Hiscox Cyber Readiness Report 2023

HISCOX

Contents

Cover illustration: johnholcroft.com
Report design: somethingbrighter.com

Introduction

This year's report reveals several shifts in the cyber landscape worth noting for anyone concerned with countering cyber criminals.

Eddie Lamb
Director of Cyber Education and Advisory Hiscox

One of the notable outcomes this year is the definite rise in the proportion of the smallest businesses being targeted – up to 36%. That is up by a half over the last three years. Being small does not mean a firm can count on being ignored by the cyber criminals. More encouragingly, however, the report also shows that the smallest firms have been ramping-up spending at a markedly faster pace than others, which may help in countering the increasing attacks.

At the top end of the survey group, the number of firms suffering seven-figure losses this year increased. But the good news is that median costs across the entire survey group were contained. That partly reflects an increasing trend towards fraud, such as payment diversion via business email compromise which generally requires less technical ability, but produces lower rewards. The increasing prevalence of cyber insurance may also have played its part here. Nearly three-quarters of attacked firms had some form of cyber cover.

Attacks involving ransomware have stayed steady and the proportion paying a ransom demand fell slightly this year. Where a ransom was demanded, the principal reason firms paid was to stop sensitive data from being released. This marks a subtle shift from data encryption to data exfiltration on the part of the hackers – something that is reflected in our own claims data. There is mounting evidence that dealing with the extortionists is a hit-and-miss affair. Less than half of firms that paid up got all their data back.

Despite the continued increase in cyber attacks, there are positives to be taken from this year's report. Whether justified or not, there is a marked improvement in sentiment, with a drop in the proportion of firms that see cyber as the number one challenge to their business.

This may be down to the rise of other issues, notably economic downturn. But it is also a reflection of rising cyber security budgets, better implementation of security measures and more buy-in at board level – or simply that cyber has become a peril to be appropriately managed like any other business risk.

Driving up levels of awareness and understanding of the cyber challenge is one of the purposes of this report. It is also an essential part of our role as an insurer. The Hiscox CyberClear Academy provides online cyber awareness training for our clients' staff with around 36,000 people from 7,000 organisations taking the course since 2017. Given the number of people who continue to fall victim to phishing emails (still the number one way in for ransomware attacks), repeated awareness training must be a priority for all businesses with a material online presence.

We also hope this report will help businesses gauge their own resilience to the cyber threat and see how their level of preparedness measures up against their peers. To do that in a more formalised manner, we invite you to visit our interactive cyber readiness model where you can identify strengths and weaknesses in your firm's cyber security measures and plan next steps to stiffen your defences. You can compare your organisation by size, sector, and country to over 16,000 other companies.

The battle with the cyber criminals is never-ending but preparedness is the key to fending off attacks and limiting potential damage to the business.

Executive summary

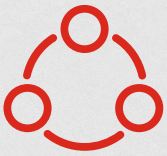
Majority report attacks
Cyber attacks rose for the third year running – 53% of firms suffered a cyber attack, up from 48% last year.

Shift in sentiment
Only five-in-eight countries now view cyber as the primary business risk. Competition and economic issues gain more focus.

Cost of attacks contained
Median costs for those attacked dipped slightly, from almost $17,000 to just over $16,000.

Big hits still possible
One-in-eight attacked businesses suffered costs of $250,000 or more.

Smallest firms hit harder
In three years, the proportion of firms attacked with less than ten employees rose by more than half to 36%.

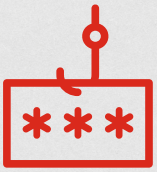


Fraud takes top threat
One-in-three attacked companies experienced financial loss due to payment diversion fraud.

Resisting ransomware
One-in-five firms received a ransom demand but those paying fell from 66% to 63% – less than half of those that paid recovered all data.

Security spend increases
Median spend on cyber security rose 39% over three years to $155,000. For firms with less than ten employees, it quadrupled in two years.

The weakest link
Business email compromise was the hackers' favourite way in, followed by a cloud or corporate server.



Risk sentiment

Cyber remains the number one worry among businesses, but green shoots of optimism are starting to appear.

Fear factor in decline

Are businesses learning to live with the cyber threat? Exposure to cyber attack still tops the list of business worries among our respondents. But this year there has been a perceptible shift in risk sentiment – for the better. The proportion of firms citing the cyber threat as high risk has dropped this year from 45% to 40% – though that has to be set against a general improvement in confidence across all categories of business risk. The cyber threat comes out just ahead of economic issues such as recession, inflation or exchange rates (38%) and the emergence of a new competitor (36%).

While the cyber threat continues to be seen as the number one danger in most business sectors, several industries – business services, construction, transport, food and drink, and travel and leisure – now consider economic issues as more important.

Seven-of-eight countries last year saw cyber as the top risk. The number has fallen to five this year, though cyber is still seen as one of the top three risks in all countries apart from Belgium. There, risks like skills shortages, economic loss and competition take precedence. This is another pointer to suggest that some businesses now feel there are other risks posing an equal or greater threat than cyber.

Top ten business risks (%)

		2023	2022
1.	Exposure to a cyber attack	40	45
2.	Losses due to economical issues e.g. inflation	38	40
3.	Emergence of new competitor	36	36
4.	Skills shortage	35	40
5.	Reputational damage e.g. negative press	35	37
6.	Regulatory or legislative changes	34	37
7.	Pandemic or infectious diseases	33	42
8.	Geopolitical conflicts disrupting operations	33	–
9.	Fraud and white-collar crime	32	38
10.	Extreme weather and natural disasters	29	33

More firms feel on top of the challenge.
The proportion of companies saying their cyber risk has lessened rose from 12% to 16%. They believe this is due to better implementation of cyber security processes and bigger budgets. Increased awareness at board level is also picked out by more of the big firms this year. More than two in five (41%) of those large companies saying their exposure to attack has decreased mention more board involvement, leading to improved risk management or risk transfer (e.g. cyber insurance).

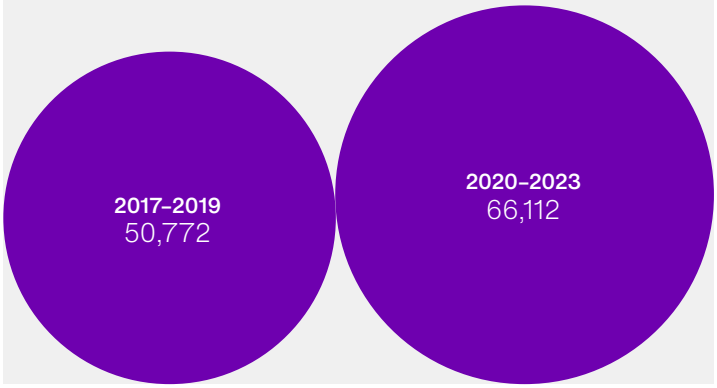
But cyber risk is still alive and well, especially for those who perceive that risk to be increasing. Nearly a third (32%) of those who considered their risk exposure had gone up in the past 12 months said one reason was the greater number of employees working remotely. That concern was more prevalent among larger firms with more than 250 employees (35%) than smaller ones (30%) – though smaller firms were marginally more likely to be worried about employees using their own devices (27% mentioned this compared with 26% of larger businesses). Controls here look more important than ever.

More patching drives concern
There is also increasing concern about the ability to keep up with the volume of vendor patches required. More than one in five (22%) of larger firms view this as a reason for increased cyber risk, up from 16% the previous year. Patching is required to close software security vulnerabilities or optimise performance. Common vulnerabilities and exposures (CVEs) have increased by 30% when comparing the last three-year average over the prior three years.

Granted, vulnerabilities have always existed in software, but over the last five-to-ten years automated scanners, bug-hunting programs, researchers, and crowd sourcing have improved discovery and public notifications.

Once discovered, software companies are required to provide patches; regulators or insurance carriers then require companies using the exposed software to patch in a timely manner. Constant patching and updates to systems are especially challenging for large businesses where patching management is often complex.

Common vulnerabilities and exposures
Three-year average



Confidence driven by experience of cyber attacks
Nearly half (48%) of those with experience of a cyber attack consider the threat as high risk. However, similar to last year, large companies and those that have been attacked are more confident in their company's ability to deal with an attack, as well as the government's approach to the threat. They have more faith in both the internal factors (such as their technology, board level buy-in) and external ones (regulatory authorities, the government) to provide a secure environment or help minimise the damage.

Small firms more hesitant about readiness
Small companies lag when it comes to confidence. Only three out of five firms (61%) with fewer than 250 employees say they are confident in their cyber security readiness. The equivalent figure for bigger firms is 71%. Smaller firm respondents are also less certain that their executive management prioritises cyber security and are more likely to question whether their IT technology is up to the job.

The smallest gap between large and small businesses is on the issue of potential damage to a company's brand if client and partner data is not handled securely. They agree unequivocally, 72% of large companies and 70% of small agreeing or strongly agreeing.

