

The Hiscox Cyber Readiness Report

2017



Contents

2	Executive summary
4	The cyber security challenge
8	The business response
12	Cyber readiness model
18	The way forward
20	Insurance
24	Methodology

Key insights – small businesses

3	Smaller firms hit hardest
5	Impact is higher for smaller firms
11	Small businesses struggle to keep up

The Hiscox Cyber Readiness Report 2017 is compiled from a survey of more than 3,000 executives, departmental heads, IT managers and other key professionals in the UK, US and Germany. Drawn from a representative sample of businesses by size and sector, these are the men and women on the front line of the business battle against cyber crime. While all are involved to a greater or lesser extent in their organisation's cyber security effort, three in five make the final decision on how their business should respond. The report not only provides an up-to-the-minute picture of the cyber readiness of businesses big and small, it also offers a blueprint for best practice in the fight to counter an ever-evolving threat.

1 Foreword

A unique gauge of cyber readiness

It is an old saying, but a true one: prevention is better than cure. In the age of e-commerce and the connected business, it has a particular ring to it. Robust defences against cyber intruders and strong processes for eliminating careless or rogue behaviour internally are now the keys to business continuity and consumer trust. Without investment in prevention, detection and training, firms leave themselves exposed to costly business interruptions and possible brand impairment.

But just how well prepared are most businesses? For the first time, we surveyed those at the sharp end of the battle against cyber crime – the executives, managers and IT specialists in charge of cyber security within their companies – to find out.

We commissioned Forrester Consulting to survey more than 3,000 of these people in Germany, the UK, and US, drawn from a representative sample of organisations by size and sector. As such, this report can be considered as one of the most authoritative of its kind.

The study also provides new perspectives on the scale of the challenge firms face in terms of frequency of attack, financial loss and the time it can take to get back to 'business as usual' following a cyber incident. The ripple effects from an attack can have a long-lasting impact on reputation and client relationships that go well beyond the immediate financial cost.

Importantly, this report also offers a series of practical recommendations for those businesses that still have work to do when it comes to preparing for the cyber risk.

Our cyber readiness model, built on the responses from every company we surveyed, provides a unique gauge of cyber readiness across the three countries and a touchstone of best practice for others to follow.

These recommendations focus in the main on strategy and process. They are not intended as a prescription for throwing more money at the problem but as a roadmap to better practice.

One part of the solution, adopted by an increasing number of organisations, is to transfer the cyber risk to an insurer. The report shows that while a large number of firms have already gone down this route, and many more are preparing to follow, the insurance industry still has a job to do in instilling trust in its policies, delivering clarity over what they cover and simplifying the way they are written.

At Hiscox our aim is to continue to play a constructive role in helping our clients understand and manage the cyber challenge. I hope this study serves as both an informative and useful guide for every business striving to reduce its exposure to cyber risk.



Steve Langan
Chief Executive, Hiscox Insurance Company

2 Executive summary



72%

US firms are the most likely to have experienced an attack with 72% of larger businesses reporting a cyber incident in the past year and nearly half (47%) of all US firms experiencing two or more.



43%

German businesses are the least likely of the three countries to believe that their government's policies are supportive, with only 43% agreeing that their government is doing enough to protect them.



45%

UK firms are the least likely of the three countries to have experienced a cyber-attack in the past 12 months, with 45% saying they have had no incidents in that time.

55%

Take-up of cyber insurance remains heavily skewed to the US with 55% saying they have taken out cyber insurance compared to 36% in the UK and 30% in Germany.

39%

Germany lags behind in terms of cyber readiness. German firms make up the biggest group of cyber novices (39% of the total) while UK and US firms account for 36% and 26% of the total respectively.

45%

UK firms are the most likely to think that a cyber insurance policy is not relevant for them with 45% having no plans to take out insurance.

49%

Nearly half of the 'expert' group in our cyber readiness model is made up of US companies.

33%

Over a third of German firms are not interested in cyber insurance. That is more than twice as high (15%) as the US.

35%

Over a third of UK businesses say that they have changed nothing following a security incident in the past 12 months.

- **The incidence of cyber-attack is high.** More than half of firms (57%) have experienced an attack in the past year and two in five (42%) have had to deal with two or more. Larger companies, particularly those in the US, are targeted most often. The average cost of the largest cyber security incident experienced ranges from €22,000 for very small German companies to US\$102,000 for very large US companies – somewhat lower than the headline figures often seen.
- **It takes time to get back to 'business as usual'.** Although three out of five businesses (62%) took less than 24 hours to uncover their biggest cyber incident in the past 12 months, and a quarter (26%) did so within an hour of its occurrence, nearly half (46%) of businesses took two days or more to get back to business as usual.
- **Cyber security spending is on the increase.** The majority of cyber security budgets (59%) are set to increase over the coming 12 months by at least 5% and one in five firms (21%) will lift spending by a double-digit amount. Nearly half (47%) of firms plan to increase spending on staffing by 5% or more.
- **Attacks prompt more technology spend.** Around a quarter of firms that experienced a cyber-attack in the past year responded by increasing their spending on prevention technologies (24%) or detection technologies (23%), even though most firms already appear to be well invested in both areas.
- **Smaller firms hit hardest.** While big firms incur the highest costs in nominal terms, the financial impact of cyber-attacks is disproportionately high for the very smallest companies. Small businesses also appear more complacent than their larger counterparts however, with 29% saying they changed nothing following a cyber security incident compared to larger firms (20%). In terms of adopting key cyber security initiatives, the gap between larger companies and smaller businesses is greater still. For example, while 62% of larger companies say that practising their crisis communications response is a critical or high priority, only 47% of smaller firms say the same.

- **More than half of firms rank as cyber 'novices' in the cyber readiness test.** Analysing the four dimensions of cyber readiness, we created a cyber readiness model, grading firms as either 'cyber experts', 'cyber opportunists' or 'cyber novices'. The experts accounted for just 30% of the survey group while novices made up more than half (53%), suggesting the majority of companies have some way to go before they can claim to be ready.
- **Six steps for moving from 'novice' to 'expert'.** Our analysis of the gaps between the experts and the novices highlights six areas where the novices can focus their efforts and make up ground. Most are strategy and process-related and do not involve a major financial outlay. The involvement of top management, more employee training, and systematic tracking and documentation are prominent among them. For most companies, throwing more money at the problem is not the answer.
- **Momentum builds behind cyber insurance.** The take-up of cyber insurance appears to be set to accelerate. More than a quarter (28%) of firms say they are planning to take out cyber cover in the coming year.

4 The cyber security challenge

How ready is your business when it comes to the cyber threat?

For every business, dealing with a cyber-attack is no longer a question of 'if' but 'when'. But while spectacular data breaches involving millions of customer details or state-sponsored hacking make the headlines, what is the real picture of the impact of cyber crime on businesses from one person micro firms to multi-nationals?

Drawing on the direct experience of those employees most involved in cyber security within their organisation, our report portrays an unrelenting battle against an insidious enemy – one that involves as many low-level skirmishes as it does set-piece battles.

Cyber attacks come thick and fast

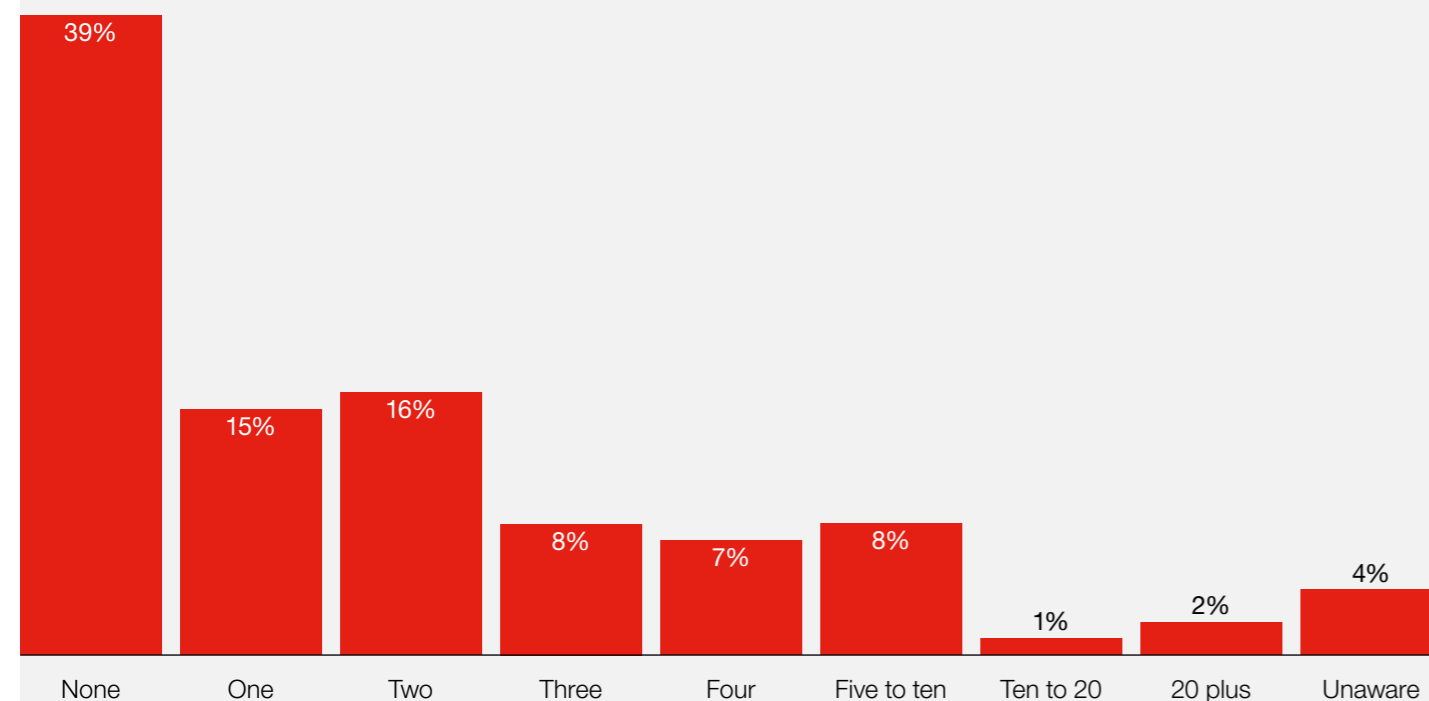
The frequency with which many firms have to grapple with cyber-attacks is striking. Overall, more than half (57%) of respondents say they have experienced an attack in the past year. More than two in every five (42%) have had at least two incidents in that period while a small minority (11%) have had five or more.

