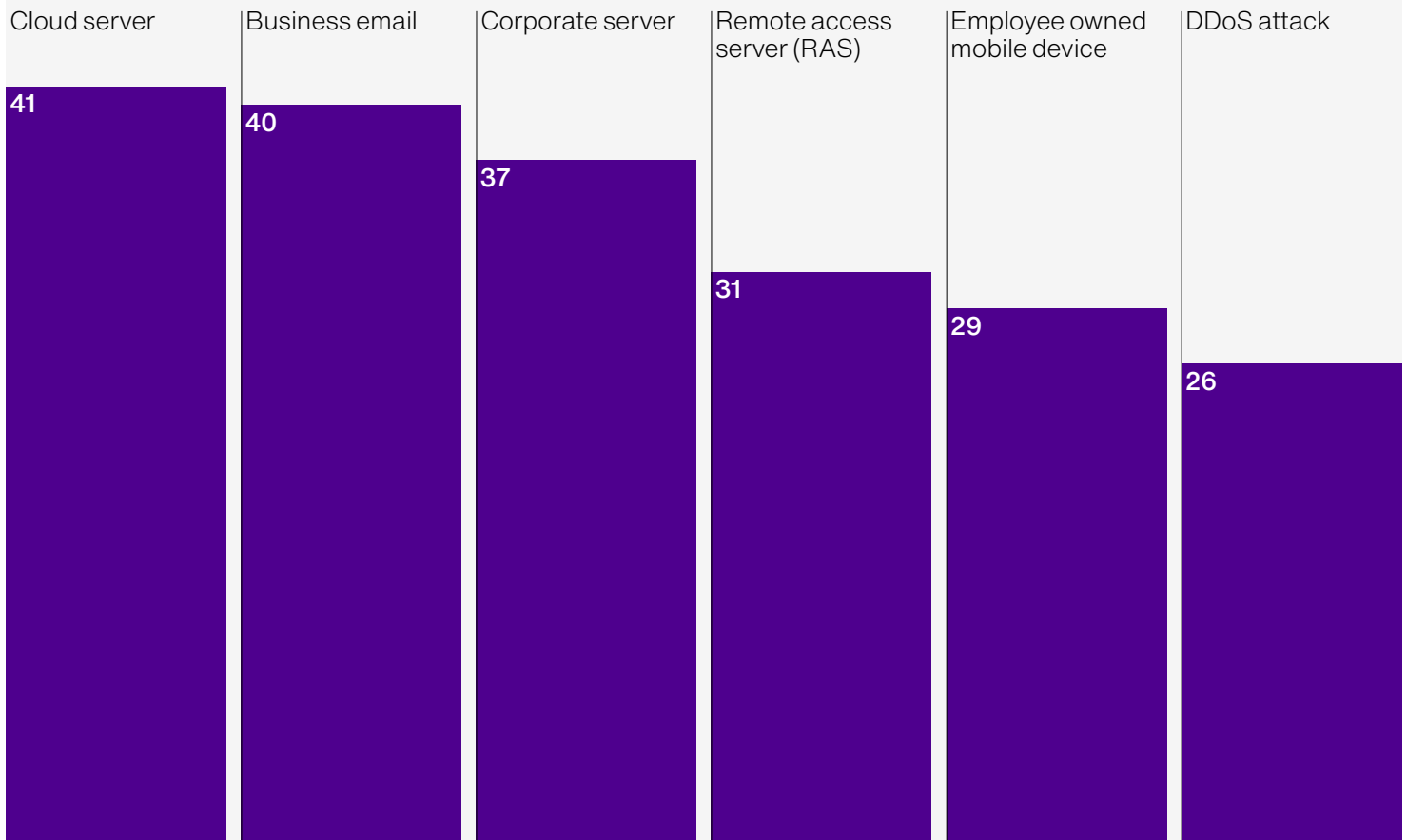
Thus, firms with between 250 and 999 employees saw the average number of attacks rise from 45 to 69. Those with ten to 49 employees sustained an average 56 attacks, up from 31, and the smallest, with under ten employees, saw a near four-fold rise – from 11 to 40.