Reality of cyber risk

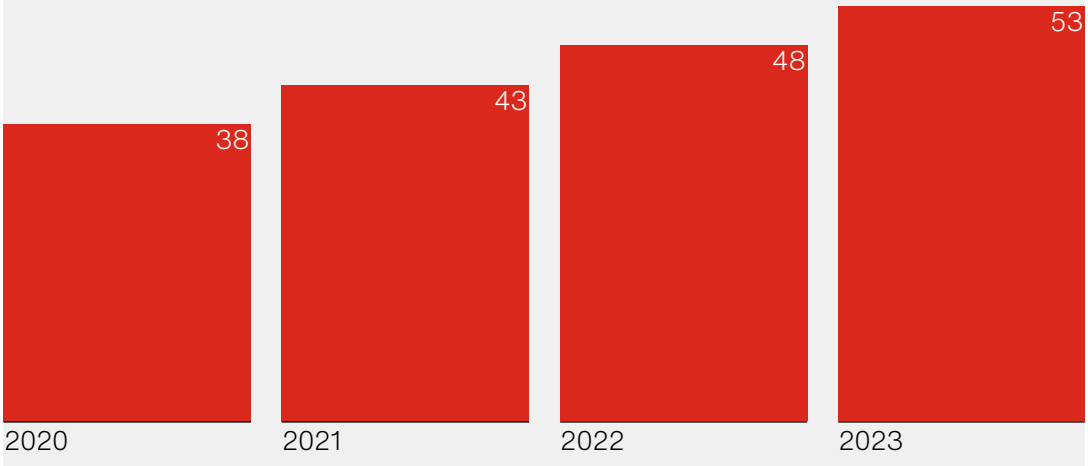
Scope and intensity of attacks rise but financial impact is contained.

Smallest of firms now caught in the cyber net

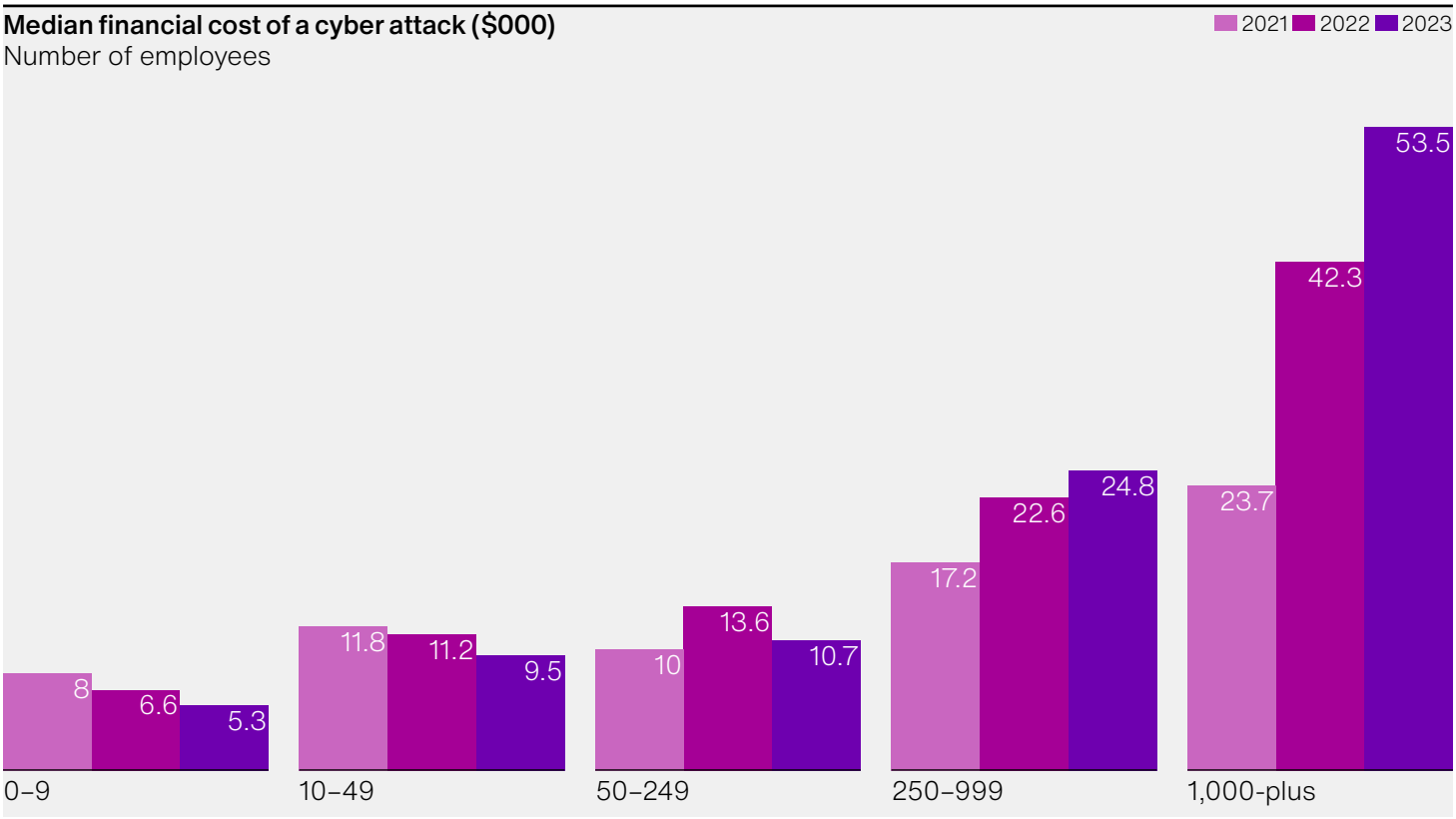
The proportion of firms reporting one or more cyber attacks has risen for the third year running – to 53%, up from 48% last year – while the intensity of attacks has increased sharply. Firms reported a median average of seven attacks, up from four last year.

These figures tell only part of the story. For the largest companies, those with 1,000-plus employees, cyber attacks are now becoming commonplace. Seven in every ten (70%) reported at least one, up from 62% a year ago. This is not just a big business issue. In the last three years, the number of those with fewer than ten employees experiencing an attack has increased from 23% to 36%. Though small businesses may be managing costs better and starting to invest more in cyber security, there is clearly an increasing risk that they must take seriously.

Companies suffering at least one cyber attack (%)



Median financial cost of a cyber attack ($000)
Number of employees



Financial impact steady
Despite this surge, the financial impact of cyber attacks has fallen slightly year-on-year, suggesting firms are getting better at spotting and disrupting attacks. There was a small increase in the number of companies that successfully defended against an attack (8% versus 7% the previous year).

Taking median figures, the cost of attacks has dropped from just under $17,000 to a little over $16,000 per targeted company. The median for the largest single attack also fell from $6,650 to $5,350. However, these numbers mask a wide range of outcomes – from $2,140 for firms with up to nine employees to $10,700 for firms with 1,000-plus employees.

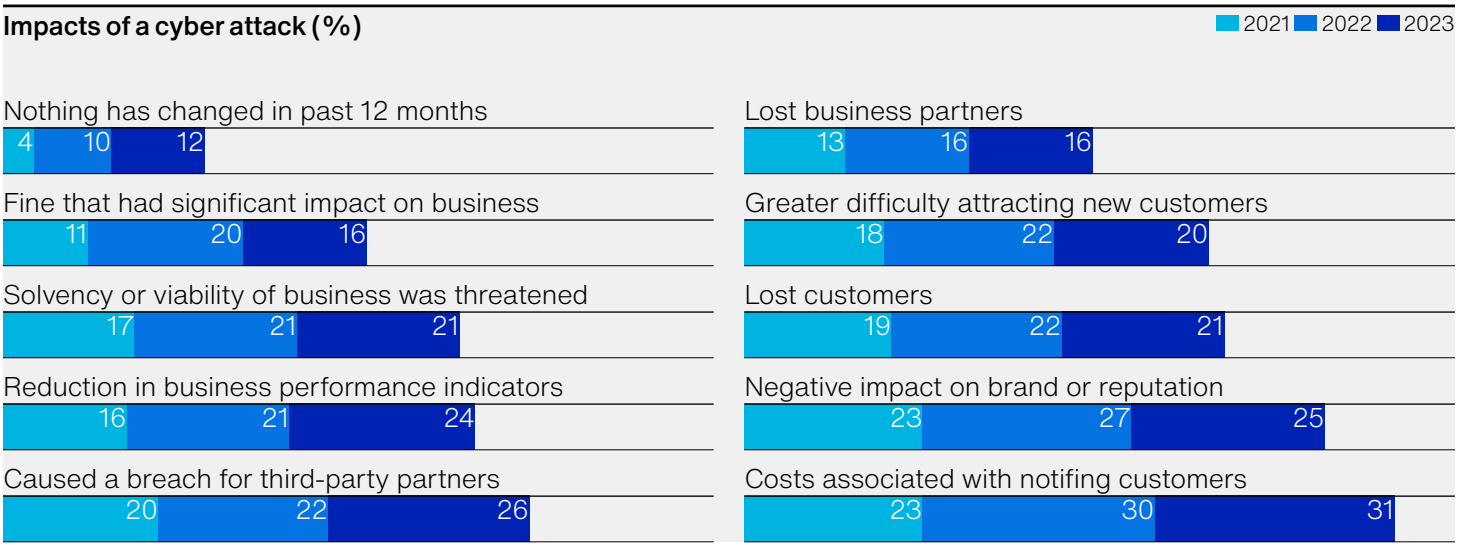
In our 2022 report, only four companies reported cyber attack costs of over $5 million. This year there were eight companies in that bracket and three at the $10 million-plus level. One in eight firms (12%) suffered costs of $250,000 or more.