US firms appear to be facing the toughest challenge. Some 63% report an incident in the past year and nearly half (47%) have experienced two or more. Two industries in the US have been particularly targeted: transport and distribution, and technology, media and telecoms businesses, where 65% and 59% respectively report two or more attacks.

In Germany, the incident rate is roughly inline with the survey averages (with 56% of respondents reporting an attack in the past year) but significantly higher in three sectors: financial services, manufacturing and technology, media and telecoms (at 64%, 65%, 65% respectively).

UK firms are least likely to have experienced an attack in the past 12 months, with 45% saying they have had no incidents in that time. Technology, media, telecoms appears the most regular target for hackers with 45% of firms here reporting two or more attacks in the past year.

Frequency of cyber attacks in past 12 months



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Companies reporting one attack or more in last 12 months

	Smaller companies	Larger companies
Germany	54%	65%
UK	48%	59%
US	68%	72%

Costs of a cyber security incident

Average estimated cost of an organisation's largest cyber incident in last 12 months

	99 or fewer employees	250 or fewer employees	250 or more employees	1,000 or more employees
Germany	€21,829	€27,776	€36,837	€45,347
UK	£25,736	£29,127	£53,543	£62,712
US	\$35,967	\$41,334	\$81,322	\$102,314

Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Larger companies are top targets

While larger companies, defined here as having 250 or more employees, are generally better prepared and equipped to deal with the cyber challenge (see page 12 – Cyber readiness model), the report suggests they are more likely to be targeted. As the table above shows, larger companies in the US stand out as the most likely victims with nearly three-quarters (72%) reporting one cyber-attack or more.

Costs range to over £500,000 per incident

We asked respondents to think back to the largest cyber security incident of the past 12 months and estimate the financial cost to the organisation – including the effects of business disruption, fines and compensation, loss of revenue and the cost of recovering assets. Where they had experienced multiple incidents, we asked them to come up with an average. More than half of those who had experienced a cyber-attack provided figures.

The results show a wide range of cost impacts – from under £1,000 to over £500,000 per incident. At the top of the range are very large organisations, defined here as those with 1,000-plus employees, where the average cost per incident ranges between €45,000 in Germany and \$102,000 in the US. American businesses appear to be confronted with more serious and costly attacks than their peers in the two other countries, a contention that is supported elsewhere in the report.

Brand damage and loss of business

There are also additional business costs not allowed for in the figures above. For example, among firms that have suffered a security incident in the past 12 months, one in ten admits

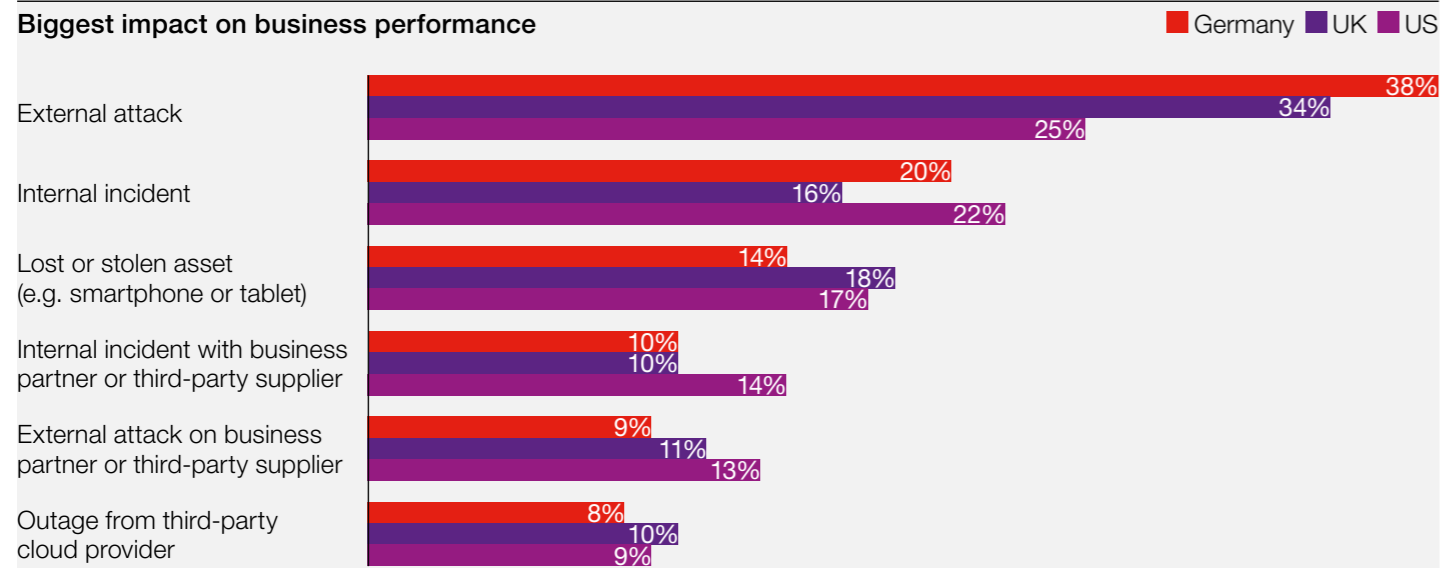
to having lost customers or experienced greater difficulty attracting new ones as a consequence. In the US, the total is nearer one in six (15%). A small proportion (8%) say they have lost business partners and a similar proportion have experienced publicity that has had a negative impact on their brand or reputation. Again the figures are higher for US respondents, at 11% and 10% respectively.

Impact is higher for smaller firms

While big firms incur the highest costs in nominal terms, the financial impact of cyber-attacks is disproportionately high for the very smallest companies (defined here as those with fewer than 100 employees). As the table above shows, the cost per incident for the smallest companies is not appreciably less than for those in the next tier up and far higher per-employee than for the largest companies.

In Germany, for instance, the average cost of a cyber security incident for the very smallest organisations is almost half (48%) the average for the very largest organisations – which are at least ten times their size. In the UK and US, the equivalent figures are 41% and 35%. In relative terms, small companies are paying the highest price for operating online.

Biggest impact on business performance



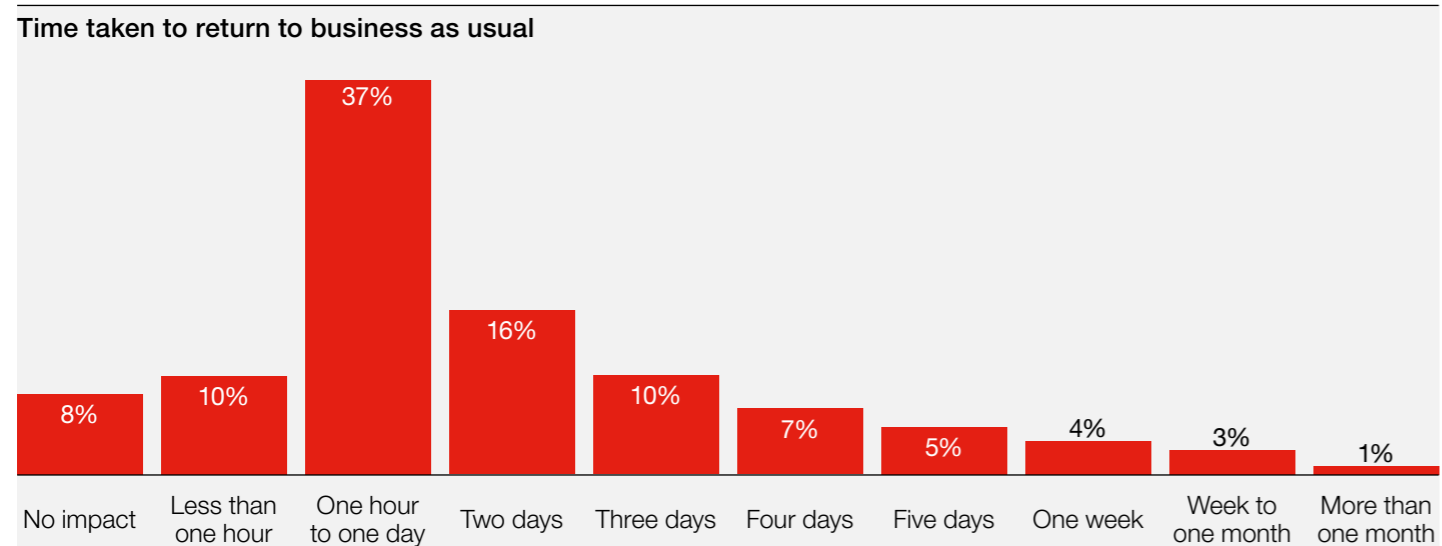
Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Top cyber security challenges by country



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Time taken to return to business as usual



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

External attacks are the key concern

Asked to identify the most common ways cyber incidents occur, 42% of respondents picked 'external attack targeting our organisation'. A similar external attack on business partners or suppliers came second (mentioned by 27% overall and 34% in the US), followed closely by an internal incident (such as an insider threat or HR incident) and lost or stolen devices such as a smartphone or tablet (both 25% overall but 32% in the US).