Companies with revenues of \$100,000 to \$500,000 can now expect as many cyber attacks as those earning \$1m to \$9m annually. This chimes with warnings from international agencies from 'big game' targets to mid-sized ones.

There was also a shift in sectoral focus. The most widely targeted sectors were travel and leisure (where 61% reported one or more attacks), professional services (58%) and retail or wholesale (56%). The previous year's top targets, energy and transport or distribution, both saw a marked fall-off in attacks.

### Most common method of entry (%)

Cloud servers are now the number one way in for cyber attacks.



# Perception vs. reality

## continued

### Costs continue to rise

The median cost per respondent of all cyber attacks suffered has risen 30% in the past year, to just under \$17,000. But that masks a wide range of outcomes – between a low of \$9,900 in Belgium and a high of \$28,100 in the UK, where costs more than doubled. Costs also doubled in Ireland – to \$16,800.

One UK firm suffered total attack costs of \$6.7m. At the worst-hit businesses in Germany, Ireland and The Netherlands, costs topped \$5m. By contrast, Belgium, France, Germany and Spain all saw stable or lower median costs.

The bare figures only hint at the impact the cyber onslaught is having. The number of respondents laying off staff following an attack has doubled – from 5% to 11%. One-in-five firms paid a substantial fine to a government agency, nearly twice as many as the previous year, and a similar proportion (21%) said the impact was enough to threaten their solvency.

Property firms reported the highest number of attacks (319), closely followed by the business services sector (304). The highest median losses were suffered by the retail and wholesale industry, at \$30,000, followed by the energy (\$23,500) and pharmaceutical and healthcare sectors (\$21,300).

### Ransomware on the increase

More firms were hit by ransomware – 19% compared with 16% the previous year. Two-thirds (66%) paid up and more than half (53%) paid ransoms on multiple occasions. US and Irish firms were most likely to pay up, German ones least likely. The single largest ransom paid was just under \$100,000, marginally up on last year's \$95,000. One strange anomaly: the food and drink sector was the least targeted with ransomware (only 14% of firms reported an attack) but the most likely to pay a ransom – 62% of affected firms gave in.

Some good news: the median of total ransoms paid is down 20% and recovery costs have nearly halved. More firms recovered or rebuilt their data from back-up on multiple occasions. Firms with 1,000-plus employees are more likely to have recovered their data successfully (68% compared with 59% on average) and much less likely to have had their data leaked (20% compared with 29% on average). Professional services firms, which are far and away the biggest spenders on cyber security at an average of \$34m, were the least likely to pay (just 18% did so).

### New surge in cyber security spending

Mean spending across all respondents has increased 60% in the past year to \$5.3m and is up 250% since 2019. Last year's biggest spenders, German firms, have been supplanted by their Irish peers at \$13.9m average per firm (up from \$2.1m).

There is, however, a big divide between large and small. Average spending by firms with 250 to 999 people has doubled in the past year. For enterprise firms of 1,000-plus it is up 65%. At nearly \$20m, their average spend has risen nearly fivefold in three years.

At the other end of the scale it is a different story. Firms with between ten and 49 employees have almost halved their cyber security budgets, from \$411,000 to \$225,000. Among those with under ten employees, spending has collapsed – from an average \$150,000 to just \$29,000. This is likely pandemic-related as companies have less in the pot to spend on IT. The percentage of IT budget spent on cyber security for this size of business has slightly increased from 17% last year to 20%. Though there's less to go around, they're not completely ignoring the importance of cyber security.

# Perception vs. reality

continued



## What do the experts do?

It is tempting to answer the question by saying they are throwing money at the problem. But that is only partly true and it is not the whole answer. There are plenty of steps firms can take without breaking the bank.