Small firms better at managing costs
There is some encouragement to be taken from this year's figures. Smaller firms are doing a good job of containing the costs of cyber attacks. Firms in the bottom two size categories have seen median costs fall two years running. It is all the more remarkable given the incidence of attacks has risen for small companies over the last three years, just as it has for larger ones. However, costs are still rising for firms in the top two categories. For businesses with 1,000-plus employees, cyber attack costs have risen 125% in two years, to around $53,500.

Costs vary widely by industry
Four sectors suffered median costs of $20,000 or more – manufacturing, transport and distribution, energy (which has featured among the top three targets for each of the last three years) and government and non-profit. Both the transport and distribution and government and non-profit sectors saw significant cost increases year-on-year (28% and 83% respectively). Manufacturers reported the highest median loss for the single worst attack – at $7,161.

The good news is that most industries managed to contain or reduce the median cost of the single largest attack suffered. For energy firms, the figure is down from more than $11,000 to just under $7,000 over two years. For the food and drink industry it has more than halved, to $4,500.

Impacts of a cyber attack (%)



Vulnerabilities and impacts

The favourite entry point for hackers was once again business email compromise, mentioned by 35% of targeted companies (and 40% of government and non-profit respondents). The corporate server, whether owned in-house (mentioned by 31%) or in the cloud (mentioned by 29%) came second and third. In both cases those percentages were way down on the previous year, suggesting preventive work is having an effect.

The energy sector appears particularly prone to breaches of a corporate owned server. The construction sector tops the list of industries hit with a cloud server breach alongside travel and leisure, as well as technology. The most common outcome of a cyber attack was financial loss due to payment diversion fraud (mentioned by 34% of attacked firms, up from 28% two years ago). Loss of data and virus outbreaks dropped for the second year running.

Some of the knock-on effects of cyber attacks were felt more widely this year than before. Nearly a third (31%) of firms that were attacked reported increased costs for notifying customers of an attack. The figure is up for the second year running. The same is true of those reporting a breach for third parties, up over two years from 20% to 26%.

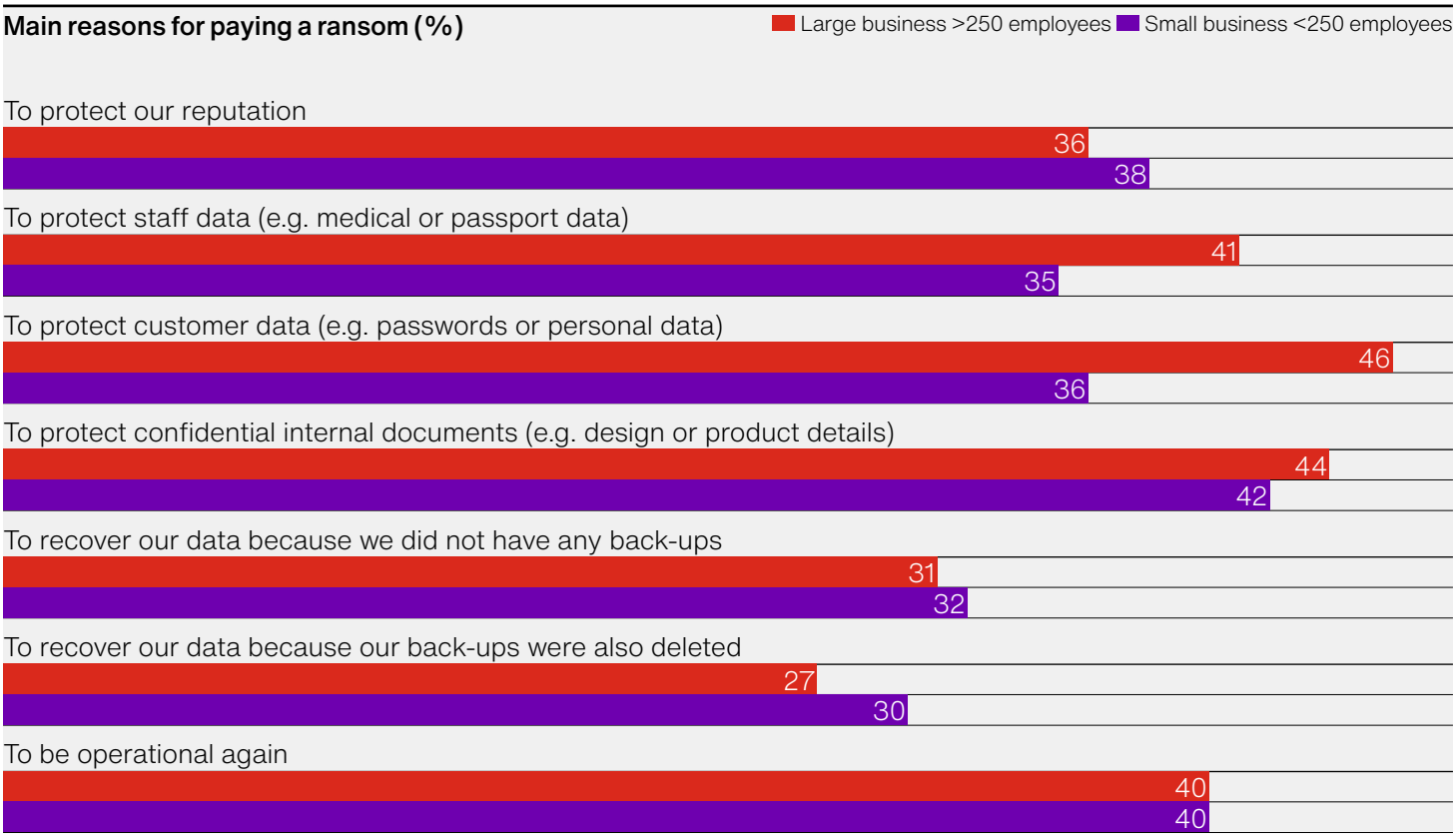
It is worth noting that the disaster scenario is not as remote as one might believe. One-in-five firms (21%) that were attacked said the impact was enough to threaten the viability of the business. That was also the case for a fifth of the very smallest firms.

Country by country: Ireland stands out

Which countries were most vulnerable? In terms of number of firms attacked, Ireland stands out this year with more than seven-in-ten firms (71%) targeted, a third more than the average for the study group as a whole. Irish firms were also targeted almost three times as often as the average median and were significantly more likely to be targeted with ransomware (30% compared with 20% on average across the study group). More than half of respondents in Ireland said the first point of entry was via the corporate owned server (57%) or a cloud server (50%).

In financial terms, the worst hit countries were the UK (with median costs per firm of $24,200), The Netherlands ($21,400) and the USA ($20,000). For US and UK firms, business email compromise ranked top, mentioned by 38% and 37% respectively.

There was a sharp jump in the number of German firms reporting attacks – up from 46% to 58% – with the median number of attacks per firm rising from six to ten. By contrast, two countries – Belgium and The Netherlands – saw a fall in the median average number of attacks experienced. It may be relevant that The Netherlands was the only country in our study to have upped its average cyber readiness score in our maturity model this year.



Ransomware is a continuing threat

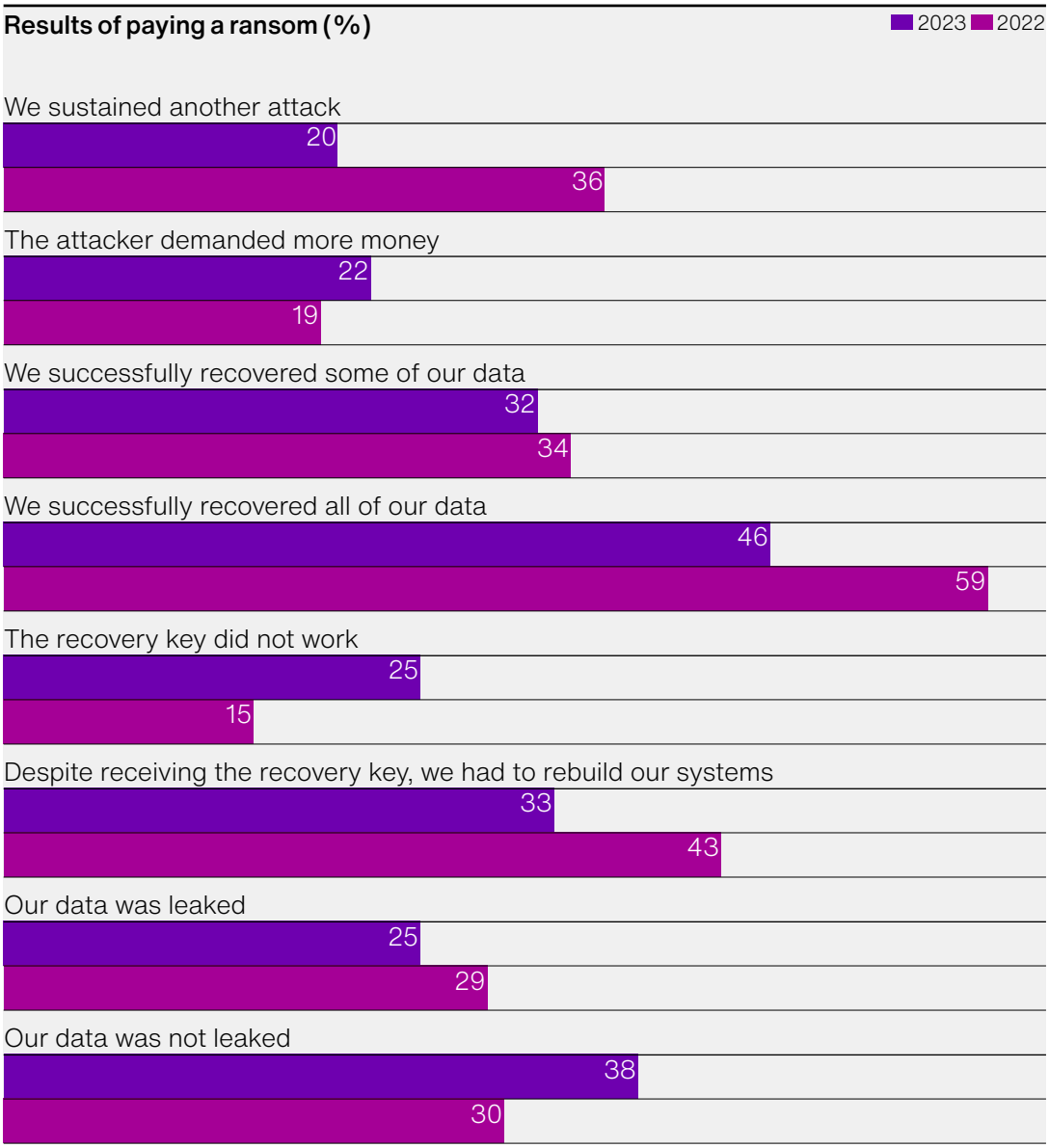
One-in-five of firms that were attacked (20%) received a ransomware demand, slightly up from 19% the previous year. The proportion paying the ransom fell from 66% to 63%, but the median ransom rose 13% to $10,700. On the same basis, average recovery costs fell slightly, to $5,400 and the maximum amount paid out was $535,000. The median figure for the single largest attack was $5,350, up from $4,000 the previous year. The main reasons given for paying the ransom were to protect confidential internal information (43%) or customer data (42%). The latter was the stand out reason among large companies for paying a ransom.