Asked to rank the different types of incidents according to their impact on the business, respondents put external attacks top of the list. Internal incidents came second, followed by lost or stolen devices. US respondents were more concerned with the potential impact of an internal incident than their UK or German peers (see chart top left – Biggest impact on business performance). This chimes with a number of studies that have shown the majority of incidents result from either negligence or fraud on the part of employees.

Business as usual? Not so fast

Three out of five businesses (62%) took less than 24 hours to become aware of their biggest cyber incident in the past 12 months, and a quarter (26%) did so within an hour of its occurrence. More than a third of respondents (37%), however, say it took them two days or more to discover the problem, but only 1% were still unaware after a week.

In terms of recovery from an attack, nearly half (46%) of firms say it took two days or more to get the business back to normal (see chart bottom left – Time taken to return to business as usual). It must be stressed that this does not necessarily include the time taken to complete an investigation and any remedial work – which could take longer. Three-quarters of respondents agree with the statement that 'when a cyber security incident occurs we resolve the problem in the time we expect it will take'.

There is, however, a marked difference in reported recovery times between the three countries. While 55% of German firms got back to business as usual within one day, only 45% of UK firms and 40% of US firms managed to do the same. And more than a quarter (29%) of IT teams in the US were still engaged in recovery work four or more days later – which may reflect the higher than average cost per incident in the US, noted above. The equivalent figures for the UK and Germany were 19% and 11% respectively.

It is worth noting, while 73% of respondents either 'agree' or 'strongly agree' with the statement that they can 'clearly measure the business impact of security incidents that disrupt our business', that leaves a substantial number (27%) who are presumably using guess-work.

The biggest cyber challenges

We asked all respondents to rate a dozen cyber security issues according to the scale of the challenge they posed. The 'changing/evolving nature of threats' came top by some margin (it was considered either a 'major challenge' or a 'challenge' by 70% of respondents) while four other issues were clustered just below. Once again, US respondents stood out for the high percentage of them that rated each issue as a challenge (see chart middle left – Top cyber security challenges by country).

Larger companies were also generally more concerned about each issue, especially when it came to lack of executive management back-up, lack of visibility within the organisation and dealing with the complexity of the technology environment.

Government support perceived as lacking

Fewer than half (43%) of German businesses believe that their government is doing enough to protect them from cyber security incidents. UK businesses are not much more positive at 48%, although 62% of US companies are happy with their government's support.

The Hiscox view

A sound strategy for dealing with the challenge is essential. Without that, it is difficult to determine where spending should be directed, while there is a danger that day-to-day matters will override any longer-term thinking.

8 The business response

Cyber security spend on the increase

How well prepared are firms to deal with the cyber threat? And how vigorously are they responding in the wake of an attack? There appears to be something of a disconnect between the way firms view their existing operational readiness and the effort being put into upgrading it.

On the one hand, more than three-quarters (77%) of respondents agree or strongly agree with the statement 'We have a clearly defined cyber security strategy' while a similar number (75%) say they are 'very confident' with their cyber security readiness. In both cases, the numbers are highest in the US, at over 80%.

Do these high figures suggest a degree of complacency when it comes to the cyber threat? Possibly, but there is no shortage of commitment when it comes to looking at firms' investment plans for cyber security. The majority are planning to increase their spending in the year ahead by more than inflation – with investment in new technology a particular focus – and there is widespread buy-in for a list of key initiatives.

US and German firms respond vigorously

We asked businesses that had experienced a cyber attack in the past year what had changed as a result. Just under a quarter (24%) said they had increased spending on prevention technologies while 23% were spending more on detection technologies (see chart bottom right – Organisational response to security incidents).

A similar proportion has put in place additional security and audit requirements and say that security and/or privacy are regularly evaluated and discussed. A significant number (20%) are spending more on threat intelligence capabilities and 18% are spending more on incident response programmes.

While these are average figures across all three countries, US and German firms appear to be responding with much more vigour than their UK counterparts. That message is reinforced by the large proportion of UK respondents (35%) who say 'nothing has changed in the past 12 months as a result of security incidents'.

In Germany and the US the comparable figures are 26% and 18% respectively.

Small businesses appear more complacent than their larger counterparts however with 29% saying they changed nothing following a cyber security incident compared to larger firms (20%).

Most firms are stepping up spending.

The majority of cyber security budgets (59%) are set to increase over the coming 12 months by 5% or more, and one in five firms (21%) will lift spending by a double-digit amount. The transport and distribution industry leads the way with 65% of respondents here saying their spending will rise by 5% or more.

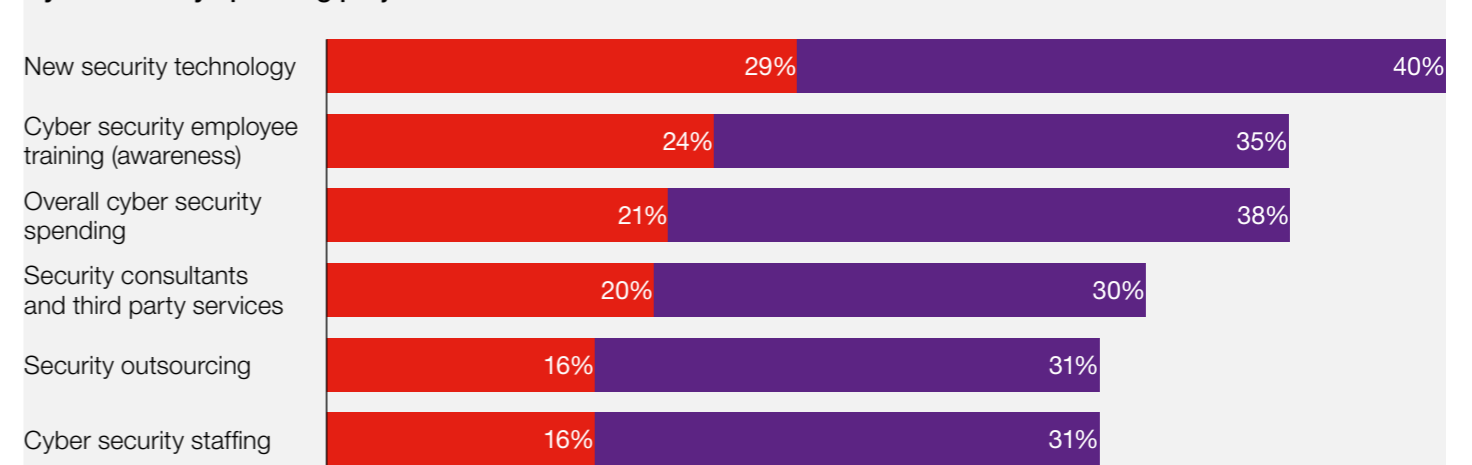
New technology tops the 'buy' list. Given that this is the area where firms already appear to be best prepared (see page 12 – Cyber readiness model) the question is whether other areas are being neglected. However, investment in employee awareness training is not far behind (see chart top right – Cyber security spending projections). Given that nearly seven out of ten (69%) respondents agree that 'employee training has reduced the number of incidents that disrupt our business' the investment looks well founded.

Once again it is US firms that appear the most committed to the counter-offensive. They top the numbers looking to invest by an additional 5% or more in all areas.

Firms are investing in more people

Nearly half of firms (47%) say they intend to increase their spending on cyber security staffing by at least 5% in the year ahead. US firms are most likely to be adding to staffing numbers (54% are planning to do so) even though they already have more people engaged in this area than their counterparts in Germany or the UK. The number of staff committed to cyber security is one of the factors that marks the 'expert' firms from the rest (see page 12 – Cyber readiness model).

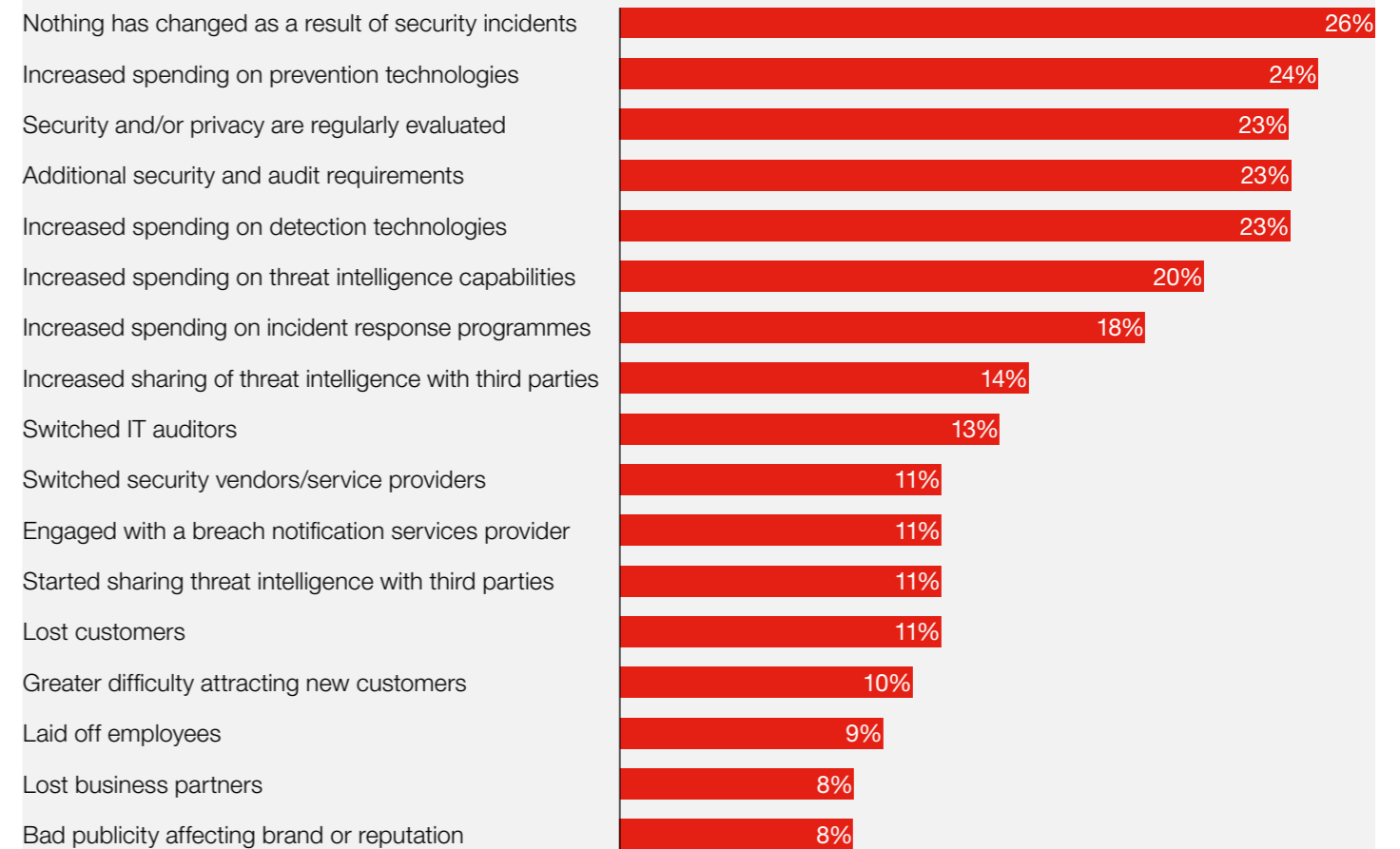
Cyber security spending projections for next 12 months