It is certainly the case that the larger companies in our study group make up the lion's share of the firms that qualify as cyber experts in our cyber maturity model. As such they enjoy substantially greater resources, not least in the fight against cyber crime.

However, with size come extra challenges. The average expert has to deal with 41 different servers, more than twenty of which are likely to be in the cloud. As is apparent elsewhere in this report, that can be an area of vulnerability. Equally, large companies are prime targets and get attacked more often than small ones. And that prompts its own responses. Firms experiencing 30 or more attacks in the past year had average cyber security budgets of \$10m-plus.

But the spending gap between the experts and everybody else has narrowed dramatically in the past year. Firms ranked as novices have pumped up average spending on cyber more than threefold (to \$3.2m) while those ranked as intermediates have lifted theirs by 63% on average. At \$6.2m, they now out-spend the average expert by \$1m.

### Not all about money

Thankfully, it is not all about money. The experts formalise their cyber security response. They don't make it up as they go along. They have one or more clearly defined roles for managing the cyber challenge, and they have board or management buy-in. The majority (87%) say the top executives have a clear view of how cyber security is being managed (compared with 69% across the study group).

And they typically work their way through the US government's National Institute of Standards and Technology (NIST) framework, spreading investment and time across the five functions – identify, protect, detect, respond and recover.

Two initiatives that increased the most were building an incident response plan and regularly simulating a cyber attack to test a firm's incident response plan. These activities are especially sensible in these uncertain times of European conflict and western sanctions. The list of priorities for experts also includes regular assessments of a firm's data and technology infrastructure, giving staff effective cyber security training and ensuring business partners comply with the firm's security requirements. There are many other recommended measures which cost relatively little to put in place. They are the low-hanging fruit firms need to seize. Some two-thirds or more of our experts have ticked every one of them.

And it is not all about size. Within that group there is roughly the same number of smaller firms – defined as fewer than 50 employees – as large ones with more than 1,000. The smaller firms are not planning to cover quite as many bases as the large ones, but they are not far behind. One example: 44% of the smaller contingent say they plan to regularly simulate a cyber attack to test their company's incident response plan compared with 58% of the big firms. For context, that compares with just 37% of novices.

Putting in the effort bolsters confidence. One-in-six experts say their exposure to cyber attack has actually decreased in the past year. Why? The top two reasons are better implementation of cyber security processes or procedures, such as patching or pen testing (mentioned by 62% of this group), and the appointment of key cyber security roles or a strengthened team of people (mentioned by 46%).

All businesses need to adopt the structured and methodical approach used by experts.

# What do the experts do?

continued



## Sharp fall in number of experts

Overall, cyber readiness scores have fallen by 2.6%, with a sharp deterioration in governance and assurance (process function) and the presence of suitably qualified and experienced personnel (people). Improvements have been made in tools and technology (technology).

This overall decrease has led to a sharp drop in the number of firms ranked as experts in our cyber readiness model from 20% to just 4.5% this year. The USA and UK still lead with 6% of firms ranked as experts. The proportion ranked as novices has also fallen sharply, leaving a great bunching of intermediates.

Our cyber maturity model relies on companies self-assessing their readiness. Two factors appear to have contributed to a fall in confidence. The principal one is the much publicised discovery in December last year that the Log4j logging library, widely used in apps and services across the internet, was vulnerable to attack.

Following this news, the proportion of respondents assessing their cyber security arrangements as 'optimised' fell from 18% to 2.9% and those saying they were very confident in their cyber security readiness fell from 73% to 67%. A contributory factor may be the increasing challenge in hiring suitably qualified people – apparent from the low scores for people in our cyber readiness model.

# What do the experts do?

## continued

### Do the basics

Given the publicity accorded to some recent cyber attacks, it's surprising that almost half of respondents (49%) considered their tools for backing up data 'optimised' or 'measured'. Among novices the figure was much lower (at just 21%) and only 17% were properly set-up to recover IT systems and data in the event of a systems failure.