The principal route in for the hackers was once again via phishing emails (mentioned by 63% of victims). For three years, phishing has been far and away the main source for a ransomware attack. The second most common method of entry remains credential theft. Defending against both begins with employee training. Ransomware is never simple, but training employees on complex passwords, protecting their credential information using multi-factor authentication (MFA), and phishing training are relatively easy and inexpensive ways of mitigating the risk for companies of any size.

Did it pay to pay?

In many cases, no. The proportion of victims saying they successfully recovered all of their data after paying up was just 46%, down from 59% the previous year. Around a third (32%) said they recovered some of their data, but in a quarter of cases data was either leaked or the recovery key failed to work. Also, one-in-five firms (20%) sustained another attack.

Encouragingly, more firms recovered their data this year from back-up (46%), though nearly a third of those attacked (32%) said they paid up because they had no back-up. That was up from 26% the previous year. For those scoring poorly on our maturity model, the top reason for paying a ransom was to be operational again (44%), meaning those that are least prepared have little option but to pay. It's essential to getting their business back up and running. But with only 46% of firms recovering all their data after paying and 22% experiencing further demands from attackers, is that a risk worth taking? When it comes to cyber security, being more mature gives firms a chance at recovering from ransomware without paying, or mitigating the attack in the first place.


Results of paying a ransom (%)
2023
2022
We sustained another attack
20
36
The attacker demanded more money
22
19
We successfully recovered some of our data
32
34
We successfully recovered all of our data
46
59
The recovery key did not work
25
15
Despite receiving the recovery key, we had to rebuild our systems
33
43
Our data was leaked
25
29
Our data was not leaked
38
30

Case study
Business paralysis in an instant

Ransomware attack
It started as a normal working day at Autobedrijf de Pee, a Dutch car repair shop. The receptionist was away so the owner, Arjan de Pee, was keeping an eye on incoming emails. He spotted one from KPN, the mobile network, with an invoice attached. He opened it with the intention of printing it off.

It felt like everything immediately went black. "*All systems failed*," he says. "*All I was shown was a black screen with plain white text – like in the old days of DOS*."

Next steps
Arjan immediately tried to reduce the damage by disconnecting the network cable. This made no difference. All files were already permanently encrypted. "*A text file was placed in each folder with the message that the files were blocked and would only be unblocked against payment in Bitcoin*" he says.

Arjan called his IT company instead. They acted quickly and were able to reinstall the programs. The business was up and running again in an hour.

The cost
The financial damage was limited to paying for the IT company's help and the installation of some extra cyber security measures. But the emotional damage was considerable. "*Our company has existed for 34 years, and I have lost all the photos of our opening,*" he says: "*we'll never get them back*."

Key lesson
All of this has driven home one message Arjan sees as important for other entrepreneurs: "*It is wise to take extra measures to protect your belongings.*" That includes digital assets. Arjan now protects his customers' data using access controls, and he makes sure any critical data is backed-up and stored separately.

Cyber criminals may still be able to attack, but at least there's another barrier in place to protect his customers' personal information. "*In addition, I now ask customers to provide only the most necessary personal information.*"

Further guidance
Arjan has other tips for entrepreneurs. One, that you map out what happens if all your computers fail. How do you get your business going again as quickly as possible? What is needed for that to happen? And how can business processes be started offline? Two, learn how to prevent a cyber attack and discuss this with all your employees. Start with the small stuff such as providing long and complex passwords for all computers.

Building resilience
Prepare a proactive strategy – and back that with spending.

How should firms build resilience?
There are two ways of looking at cyber risk management. One is a proactive attitude. The other is a reactive, or defensive, attitude. The businesses in our study group overwhelmingly sit in the former camp. Nearly half (48%) are primarily motivated by positive drivers while only 6% lean more towards the reactive or negative drivers. Top positive motivations include wanting to reassure customers the firm takes cyber security seriously (27%) and avoiding business interruptions (26%). Negative drivers focus around satisfying regulatory requirements (25%) or acting because customers demand it (17%).

The same proactive attitude percolates down to the smallest firms – those with fewer than 50 employees – but here the stand-out driver is the desire to avoid business interruption. Firms that did not sustain an attack this year were more likely to be positively motivated – with 56% of non-attacked firms acting proactively compared with 42% of attacked firms. So if a proactive mindset is the way to go, where should companies be focusing?

What factors predict a cyber attack?

A cyber maturity assessment evaluates how effective your security controls are at managing the risks a company faces. The more mature an organisation's defences, the better equipped it is to prevent a cyber attack or minimise the impact.

Though a cyber attack is not wholly predictable, looking at our Hiscox Cyber Maturity Model this year, lack of focus on the following ten maturity attributes can indicate an attack is likely.

- Conducting vulnerability assessments and penetration tests.
- Testing new software for vulnerabilities.
- Enforcing multi-factor authentication (MFA).
- Centrally aggregating and storing security data.
- Inspecting encrypting communications.
- Providing virtual private networks (VPNs).
- Identifying new hardware, software and data assets on the network.
- Detecting suspicious network communications.
- Fixing security vulnerabilities.
- Monitoring and analysis of security event data.

What are the experts doing?
Cyber experts are firms that score over four out of five within our cyber maturity model (view full results of this year's assessment on page 14). There continues to be only a few that meet the mark – just 3% this year.

Energy firms have proportionally more experts (6%), followed by financial services and government (4%). Larger companies are least likely to be among the lowest scoring group ('novices'). Only 20% of 1,000-plus employee companies are novices compared with 42% of the smallest (1-9 employees). There are also 1% fewer remote workers in expert firms.

One of the big differentiators for firms classified as experts is board-level buy-in to cyber security. Some 86% of them say top management has a clear view of how cyber security is managed; only 57% of novices can say the same.

Key actions by our cyber experts

Fewer than 250 employees

✔	Ensuring multi-factor authentication is used for sensitive or privileged access to IT systems, such as access to personally identifiable information (PII), remote access and systems administration functions.
✔	Controlling communications between networked devices, for example using a host-based firewall such as Windows Defender.
✔	Proactive identification and removal of malicious software, for example using antivirus (AV) or endpoint detection and response (EDR).
✔	Backing-up data to a secure remote source to eliminate the potential for unrecoverable data loss.
✔	Managing the lifecycle of software patches and necessary updates for IT systems and software.

More than 250 employees

✔	Proactive identification and removal of malicious software, for example using antivirus (AV) or endpoint detection and response (EDR).
✔	Centrally aggregating and storing security event data.
✔	Supporting, permitting and enforcing the encryption of data stored on portable devices such as smartphones and laptops.
✔	Inspecting encrypted communications entering and leaving systems, for example blocking potential harmful content.
✔	Ensuring every user has a consistent and unique identity or username across IT systems.

Cyber security median spend ($)
Number of employees

	1-9	10–49	50–249	250–999	1,000-plus
2023	8,100	47,900	147,700	922,000	4,900,000
2022	4,600	35,300	60,200	938,800	5,500,000
2021	2,000	20,000	59,300	355,800	2,500,000

The link with cyber budgets

Not surprisingly, money is also seen as important. Bigger cyber risk budgets are prominent reasons for feeling more cheerful about the cyber threat. Some 45% of bigger firms that say their exposure to cyber attack has gone down cite bigger budgets and better risk reduction solutions as a reason why. That is up from 36% the previous year. It begs the obvious question: is there a link between the size of budgets and reduced cyber risk? There are tentative reasons for thinking so this year.