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Organisational response to security incidents

What has changed in the last 12 months



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.



“ US and German firms appear to be responding with much more vigour than their UK counterparts. That message is reinforced by the large proportion of UK respondents who say ‘nothing has changed in the past 12 months as a result of security incidents’.

Insurance is a key priority

While 40% of firms say they already have cyber insurance, nearly half of the remainder (46%) say they intend to take out insurance in the coming 12 months. Overall, 57% of respondents say they intend to purchase or enhance cyber insurance cover.

Larger companies are more likely to be insured than smaller ones (48% versus 37%) but more than half of both groups intend to buy or enhance cover in the coming 12 months (see page 20 – Insurance).

Small businesses struggle to keep up

We asked firms to tell us what their key security initiatives were going to be in the year ahead and to rank them according to priority. Three initiatives emerged as either a critical or high priority for more than 60% of respondents: ensuring a quick response to cyber incidents (selected by 65% of respondents), addressing existing threats and vulnerabilities (63%) and achieving and/or maintaining regulatory compliance (61%).

However, there is a major gulf between the larger and smaller firms. While the priorities of both appear broadly similar, a much lower percentage of smaller firms are likely to undertake these initiatives. There is typically a 10% difference (see table below).

In some areas, the gap is greater still. While 62% of larger companies say that practising their crisis communications response is a critical or high priority, only 47% of smaller firms say the same. Some 59% of larger companies also prioritise ‘presenting the value of cyber security to executives in business terms’. The equivalent figure for smaller companies is 47%. The figures suggest a substantial proportion of smaller firms are struggling to keep up.

The Hiscox view

Cyber security is not just an IT issue – it is an organisational issue. With our experience showing that the majority of incidents result from the negligence or activity of insiders, it’s not a surprise that our study reveals that increased investment in cyber awareness training for employees is second only to new security technology. Employee training should be one of the most important elements of a cyber security strategy.

Top cyber initiatives for coming year

Number ranking the initiative a critical or high priority

Large companies	
Quick response to cyber incidents	70%
Addressing existing threats/vulnerabilities	70%
Achieving/maintaining regulatory compliance	68%
Leveraging cloud-based or managed security services	66%
Enhancing threat intelligence capabilities	66%
Smaller companies	
Quick response to cyber incidents	64%
Addressing existing threats/vulnerabilities	59%
Achieving/maintaining regulatory compliance	58%
Purchasing/enhancing cyber insurance	56%
Leveraging cloud-based or managed security services	54%

Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

12 Cyber readiness model

Gauging cyber readiness: experts vs novices

How well prepared are businesses to deal with cyber-attacks? As the number of cyber incidents continues to rise, many firms have responded by stepping up their spending on technology, tightening their security requirements or reviewing their incidence response programmes. But are they responding effectively? How much is strategically driven? Does it result in optimum preparedness?

To answer these questions, we conducted a quantitative analysis spanning four dimensions of cyber readiness – strategy and oversight, resourcing, technology and process.

In each area, organisations were asked to score out of five how well they aligned with a series of statements. We then used those scores to rank firms into ‘cyber novices’ (those with the least developed approach to cyber readiness), ‘cyber opportunists’ (firms that are well prepared in some, but not all, areas) and ‘cyber experts’. To rank as an expert, an organisation had to achieve an average score of 4.0 or more.

The strategy and oversight statements covered key aspects of strategy from implementation and integration to the existence of metrics to track return on investment and impact on the business. Resourcing spanned everything from training and knowledge transfer to the formal involvement of the firm’s leaders.

The technology and process statements covered the main technology capabilities for detecting and combating cyber intrusions and the policies and procedures for responding to them effectively.

As the table below shows, firms scored highest in the area of technology. This may in part reflect the fact that the respondents include a heavy weighting of technologists to a greater or lesser degree, but it also shows that technology tends to be the easier solution to implement – either by outsourcing and/or spending more. Also, cyber risk typically sits with the IT department rather than the board and IT is more likely to deploy technology as a solution to a problem.

Experts are in the minority

Taking the scores for all organisations, and adjusting the weightings to avoid unfairly favouring larger organisations, we built a cyber readiness model to demonstrate the relative preparedness of the respondents in our study.

The most striking message of this analysis is that the majority of firms are either novices or experts – there are relatively few in between – and the experts make up just 30% of the total. Novices account for more than half of our survey group, suggesting the majority of companies have a long way to go before they can claim to be cyber-ready.

Cyber readiness	
Average score out of five	
Strategy and resourcing	3.66
Strategy	3.66
Resourcing	3.66
Technology and process	3.78
Technology	3.91
Process	3.70

Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Who are the experts? Nearly half of them (49%) are US companies. Large organisations are heavily represented: they make up 37% of the expert group compared with just 27% of survey constituents overall. Multinationals are prominent among them, accounting for 39% of the total. Technology (11%) and financial services firms (10%) are also more likely to be experts.

Who are the novices? German companies make up the biggest group (39% of the total) while UK firms account for 36% of the total. The very smallest companies – those with fewer than 100 employees – and local organisations with operations in only one country are also more likely to rank as novices.

IT leads, but board members lag

One telling feature of the rankings is that directors and members of the executive management within our survey group fare poorly compared with those involved in IT or finance.

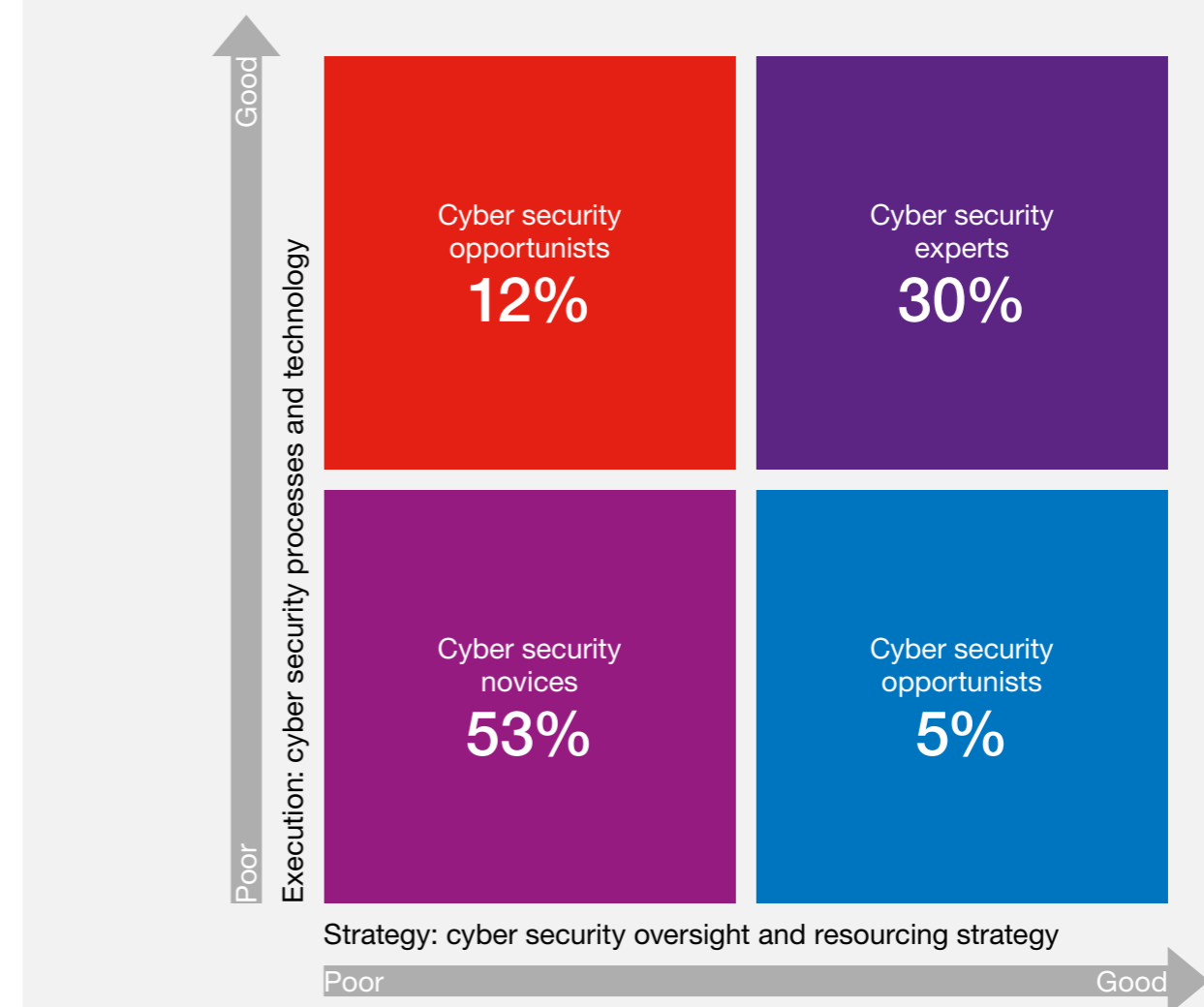
Directors and executives make up 20% of our survey sample, but they account for 23% of novices and only 16% of experts. IT people are over-represented among both opportunists and experts (they make up 48% of the latter compared with a 40% weighting in the survey).