While four-fifths of the experts had a measured or optimised approach to pre-employment screening checks, prohibiting the use of generic new accounts or the sharing of credentials among users, the equivalent figure for the novices was one in five or fewer. Doing the basics well is vital, and relatively low cost, especially when set against the cost of managing a ransomware attack.

### Bolster defences after attacks

Asked how they had responded to cyber attacks, around two out of five experts said they had put additional cyber security and audit requirements in place (41%), stepped-up employee training (39%) and improved preparations for cyber attack (39%). The figures are generally higher for large firms.

The small-firm experts lead when it comes to the first of those moves: more than half say they have implemented additional cyber security requirements post-attack. Similarly, more of them have engaged with an incident response provider – though that may reflect the fact that their bigger brethren already have outside help in place or do not need more.

### Cyber insurance protection

Taking the entire study group, more than a third (35%) of firms with 250 or more employees have a standalone cyber policy in place and 40% have cyber cover as part of another policy. Below that threshold the equivalent figures are 28% and 29%.

The relevance for smaller firms that cannot employ large teams of cyber specialists is obvious, particularly since evidence elsewhere in this report shows small companies are increasingly in the firing line.

Among the study group as a whole, the ability to access expertise, such as crisis management or IT forensics, is among the top three reasons for taking out cyber cover (after concerns about data security and slightly ahead of the need to show clients the firm is serious about cyber protection). But among the experts, who generally have in-house expertise, the number two reason is the concern that, if the business is attacked, clients could make a claim against them. In total, 46% of experts currently have a standalone cyber insurance policy (compared with 31% on average and 29% of novices).

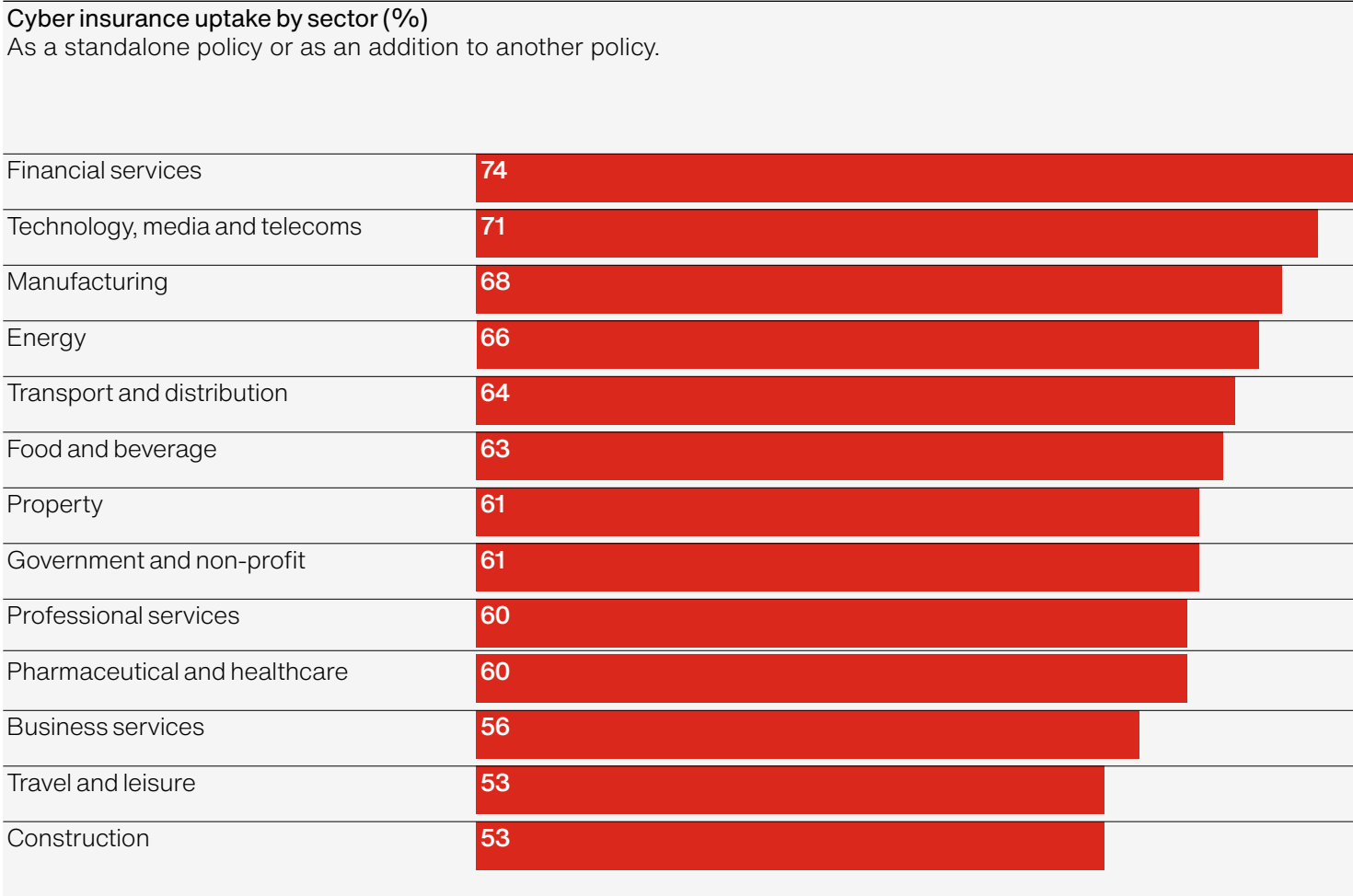
Unsurprisingly, adoption of cyber insurance is highest in the financial services industry, where 74% have cover either through a standalone policy or as part of a wider policy and a further 18% say they plan to get coverage soon. Construction and travel and leisure firms are at the other end of the spectrum: 53% of both industries have some form of cyber coverage.