As mentioned earlier, smaller firms have managed to reduce the median cost of cyber attacks despite their greater intensity. At the same time, smaller companies in the 1-9, 10-49 and 50 to 249 employee segments have materially upped their median spending – by 77%, 36% and 145% respectively. Over two years, firms with less than ten employees actually quadrupled their median cyber security spending. By contrast, at the top end – firms with 250 or more employees – median spending has been trimmed this year. Here the financial impact of attacks has continued to rise.

Looking at the country data, Belgian firms spent less on cyber security than any other group – $69,000 as a median average, down from $144,000 the previous year. Median losses from cyber attacks nearly doubled. 62% of respondents reported costs of $10,000 or more – nearly twice the average for the study group. By contrast, German firms were the biggest spenders, at a median of $212,000, and saw a reduction in losses from $21,000 to $16,000. Admittedly, German firms have topped the cyber security spending averages for the past three years. But they are the only group that has seen a material reduction in attack costs over that period. One thing is certain: the experts in our survey tend to spend a larger proportion of their IT budgets on cyber: 25% on a mean basis, compared with 23% on average and under 22% for novices.

Money is only part of the resource equation

The number of people being deployed to counter the cyber threat is also relevant. Belgian, Irish and US companies lead in this area with an average 97, 95 and 84 people in the cyber team respectively. They are way ahead of the rest. Yet behind those averages lies an interesting statistic: 15% of US and UK firms are without a managerial role dedicated to cyber security. That compares with just 8% of German firms, for instance. The USA and the UK happen to be two of the three worst hit countries in this year's survey.

The existence of a dedicated cyber security head is one of the key differentiators between the experts and the rest. Only 4% of the firms qualifying as experts this year lacked a role dedicated to cyber. That contrasts with more than a quarter (27%) of the novices. Many of them are smaller companies for whom this is clearly a resource issue. More than a third (34%) of firms with fewer than ten employees said they had no defined role for cyber security. This dropped to 9% for firms in the ten to 49 employee bracket. However, and perhaps more worryingly, smaller firms also lag in less money sensitive areas such as putting in additional security or employee training after an attack.

The importance of risk transfer

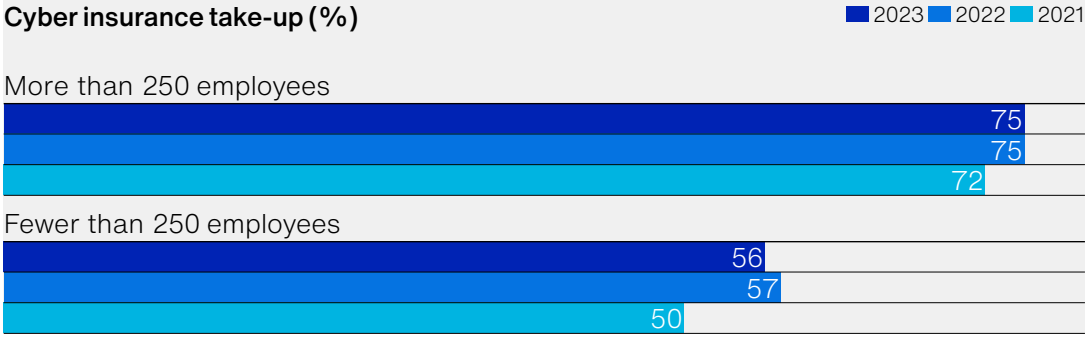
One of the big divides between the experts and the novices in our study group is a willingness to respond to attacks by taking positive action – such as implementing better processes or procedures (44% of the experts said they did this last year compared with just 30% of novices). One of the key actions is to transfer risk by taking out cyber insurance cover.

There is a close correlation between the experience of an attack and the decision to insure. Nearly three-quarters of those attacked (73%) have either a standalone cyber insurance policy or cover within another policy. That compares with just over half (52%) of those who have not been attacked. Firms with cyber insurance are also more likely to take further steps to improve security in the wake of an attack: 36% compared with 29% of the non-insured.

Some 42% of experts say they have a standalone cyber insurance policy, while a further 36% have cyber cover within another policy. By contrast, the equivalent figures for the novices are just 24% and 26%. More than one in five of the novices say they have no plans to take out cyber insurance. Smaller firms (up to 250 employees) lag bigger ones in insurance take-up.

There is a broad spread of motivations for taking out a standalone policy but among experts there is one principal reason: to demonstrate to customers and prospects that the firm is careful about cyber protection. Nearly half of experts (46%) cite this reason – half as many again as the average.

Cyber insurance take-up (%)



2023 cyber maturity assessment

Our cyber maturity model measures firms' alignment with best practice in six domains across three functional areas. 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	Average
Business resilience management	2.90	2.93	3.00	2.94
Cryptography and key management	2.78	2.73	2.86	2.79
Identity and access management	2.99	2.81	2.85	2.87
Security and event management	2.86	2.78	2.69	2.85
Threat and vulnerability management	2.89	2.91	3.28	3.03
Trust management	2.93	2.98	3.02	2.98
Average	2.89	2.85	2.94	2.90

Case study
The vital role of insurance

Total shut down
It's not until you've been shutdown by a cyber attack that you fully appreciate the importance of cyber insurance. That was the key takeaway for the owners of GF Schäfer Trennwandsysteme GMBH, a medium-sized firm in Germany's picturesque Westerwald, after its IT systems all stopped working early one Thursday morning.

While everything was paralysed, there was a readable file in each folder that told them their data files were now encrypted. The company's management were in a state of shock: there had been no reason to think they could be on the hackers' radar as the firm had no patents and no secret data. But, thankfully, they had taken out cyber insurance with Hiscox.

Next steps
Hiscox's response partner stepped in with two crisis coaches. And with the help of the crisis team, it got the firm's processes up and running again quickly.

In addition, the response partner brought in IT forensic experts who worked to find out how the attacker got in. The response team went deep into the firm's systems and were able to understand what had happened based on the log files.

This case study is based on a Hiscox insured's experience, and was not a part of the report's research data.

Legal obligations
Data protection was a concern because it was not possible to know whether personal data had been leaked or not.

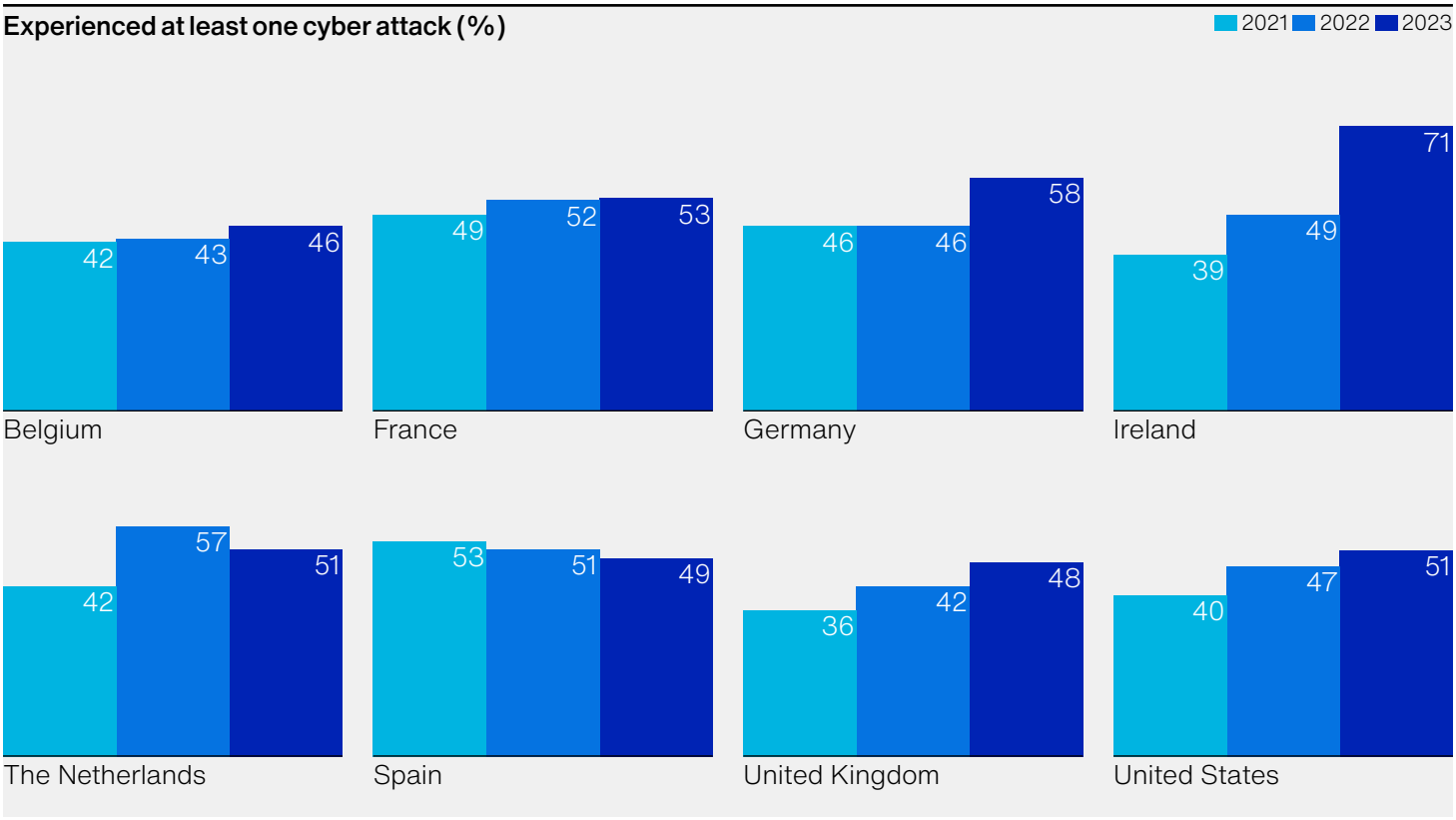
Hiscox provided the business with a law firm which worked with the company's own external data protection officer – who then filed a report with the Rhineland-Palatinate state data protection officer.