Finance specialists make up 12% of experts compared with a 9% weighting in the survey sample. The figures suggest a lower level of buy-in and awareness at board level for the key elements of cyber readiness.

All is not what it seems

It appears counter-intuitive, but expert companies actually experience more cyber incidents than their less well prepared counterparts (see table top left page 14 – Number of incidents in last year by ranking). They also take longer to return to business as usual – 29% of them take four days or longer compared with 15% of novices.

Cyber readiness model



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Number of incidents in last year by ranking			
	Novices	Opportunists	Experts
None	46%	38%	28%
One	14%	14%	18%
Two to four	25%	32%	37%
Five to ten	6%	10%	10%
More than ten	3%	3%	5%

Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

There are a number of possible explanations. The experts are generally larger companies and more interesting targets for hackers. More than half of them (55%) say external attacks targeting their organisation are the commonest security incidents to impact their business. That is a significantly higher figure than for novices or opportunists (35% and 41% respectively). Greater awareness may also lead to better detection.

As for response times, three-quarters (75%) of them say their biggest cyber security challenge is the complexity of their technology environment. They are also more likely to investigate an incident more thoroughly, increase their spending on prevention and detection technologies or take other action such as switching security vendors and service providers.

It is notable that, while a third of novices (34%) say they changed nothing following an attack, fewer than one in six experts (13%) say the same. For all that, speeding up response times is a priority over the next 12 months for 85% of the expert firms.

What makes an expert?

Respondents who scored high in the rankings share a number of common characteristics.

— **Top-level buy-in.** Nine out of ten experts (91%) say 'cyber security is a top priority for executive management/board'. Only 62% of novices and 79% of opportunists say the same. With this comes a clearly defined cyber security strategy (again mentioned by 91% of experts but only 66% of novices).

— **A cross-functional approach.** Expert firms tend to involve a broader mix of stakeholders from across their organisation when setting their cyber strategy. Around a fifth of them engage people from HR, marketing and communications, product management, procurement and sales in addition to the more obvious functional

areas (see chart top right – Key functions involved in cyber security strategy).

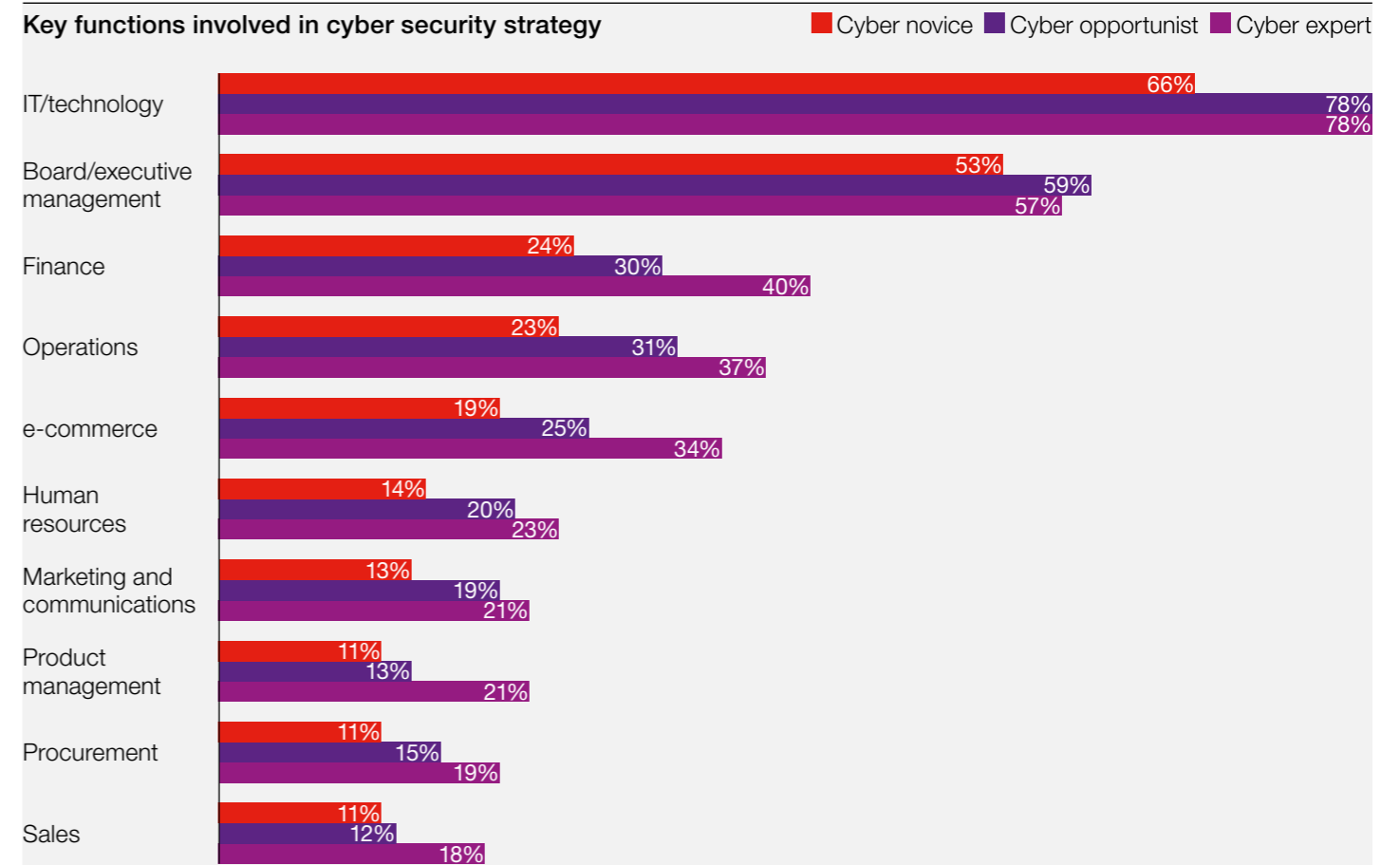
— **Higher spend, more staff.** Experts spend a higher proportion of their revenue on cyber prevention and mitigation, and on average employ twice as many staff on cyber security as novices (16 full-time and nine committing half their time or more). Smaller companies are typically committing a much larger proportion of their workforce to cyber security than larger ones.

The gap between the experts and the novices is widening. More than two-thirds (69%) of experts plan to increase their spending in this area by 5% or more in the coming year. That compares with just over half (53%) of novices.

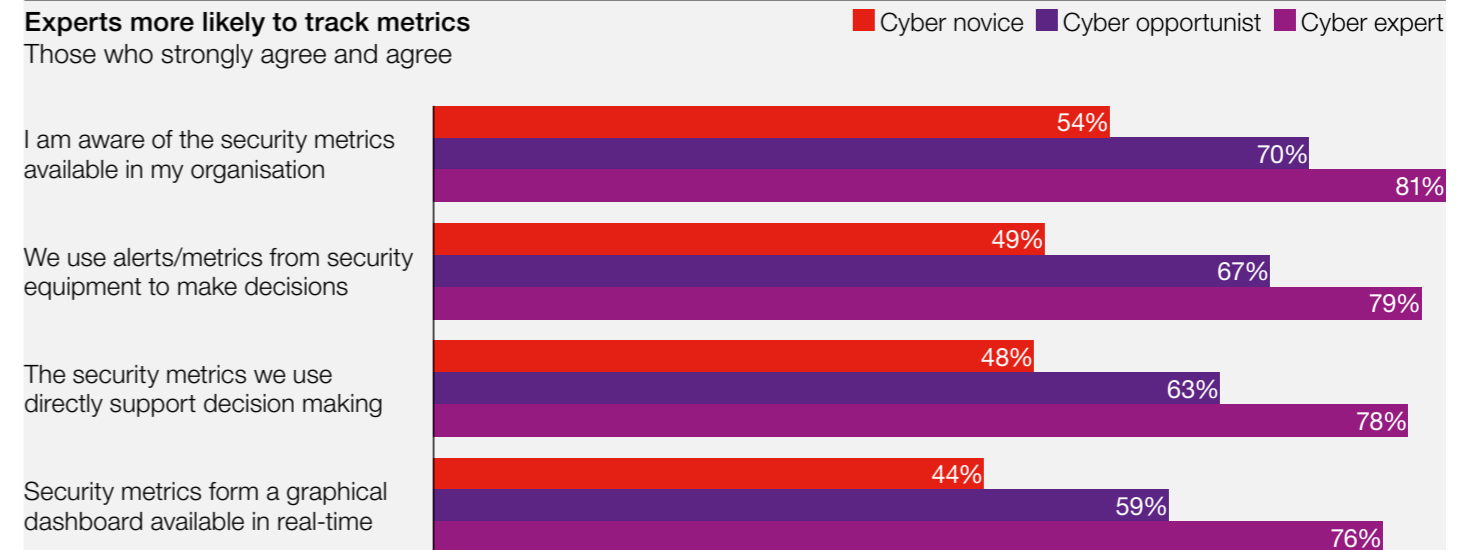
— **More employee awareness training.** Nearly nine out of ten experts (86%) agree that employee training has reduced the number of incidents. The figure for novices is 57%. Experts manage their training better. And two-thirds of them (66%) are planning to increase their spending in this area in the year ahead by 5% or more (compared with 54% of novices).