It is notable that insured firms are more likely to respond to a cyber attack by stepping up their defences than the uninsured. One reason may well be that an insurer would ask if they have mitigated against certain threats or have assisted them to fix an issue after a previous attack.

The experts have also responded more purposefully to the pandemic challenges. They are much more likely to have increased remote working, adopted cloud-based and collaborative technologies, shifted payments online and accelerated their digital transformation plans.

# What do the experts do?

continued

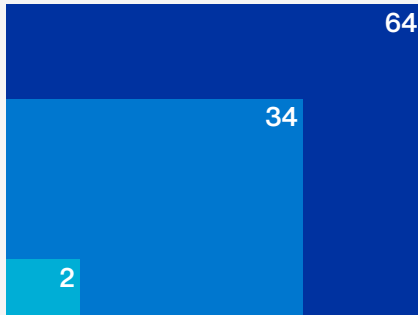


# Country snapshots

## Belgium

### Cyber maturity (%)

- Novice
- Intermediate
- Expert



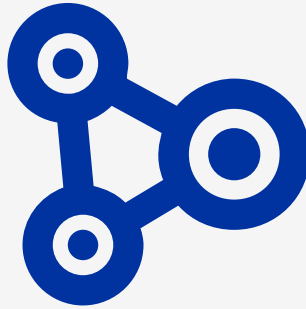
# +10%

Bad publicity and negative impact on brand up 10% over the last two years.



# x2

Companies who caused a breach for third-party partners have doubled since last year to 24%.



### Top three spending priorities

1 Addressing existing threats and vulnerabilities.

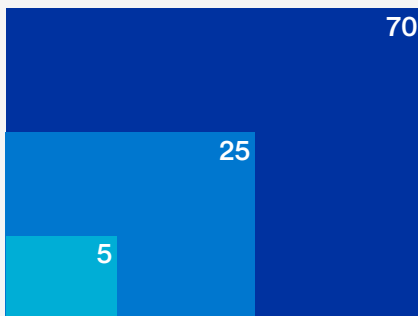
2 Achieving or maintaining regulatory compliance.