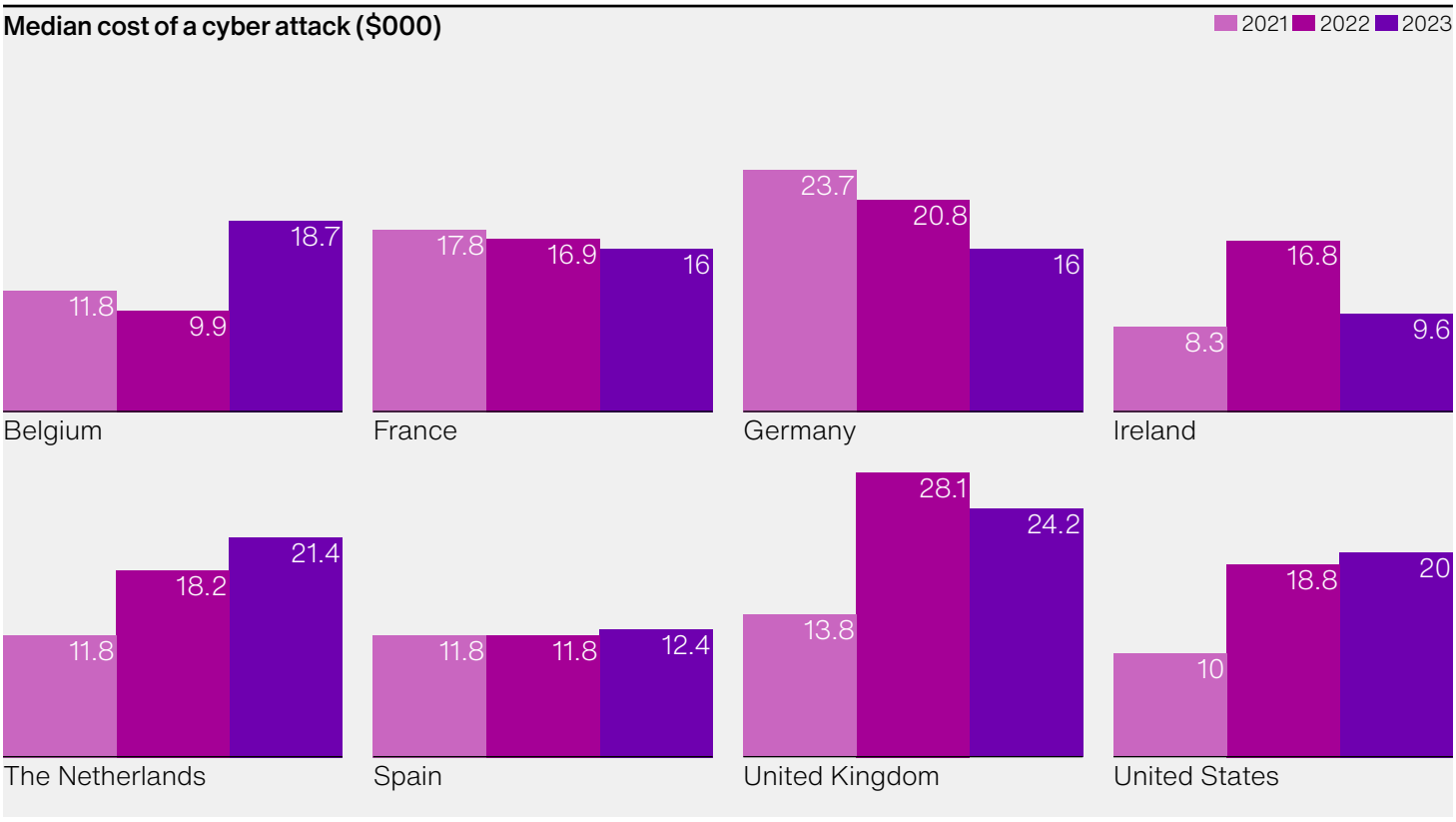
There was a legal obligation to do this but "*it was good to have a competent partner at our side*", said Martin Schäfer of GF Schäfer Trennwandsysteme GMBH.

Public relations
Communication was important, and needed to be actively managed. It was clear that news of this incident would get out, and Hiscox brought in an expert to advise. As a result, the firm went public quickly, which helped build trust and understanding among employees, suppliers and, above all, their customers.

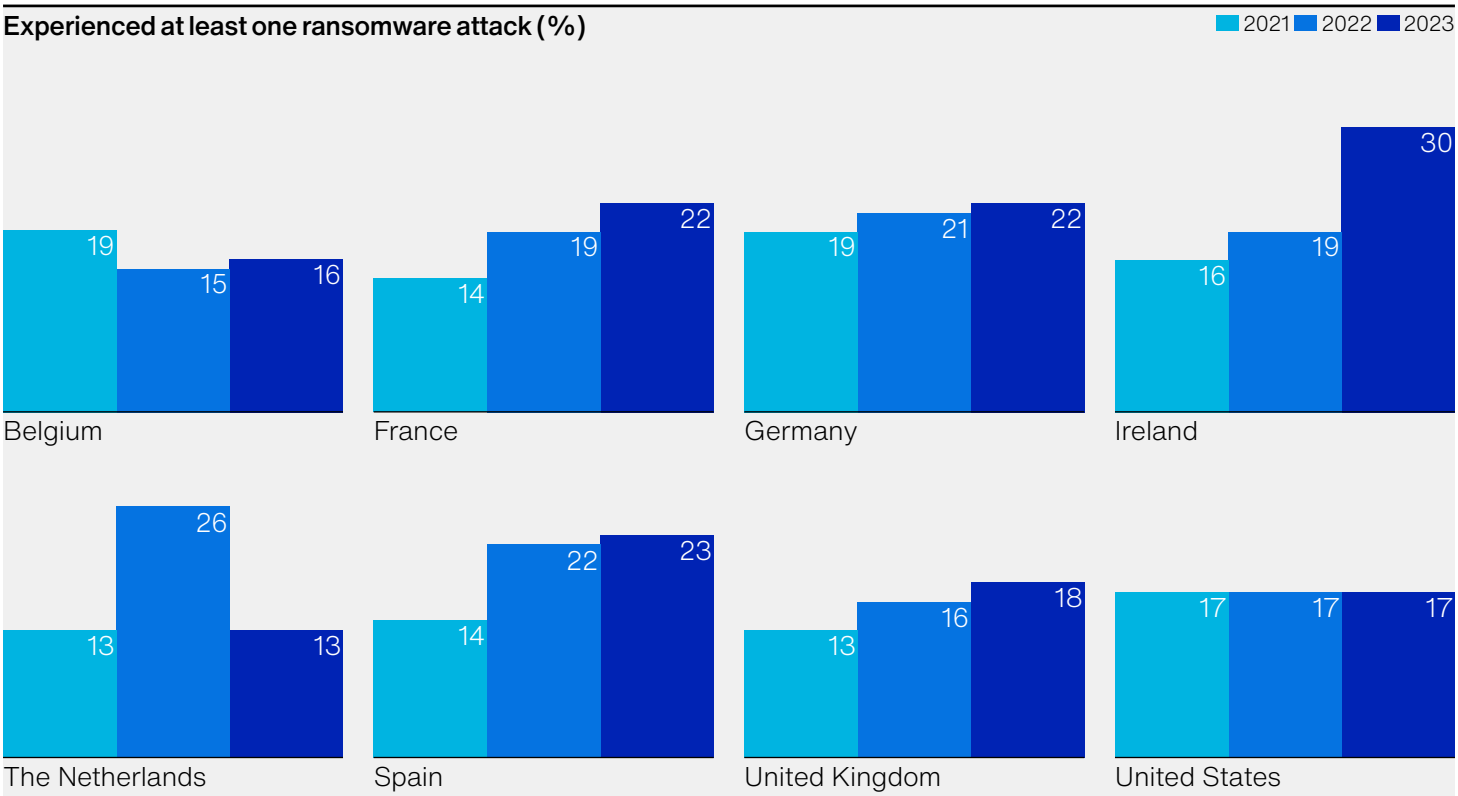
Initially, it was thought that all data had gone. But, with the help of the response agency, the firm recovered a lot in a matter of four or five days. The attack demonstrated the value of insurance. Hiscox's service providers help customers quickly and effectively in the areas of crisis management, forensics and data protection. "*Looking back, it's good that we had many good advisers on our side*." says a director.