— **Better use of metrics.** Four out of five experts (81%) say they are aware of the security metrics that are available within the organisation and a similar proportion (78%) use them to 'directly support decision-making' (see chart bottom right – Experts more likely to track metrics). The equivalent figures for novices are 54% and 48% respectively. Around nine out of ten experts (89%) say 'we can clearly measure the business impact of security incidents that disrupt our business.'

— **Implementation of security standards.** More than half (51%) of experts have implemented the ISO 27001 standard.



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Experts are more 'cyber-aware'

There is a further characteristic shared by most of the experts, though it is less easily defined: they are more aware of the challenges associated with facing today's complex cyber risks and more conscious of the need to continue ramping up the defences.

Confronted with a list of 12 security challenges, the majority of experts tick them all as either 'challenges' or 'major challenges'. That includes the 'inability to measure the effectiveness of our security programme' (ticked by 70% of experts but only 48% of novices), even though the experts are plainly shown elsewhere in the survey to be keen users of metrics.

The experts also understand the need for continued effort on a broad front. As the table, below demonstrates, the great majority of experts see the reinforcement of cyber defences as a near-continuous process.

Experts are twice as likely as novices to label as priorities areas such as compliance with the security requirements of business partners, or the need for organisation-wide awareness training for employees. Greater recognition of the scale of the challenge is part of what defines the maturity of their cyber readiness effort.

The Hiscox view

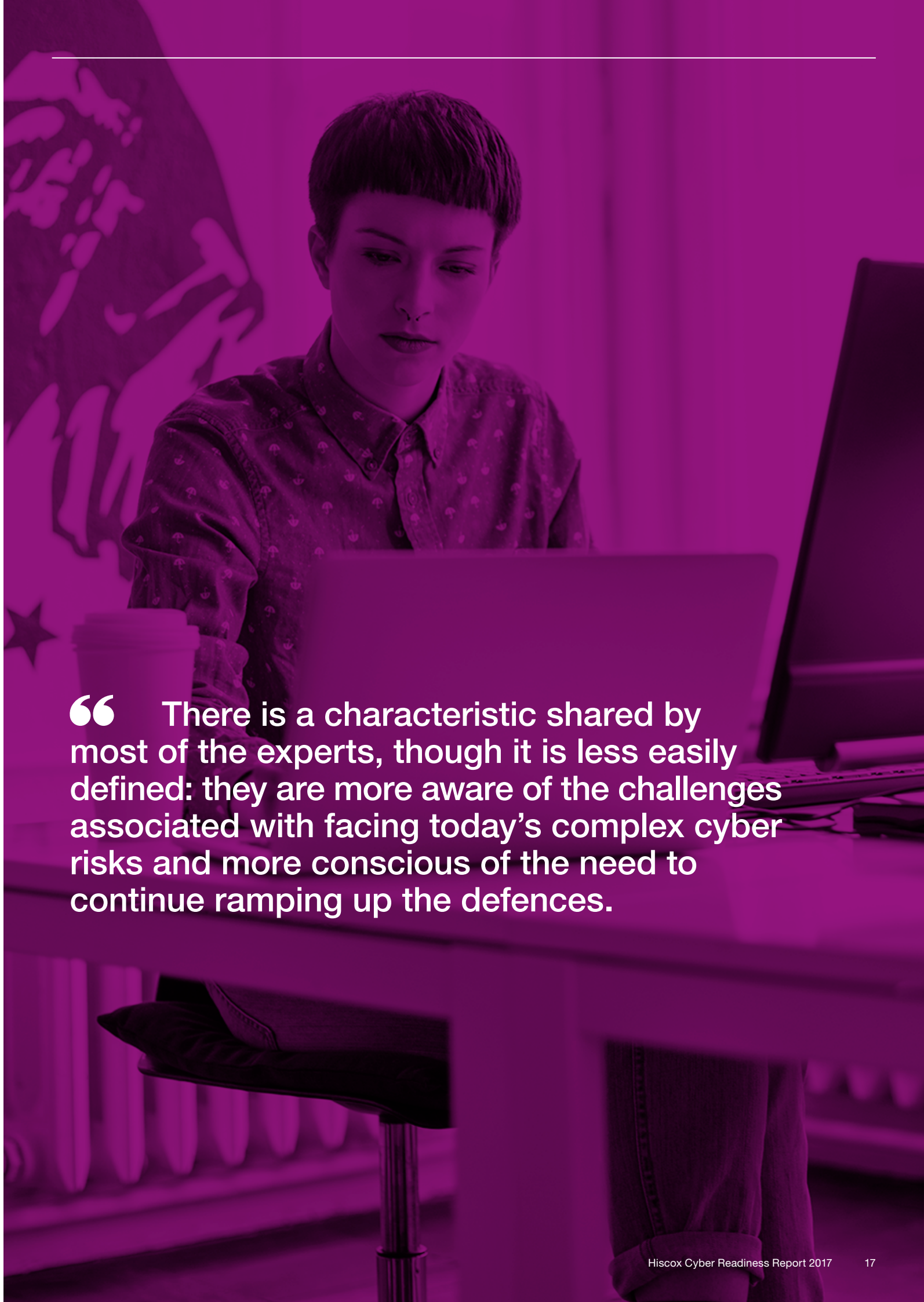
Firms must have a sound cyber security strategy otherwise it is difficult to determine where the spending should go. Simply layering software on software is not the answer. As many of the cyber ready experts point out, complexity becomes its own challenge. The amount of spend is not an indication of success here. It is where and how it fits with an overarching strategy that counts.

Smaller companies are particularly vulnerable as our study shows as they tend to rank as novices in our cyber readiness model and are increasingly attracting the attention of cyber criminals who also see them as possible 'gateways' into larger companies.

Top five cyber priorities for the coming 12 months

	Novices	Opportunists	Experts
Quick response to cyber incidents	51%	74%	85%
Addressing existing threats	48%	71%	82%
Regulatory compliance	46%	68%	83%
Leveraging cloud-based or managed security services	42%	64%	80%
Purchasing/enhancing cyber insurance	43%	61%	80%

Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox



“ There is a characteristic shared by most of the experts, though it is less easily defined: they are more aware of the challenges associated with facing today's complex cyber risks and more conscious of the need to continue ramping up the defences.

18 The way forward

Moving to the next level of cyber readiness

Our quantitative analysis highlights significant gaps in the cyber readiness of more than half the firms in our survey and some catching-up to do on the part of many more. Closing the gaps is clearly desirable for those who lag.

The good news is that this does not have to involve a major financial investment. Most firms already score well in the area of technology so more spending in this area is not necessarily the answer. Analysis of the responses on which our maturity model is built shows that all but two of the ten biggest gaps between those in the novice group and those in the expert group involve strategy and process. These areas are where novice firms should concentrate their efforts.

Firms of all sizes can up their game by following these six steps.

— **Involve top management.** One of the defining characteristics of firms that rank as experts is the involvement of their board and executive management in setting cyber security strategy. Yet, overall, only just over half (55%) of respondents say their top executives are so involved.

The overall responsibility for cyber risk should sit at board level and not with the IT team who need to ensure there is a consistent transfer of cyber security-related knowledge up to the senior management in order to inform the decision-making process. That should be supported by formal, defined interactions rather than corridor meetings.

When asked their priorities for the year ahead, three-quarters of experts included 'enhancing executive management/board engagement in cyber security policies and procedures' and 'presenting the value of cyber security to executives in business terms'. These are common sense goals that are surely relevant for all firms.

— **Formalise strategy.** Experts tend to have a formal cyber security strategy in place with clearly defined structures, processes

and criteria to ensure decisions are based around the needs of the business and its cyber security tolerance. For nine out of ten experts (92%), their strategy includes a budgeting process that is integrated into all security projects and activities. Only 40% of novices can say the same.

Part of the process ensures frequent collaboration between business and IT counterparts to capitalise on opportunities and protect against emerging risks. Cyber security becomes a critical aspect of all relevant planning processes.

Novices have some catching-up to do when it comes to metrics and cyber security data. Only 37% have metrics in place to track security return on investment and impact on business performance while 36% say that relevant and near real-time cyber security data are available as needed. The equivalent figures for experts are 90% or better.

— **Training and resource.** There is a wide gulf between novices and experts in the area of employee training. More than nine out of ten experts (93%) say that their 'organisation incorporates security training and awareness across the organisation'. Among novices, the figure is less than half that, 43%. As we have seen, most experts say employee training is effective at reducing the number of incidents. Stepping up training can be a quick win.

The human resources team has a major role at the highest-scoring firms. Cyber security competencies are reviewed regularly, using established metrics reflecting the different roles and responsibilities. HR is involved in evaluating cyber security capabilities and business requirements to ensure an effective team is in place. Cyber security criteria form part of the performance evaluation of all employees with any cyber security responsibilities.