3 Security of customer-facing services and applications.

## France

### Cyber maturity (%)

- Novice
- Intermediate
- Expert



# 24%

Percentage of businesses whose solvency was materially threatened by an attack.



# #1

Number one reason for investing in cyber insurance is security concerns about data.



### Top three spending priorities

1 Addressing existing threats and vulnerabilities.

2 Achieving or maintaining regulatory compliance.

3 Security of customer-facing services and applications.

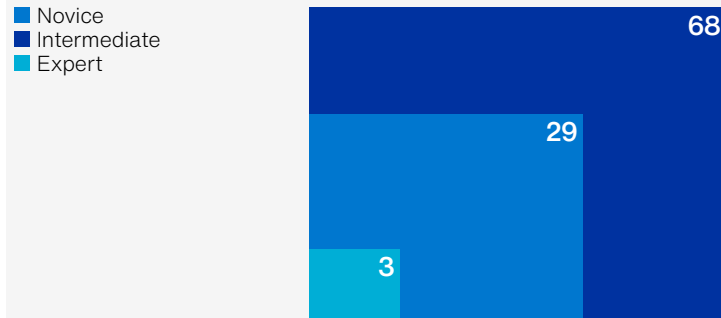


# Country snapshots

continued

## Germany

### Cyber maturity (%)



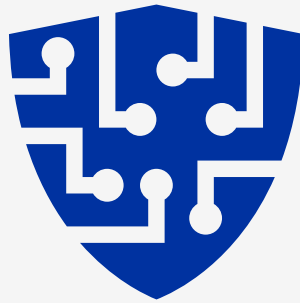
# \$3.4m

Single largest cyber attack suffered in past year.



# 27%

Percentage of companies that purchased or enhanced cyber insurance after an attack.

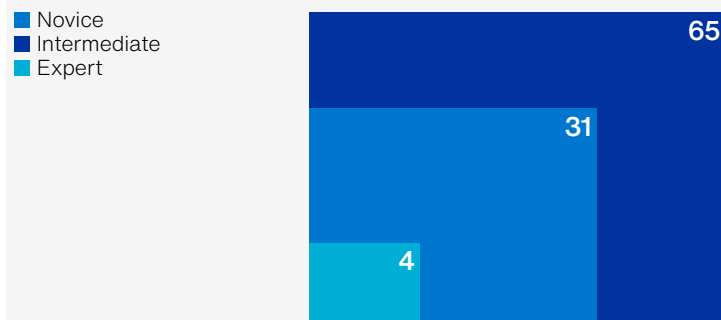


### Top three spending priorities



## Ireland

### Cyber maturity (%)



# #1

Number one reason for investing in cyber insurance is fear of the cost of a potential breach.



# 34%

Percentage of businesses that purchased or enhanced cyber insurance after an attack. Up 24% from last year.

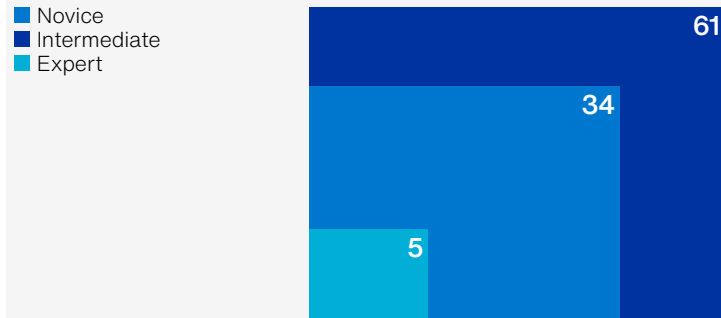


### Top three spending priorities



The Netherlands

Cyber maturity (%)



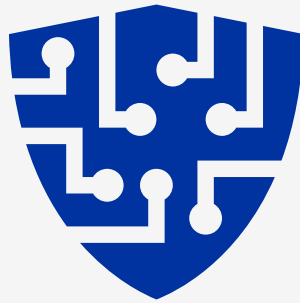
**\$2.3m**

Single largest cyber attack suffered in past year.