Country comparisons

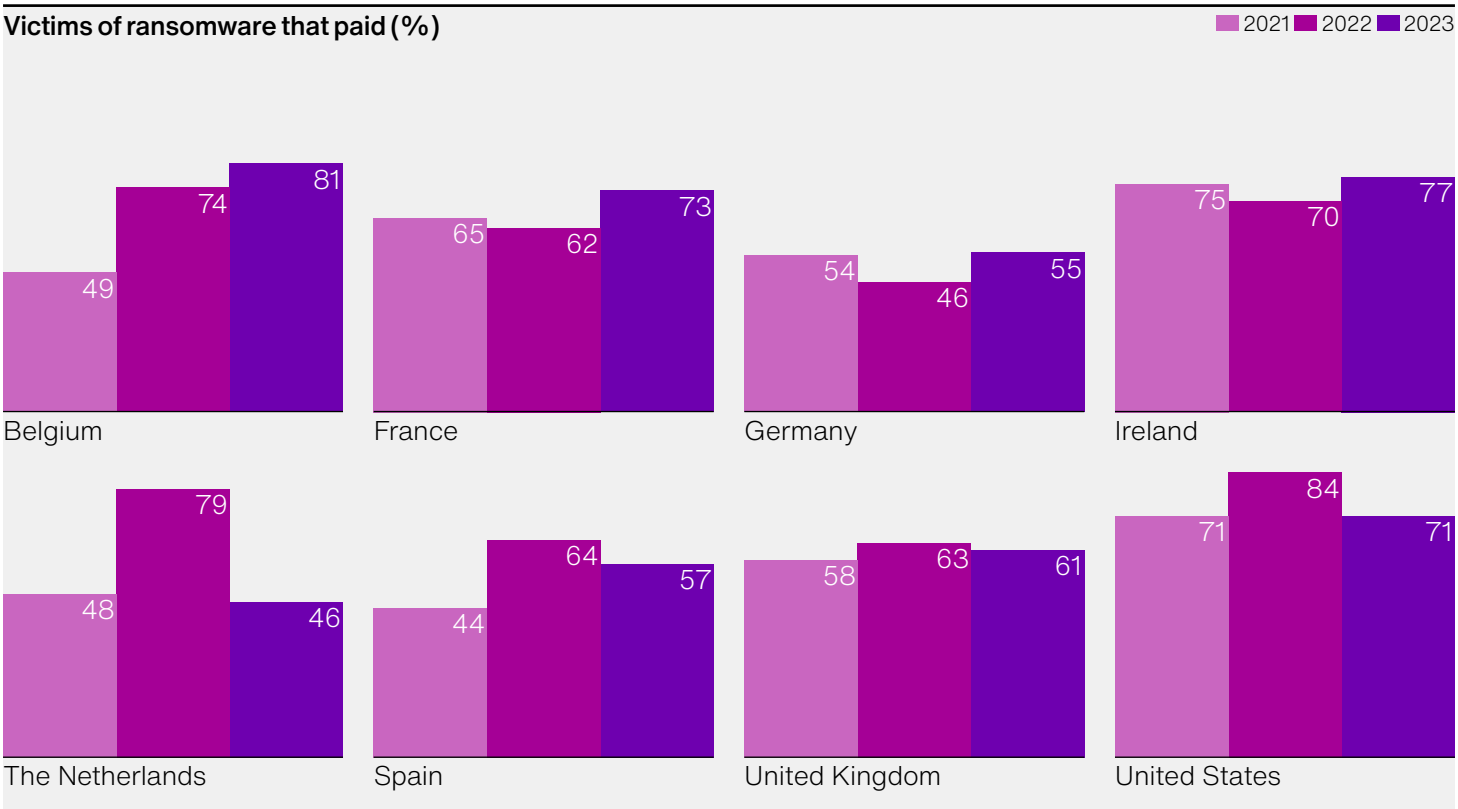




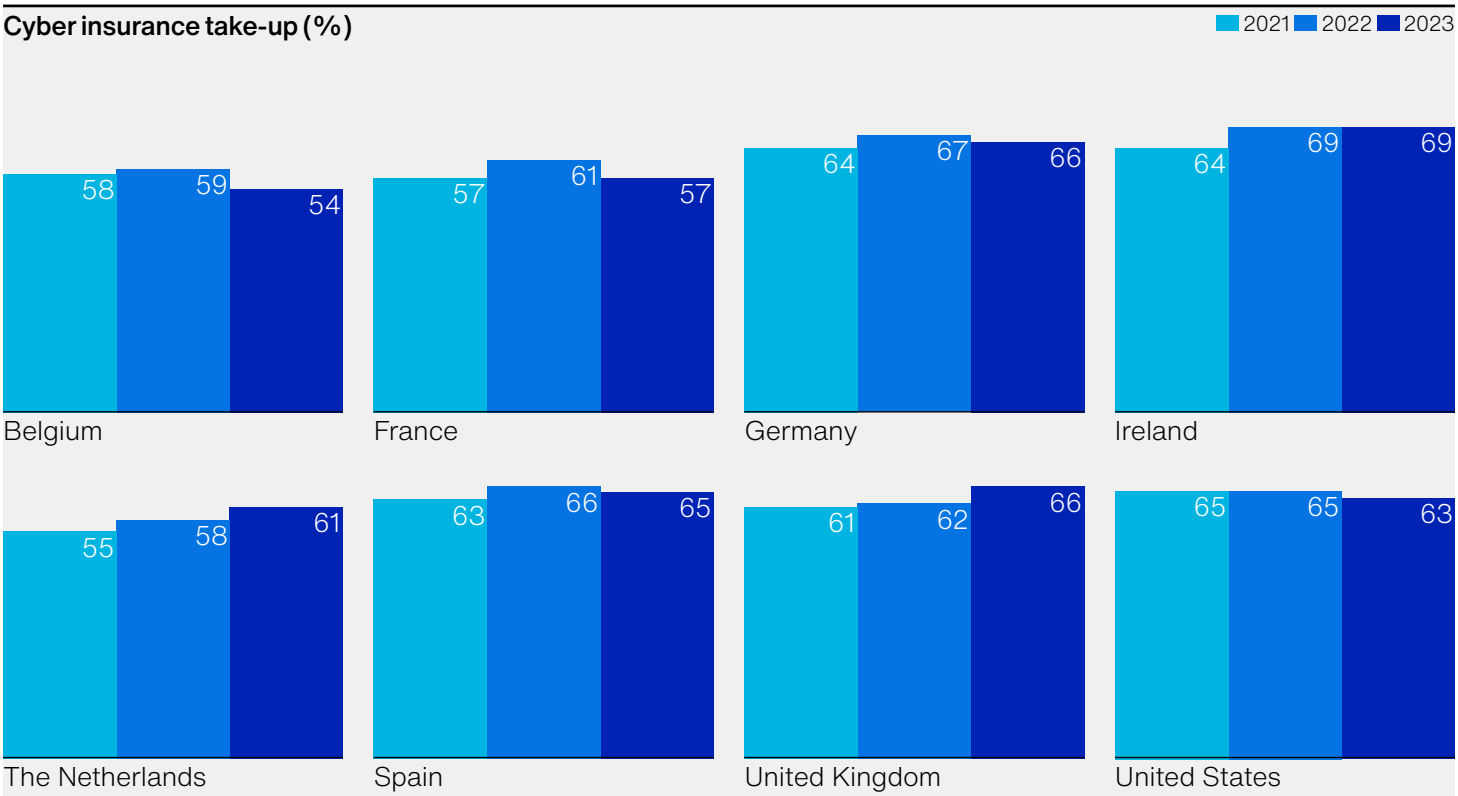
Experienced at least one ransomware attack (%)