— **Document process.** Recording, tracking, documentation – these are areas where novice firms have scope for improvement at only moderate cost to the organisation. For instance, while the overwhelming majority of experts (96%) say their organisation has a core source of cyber security guidelines for employees, partners and external users, only 42% of novices are as well organised.

There are also disparities between the two groups in the numbers that document their response plans, measure the effectiveness of their response efforts and operate documented containment processes that involve defined procedures. They also lag behind in gauging the cyber security risk associated with vendors and other third-parties.

Only two out of five (41%) say that all relevant employees receive formal training and testing to ensure they meet the cyber security guidelines. In all the above areas, the overwhelming majority of experts are able to tick the box.

— **Tighten up technology.** The gaps between novices and experts are generally less pronounced in technology deployment, and the opportunists also score more highly here than in many other fields.

Where the novices need to up their game is in internal and external message encryption and the integration of strong authentication throughout the organisation. In both areas, most are a long way behind both the opportunists and the experts.

— **Transfer risk.** Nearly two-thirds of experts (64%) have taken out cyber insurance. That compares with just 28% of novices and 39% of opportunists. Large numbers of experts are also intending to extend their cover in the coming year (see page 20 – Insurance).

The Hiscox view

There are a lot of quick wins that smaller companies can exploit, particularly in the area of training. The human element in cyber breaches is enormous and a modest investment in employee training can have a big impact on cyber readiness. Sometimes it also comes down to companies only focusing on what they do best and not wanting to be distracted by areas where they have less expertise – for those companies of sufficient size, buying in the resource/skillset they need is a good solution. It is also clear that the close involvement of the board and executive management in setting cyber security strategy is absolutely key.

20 Insurance

Momentum builds in cyber insurance

The take-up of cyber insurance appears to be set to accelerate, the report suggests. More than a quarter of firms (28%) say they are planning to take out cyber cover in the coming year. This is in addition to the 40% of respondents who say they are already covered.

Cyber insurance has been one of the fastest growing areas of the worldwide insurance market in recent years as a stream of high-profile data breaches and increasing regulatory pressures have combined to increase risk awareness in corporate boardrooms.

The market has developed most quickly in the US where it has been boosted by the progressive introduction of mandatory notification of data breaches from 2003 onwards. As the survey highlights, take-up of cyber insurance remains heavily skewed to the US. While 40% of respondents overall say they have taken out cyber insurance, the figure for US respondents is 55%. The UK and Germany lag behind at 36% and 30% respectively.

In each case, these figures are higher than generally estimated elsewhere. Financial services emerges as the most insurance-aware sector, with 53% of respondents here saying they already have cyber insurance.

German and UK firms are catching up

Looking ahead, large numbers of respondents in both Germany and the UK say they are planning to take out cyber insurance in the next 12 months. In Germany the number is 31%, in the UK 28% (see chart top right – Cyber insurance). Interest in cyber insurance in Germany has taken off since 2015 when the parliament, the Bundestag, was penetrated by hackers.

The EU's new general data protection regime, which allows for the imposition of financial penalties in the event of a major data breach, is also focusing minds across Europe. It is due to take effect in 2018.

Uptake of cyber insurance is significantly higher among larger organisations in the survey (defined as those with 250-plus employees) than smaller ones (at 48% compared with 37%).

The difference is particularly marked in the UK, where 45% of larger firms say they already have cyber cover compared with 32% of smaller ones, and Germany (39% compared with 26%).

One third of German firms (33%) and nearly as many UK ones (30%) still say they have no plans to take out cyber insurance. In the already well-insured US, the equivalent figure is just 15%.

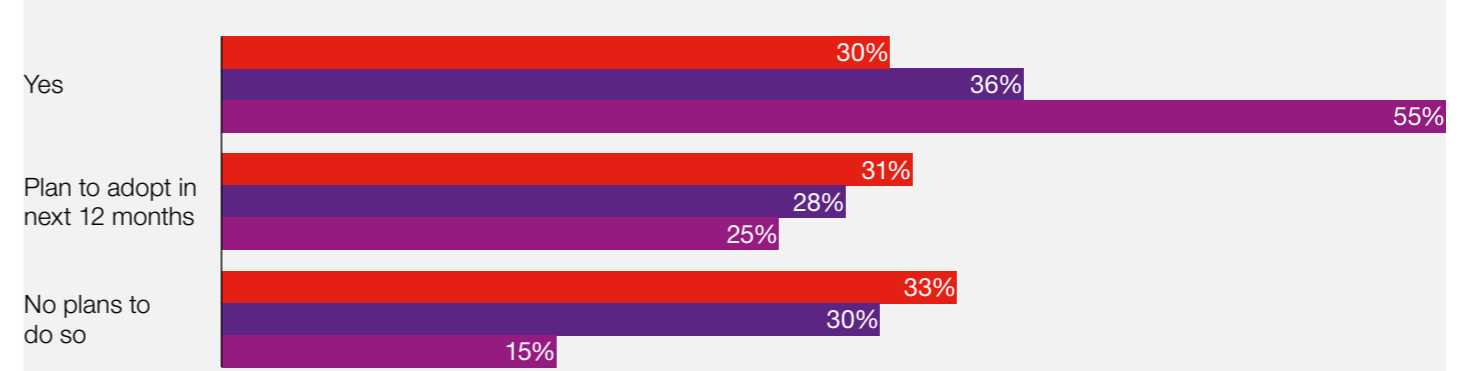
Two big drivers are cited for taking out insurance. The first is the cost of a potential breach and the need for the peace of mind that protection brings (mentioned by 41% of respondents overall and 45% in Germany). The second is concern about data security (mentioned by 40%).

US respondents cite a much broader range of concerns than their counterparts in the UK and Germany (see chart bottom right – Reasons for taking out cyber insurance). It is notable that 36% of US companies mention the impact of new data regulations compared to 26% for the UK and 27% for Germany. Contractual requirements are also driving demand for insurance take-up.

And what about those who have decided not to take out cyber cover – 26% of the survey sample – and have no plans to do so? Two in five (41%) of them say 'a cyber insurance policy is not relevant for me'. The figure is particularly high in the UK, at 45%, and among members of the construction industry (at 53%). This finding highlights the need for continuing education in this area. More than one in six (17%) of those who have no plans to take out cyber insurance agree with the statement 'Cyber insurance policies are so complicated – I don't understand what cyber insurance would cover me for'. Some 7% of smaller firms and even 3% of larger ones say they are 'not sure what cyber insurance is'.

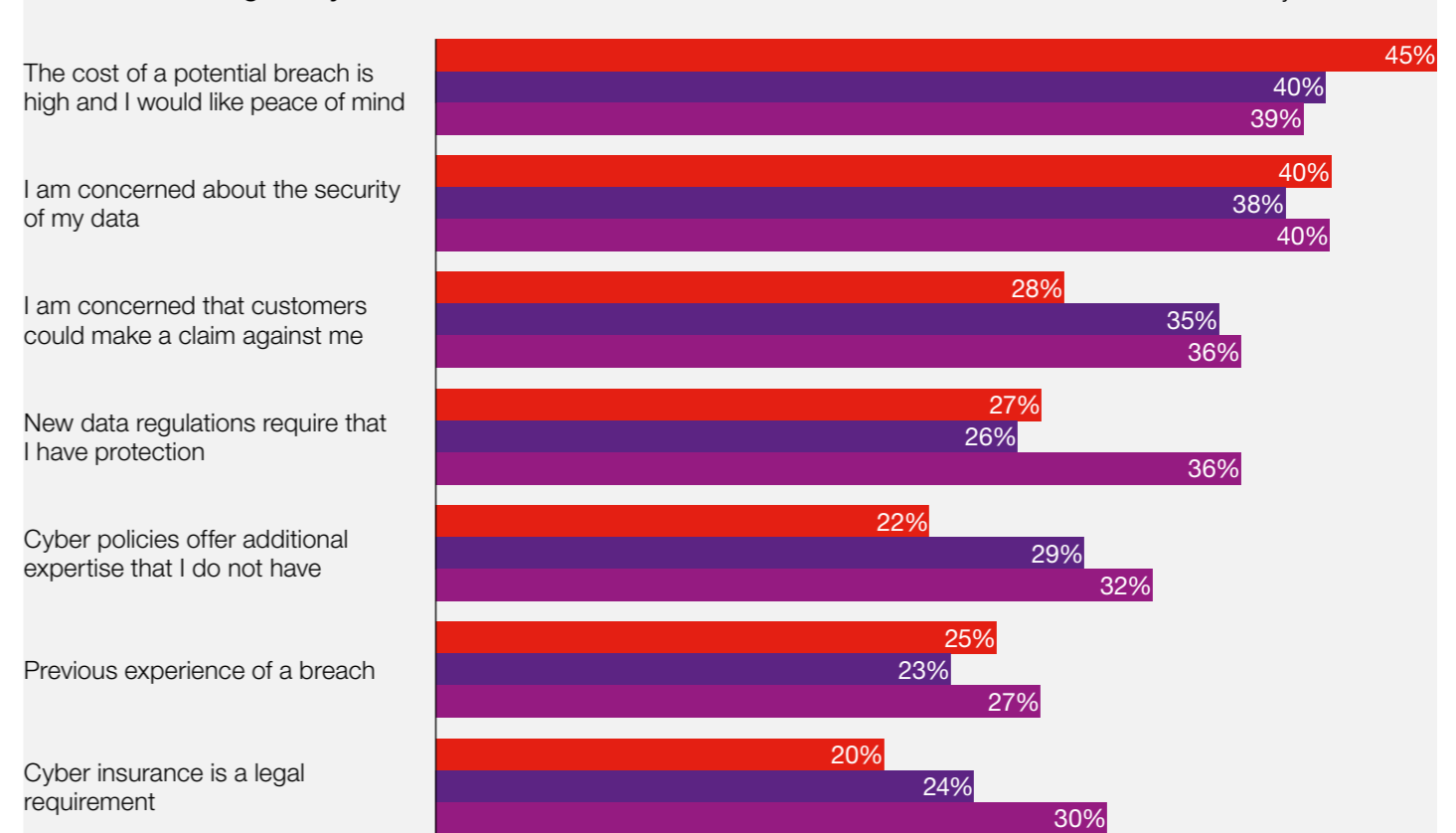
Cyber insurance

Do you currently have cyber insurance?