**x3**

Companies that purchased or enhanced cyber insurance after an attack over the past 12 months tripled.

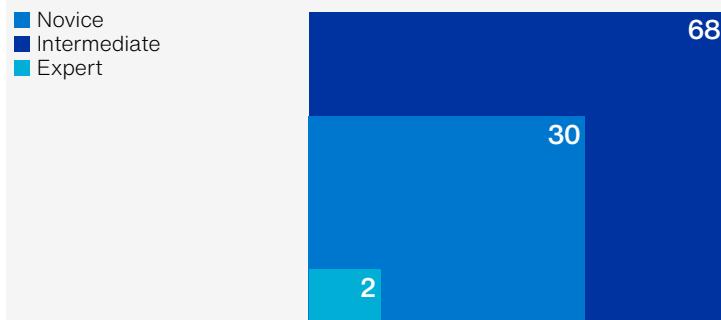


Top three spending priorities



Spain

Cyber maturity (%)



**#1**

Number one reason for investing in cyber insurance is security concerns about data.

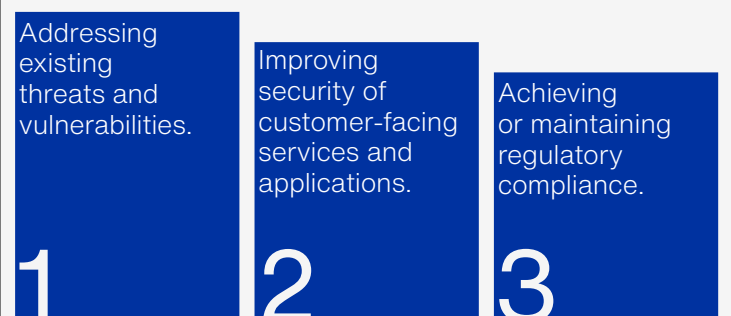


**x2**

Businesses who have lost customers as result of a breach have more than doubled over the past two years.



Top three spending priorities

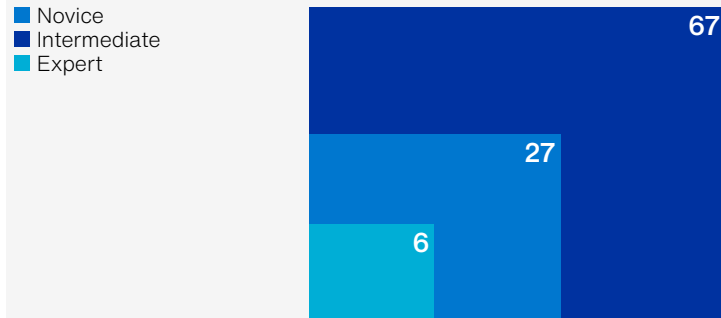


# Country snapshots

continued

## United Kingdom

### Cyber maturity (%)



**x2**

Businesses experiencing a substantial fine from a breach more than doubled in the past year.



**20%**

Percentage of companies whose solvency was materially threatened by an attack.

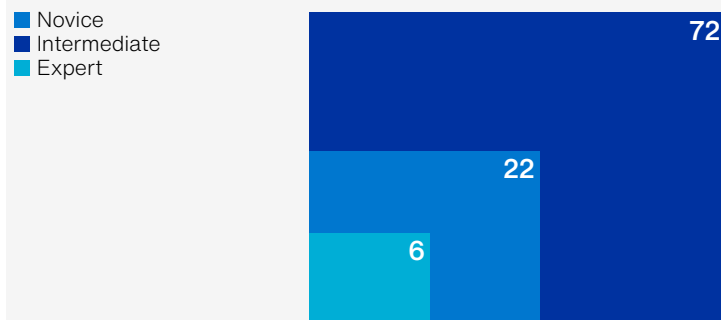


### Top three spending priorities



## United States

### Cyber maturity (%)



**29%**

Percentage of companies who had increased difficulty attracting new customers after an attack.