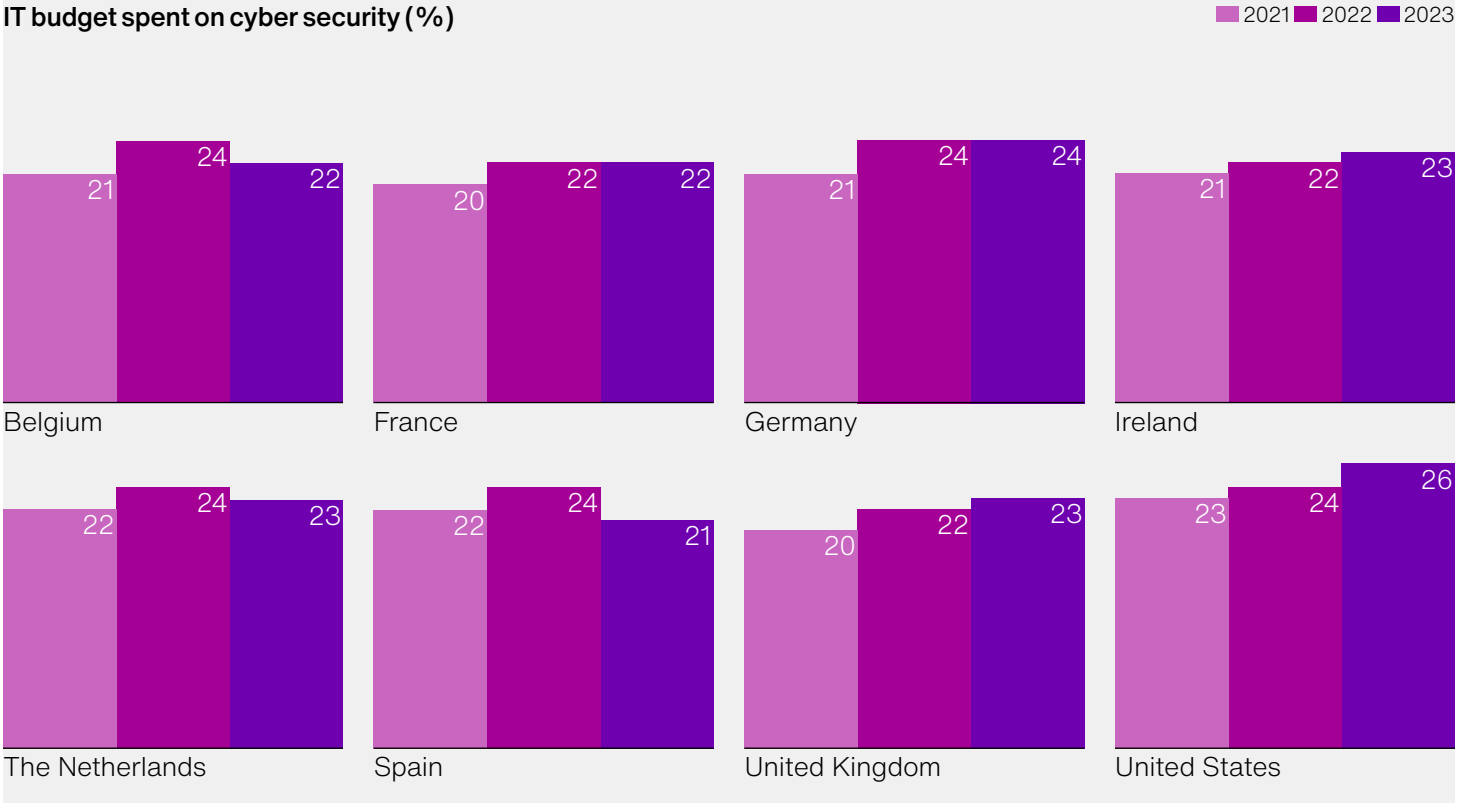
Victims of ransomware that paid (%)



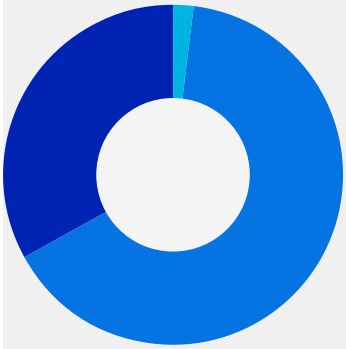
Cyber insurance take-up (%)



IT budget spent on cyber security (%)



Belgium

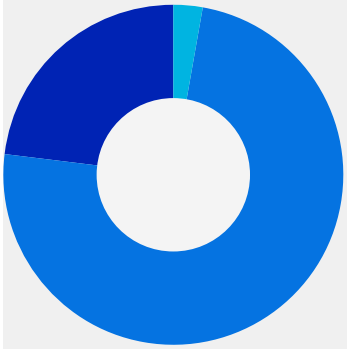


Cyber maturity	%
Expert	2
Intermediate	65
Novice	33

Only country in the study group where cyber is not a top-three business risk.

Spending on employee cyber training nearly doubled in three years.

France

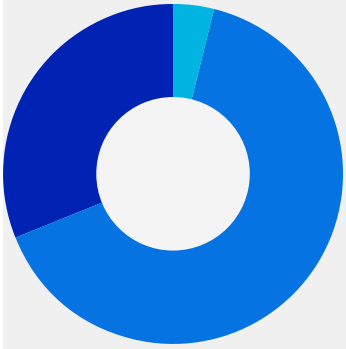


Cyber maturity	%
Expert	3
Intermediate	74
Novice	23

41% experienced payment diversion fraud from a cyber attack.

Top reason to purchase insurance: concern about the security of data.

Germany

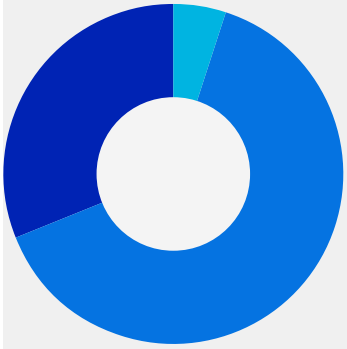


Cyber maturity	%
Expert	4
Intermediate	65
Novice	31

26% increase in cyber attack incidents from last year.

40% rise in payment diversion fraud as a result of a cyber attack.

Ireland

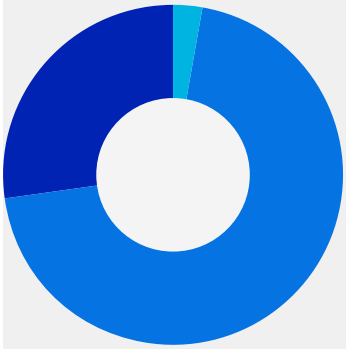


Cyber maturity	%
Expert	5
Intermediate	64
Novice	31

69% of respondents had cyber insurance, the highest in the study group.

50% increase in attackers demanding more money after a ransom payment.

The Netherlands

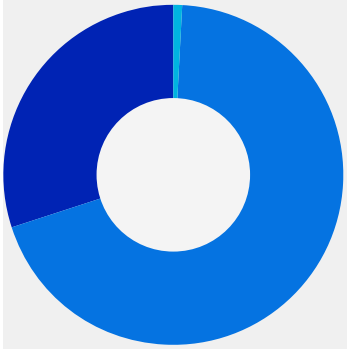


Cyber maturity	%
Expert	3
Intermediate	70
Novice	27

Only country in the study group to increase its cyber readiness score.

50% decrease in ransomware from last year.

Spain

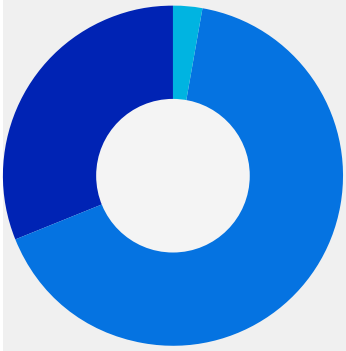


Cyber maturity	%
Expert	1
Intermediate	69
Novice	30

Most common point of entry was corporate server in the cloud.

25% rise in belief that cyber risk is reducing due to increasing cyber budgets.

United Kingdom

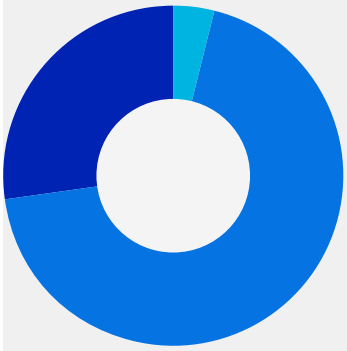


Cyber maturity	%
Expert	3
Intermediate	66
Novice	31

Nearly three quarters believe brand will be damaged if customer data not protected.

Country with second lowest score (48%) for a cyber attack.

United States



Cyber maturity	%
Expert	4
Intermediate	69
Novice	27

Over one-in-five company's solvency materially threatened after a cyber attack.

The number one reason to proactively manage cyber risk: to reassure customers.

Methodology

A total of 5,005 professionals responsible for their company's cyber security strategy were surveyed. This includes over 900 each from the USA, UK, France and Germany; over 400 from Spain; and 200-plus from Belgium, The Netherlands and the Republic of Ireland. Respondents completed the online survey between 9 January 2023 and 2 February 2023.

The full make-up of respondents is detailed below.

Respondents

Employees	%	Level	%
1–9	26	C-level executive	29
10–49	19	Vice president	24
50–249	15	Director	32
250–999	15	Manager	15
1,000-plus	25		

Sector	%	Department	%
Business services	7	Executive management	9
Construction	8	E-commerce	4
Energy	4	Finance	9
Financial services	10	General counsel	4
Food and drink	4	Human resources	7
Government and non-profit	5	IT and technology	18
Manufacturing	8	Marketing and communications	5
Pharmaceutical and healthcare	9	Operations	10
Professional services	8	Owner	14
Property	3	Procurement	4
Retail and wholesale	8	Product management	5
Technology, media and telecoms	18	Risk management	5
Transport and distribution	5	Sales	5
Travel and leisure	4		

One Hiscox customer claims story was used, on page 15.

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 from real experts – crisis managers, IT specialists, data protection lawyers and PR consultants. Since 2018, Hiscox has offered free employee training to all our small-and mid-sized insureds around the globe, partnering with various expert providers.

Sharing our expertise and building awareness
We have built free-to-all tools like our online cyber maturity self-assessment model to help companies understand their cyber security strengths and weaknesses. Using the Hiscox maturity model, compare company performance to over 16,000 other companies.

Keeping you informed about the cyber security landscape
For the seventh year running, we've produced the Hiscox Cyber Readiness Report. Each year, this report 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, it reflects the direct experience of those on the front line of the business battle against cyber crime.

What's your cyber readiness score?
Our cyber maturity model is a free, interactive tool to help you review your company's cyber readiness using industry accepted frameworks.

www.hiscoxgroup.com/cyber-maturity

Hiscox Ltd
Chesney House
96 Pitts Bay Road
Pembroke HM 08
Bermuda

+1 441 278 8300
enquiry@hiscox.com
hiscoxgroup.com

22594 10/23