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

Reasons for taking out cyber insurance



Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

“ Cyber insurance has been one of the fastest growing areas of the worldwide insurance market in recent years as a stream of high-profile data breaches and increasing regulatory pressures have combined to increase risk awareness.

In addition, 29% say they do not trust their insurer to pay out in the event of a claim resulting from a cyber-attack. That scepticism is highest in Germany (32%).

21% of US businesses say they are deterred from taking out cyber insurance because they would have to undertake additional security measures first. That compares with a survey average of 15%.

It is worth noting that 13% of those with no plans to take out cyber insurance say cover is already provided as part of their existing insurance coverage. The number is highest in Germany, at 17%. More than a fifth (21%) of financial services and travel and leisure firms say they already get cyber insurance as part of their other insurance cover.

There is keen demand for add-on services

Many insurers and their agents offer related services in addition to, or bundled with, the insurance package. We asked those firms that had taken out cyber insurance or were planning to do so which of these services were they planning to use. Overall, the level of uptake was high, with larger companies generally more likely to be accessing agents' other services.

Employee training topped the list (taken by 45%). The importance of employee training is underscored elsewhere in the survey, with 69% of all respondents agreeing that 'employee training has reduced the number of incidents'. Among companies that rank as cyber experts, the figure is higher still, at 88%.

Training was followed closely by risk assessments (41%), preventative hardware or software and up-to-date threat intelligence (both 40%). There were, however, differences between countries (see table below).

The Hiscox view

The cyber insurance take-up numbers here appear higher than commonly reported – this may of course be a consequence of some companies thinking they are covered under a different policy. Our results show that education is still a big challenge for the insurance industry in terms of understanding the cyber risk and how insurance can help to mitigate the risk. Given it is commonly understood that cyber insurance policies are complicated, the industry must put more effort into making sure the cover is easier to understand.

The evidence for the demand for add-on services such as employee training and risk assessments also indicates the additional value the insurance industry can bring to the cyber market in terms of preventing and mitigating attacks.

Additional cyber services taken by country

US	
Employee training	49%
Risk assessments	42%
Preventative hardware/software	41%
UK	
Employee training	44%
Up-to-date threat intelligence	44%
Risk assessments	41%
Germany	
Consultation	44%
Preventative hardware/software	41%
Employee training	40%

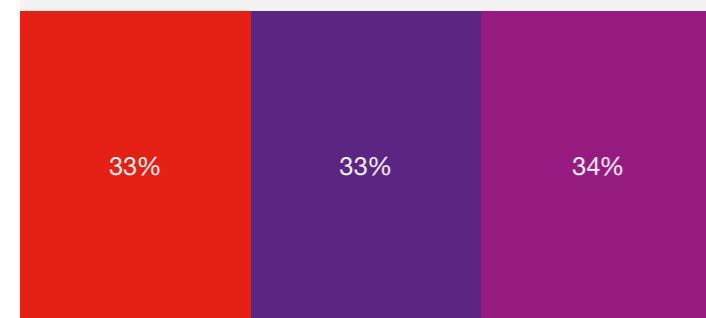
Data from a Nov-Dec 2016 commissioned survey conducted by Forrester Consulting on behalf of Hiscox.

24 Methodology

Profile of respondents

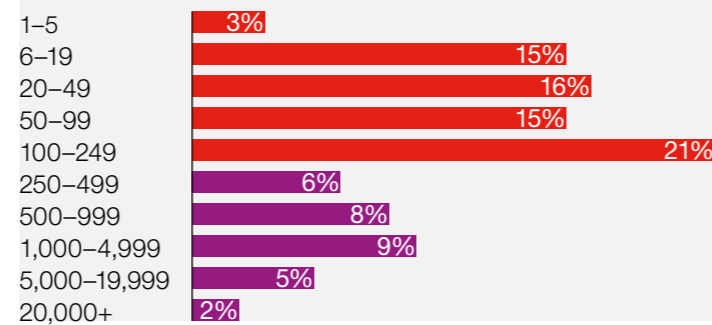
Country in which headquartered

Germany UK US

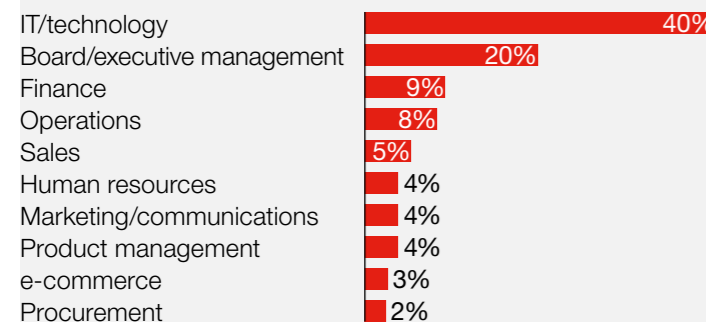


Size of business

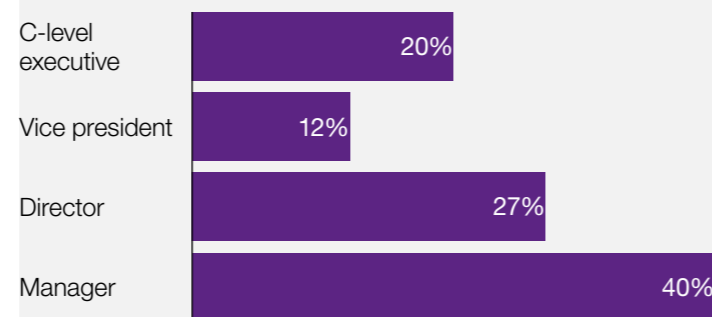
<250+ employees (70%) 250+ employees (30%)



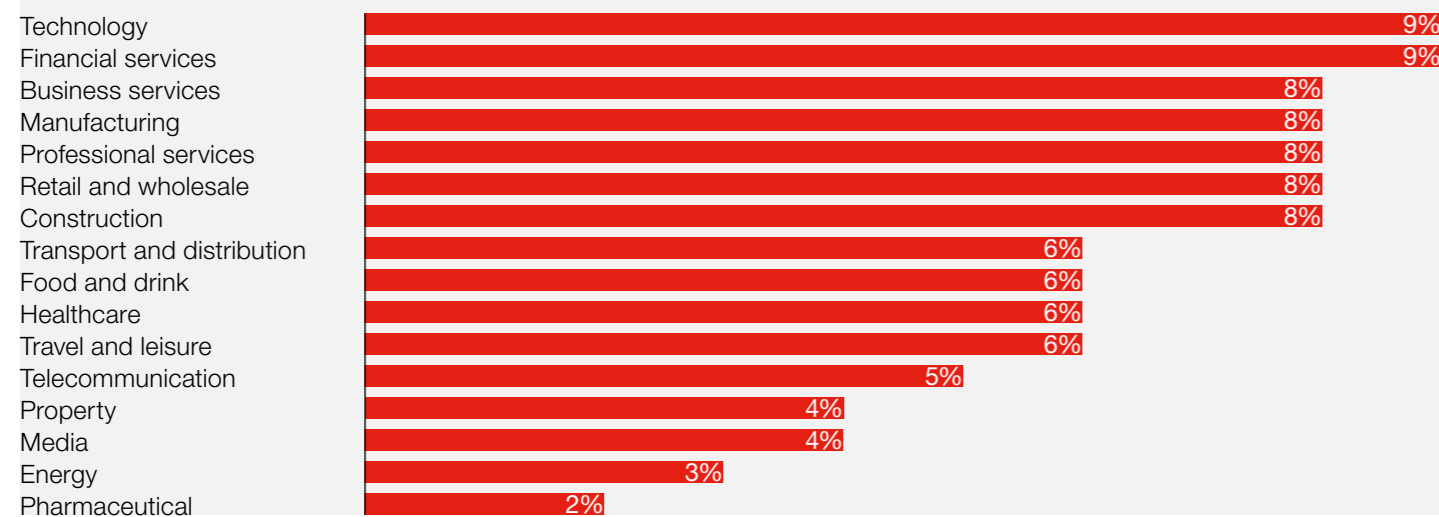
Department in which respondents work



Respondent job level



Industry



Hiscox commissioned Forrester Consulting to assess organisations' cyber readiness. In total 3,036 professionals responsible for cyber security decisions at their companies were contacted (1,000 plus each from the UK, US, and Germany). Seventy percent of respondents were from companies with fewer than 250 employees (small firms), and the remaining 30% from companies with 250 or more employees (large firms). Respondents completed the online survey between the 16th of November and the 5th of December 2016.

About Hiscox

Hiscox, the international specialist insurer, is headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). There are three main underwriting divisions in the Group – Hiscox Retail (which includes Hiscox UK and Europe, Hiscox Guernsey, Hiscox USA and subsidiary brand, DirectAsia), Hiscox London Market and Hiscox Re. Through its retail businesses in the UK, Europe and the US Hiscox offers a range of specialist insurance for professionals and business customers, as well as homeowners. Hiscox underwrites internationally traded, bigger ticket business and reinsurance through Hiscox London Market and Hiscox Re.



1 Great St Helen's
London EC3A 6HX
United Kingdom

T +44 (0)20 7448 6000

F +44 (0)20 7448 6900

E enquiry@hiscox.com

hiscoxgroup.com