**#1**

Number one reason for investing in cyber insurance is to mitigate customer claims following an attack.



### Top three spending priorities



# Top spending priorities checklist

After two years of the pandemic, and several large-scale vulnerabilities, businesses appear to be going back to basics. They are focusing on existing threats (ensuring devices are patched and up-to-date) as well as ensuring policies and procedures are up-to-date, especially testing incident response plans. Finally, they are combating phishing attacks, the most prevalent method of entry for ransomware attacks, by rolling out cyber security training across their business.

## Large businesses (1,000+ employees)

- ✓ Address existing threats and vulnerabilities
- ✓ Achieve or maintain regulatory compliance
- ✓ Review internal cyber security policies and procedures
- ✓ Improve the security of customer-facing services and applications
- ✓ Implement a formal IT cyber security management framework

## Small businesses (0-49 employees)

- ✓ Address existing threats and vulnerabilities
- ✓ Achieve or maintain regulatory compliance
- ✓ Implement systems to detect unauthorised people, connections or devices
- ✓ Ensure business partners and third parties comply with security requirements
- ✓ Implement vulnerability scans of environment

This is not an exhaustive list and only reflects some of the top priorities by businesses according to this research. This does not qualify as a recommendation by Hiscox, nor does it guarantee that if a business completes the checklist they will be completely cyber-secure.

Hiscox commissioned Forrester Consulting to gather information about businesses cyber activities and readiness. In total 5,181 professionals responsible for their company's cyber security strategy were surveyed (over 900 each from the USA, UK, France and Germany; more than 400 each from Belgium, Spain and The Netherlands; and more than 200 from the Republic of Ireland). Respondents completed the online survey between 30 November 2021 and 21 January 2022.

The full make-up of respondents is detailed below.

| <b>Respondents (%)</b>         |    | <b>Respondent department (%)</b>          |    |
|--------------------------------|----|-------------------------------------------|----|
| C-level executive              | 32 | Executive management                      | 12 |
| Vice president                 | 23 | e-commerce                                | 3  |
| Director                       | 34 | Finance                                   | 9  |
| Manager                        | 12 | General counsel                           | 4  |
|                                |    | Human resources                           | 5  |
|                                |    | IT and technology                         | 19 |
|                                |    | Marketing and communications              | 5  |
|                                |    | Operations                                | 10 |
|                                |    | Owner                                     | 18 |
|                                |    | Procurement                               | 3  |
|                                |    | Product management                        | 4  |
|                                |    | Risk management                           | 4  |
|                                |    | Sales                                     | 4  |
| <b>Respondent sector (%)</b>   |    | <b>Respondent number of employees (%)</b> |    |
| Business services              | 9  | 1,000+                                    | 25 |
| Construction                   | 7  | 250-999                                   | 15 |
| Energy                         | 4  | 50-249                                    | 15 |
| Financial services             | 9  | 10-49                                     | 19 |
| Food and drink                 | 4  | 1-9                                       | 26 |
| Government and non-profit      | 5  |                                           |    |
| Manufacturing                  | 8  |                                           |    |
| Pharmaceutical and healthcare  | 8  |                                           |    |
| Professional services          | 9  |                                           |    |
| Property                       | 4  |                                           |    |
| Retail and wholesale           | 8  |                                           |    |
| Technology, media and telecoms | 18 |                                           |    |
| Transport and distribution     | 5  |                                           |    |
| Travel and leisure             | 3  |                                           |    |

**Hiscox Ltd**

Chesney House  
96 Pitts Bay Road  
Pembroke HM 08  
Bermuda

+1 441 278 8300

[enquiries@hiscox.com](mailto:enquiries@hiscox.com)

[hiscoxgroup.com/cyber-readiness](https://hiscoxgroup.com/cyber-readiness)