CYBER RESEARCH 2018

Insurance POST

In association with

CYBERSCOUT®

WE'LL TAKE IT FROM HERE™

CONTENTS

INTRODUCTION AND METHODOLOGY

INTRODUCTION

"WE HAVE DECIDED TO CALL THE ENTIRE FIELD OF CONTROL and communication theory, whether in the machine or in the animal, by the name Cybernetics," stated mathematician and philosopher Norbert Wiener in 1948, the same year the word cybernetics – now cyber – first entered the Oxford English Dictionary.

Cyber has come a long way since 1948, yet its meaning has remained the same: it still encompasses the notions of control and communication. Today the insurance industry is in an ongoing and prolific yet invisible battle to afford its customers rightful and autonomous control of their machines, their gadgets and, ultimately, their lives. ■

METHODOLOGY

DURING DECEMBER 2017 AND JANUARY 2018, insurers [which for our research purposes also includes managing general agents] and brokers within the insurance industry were invited to participate in an online survey relating to cyber.

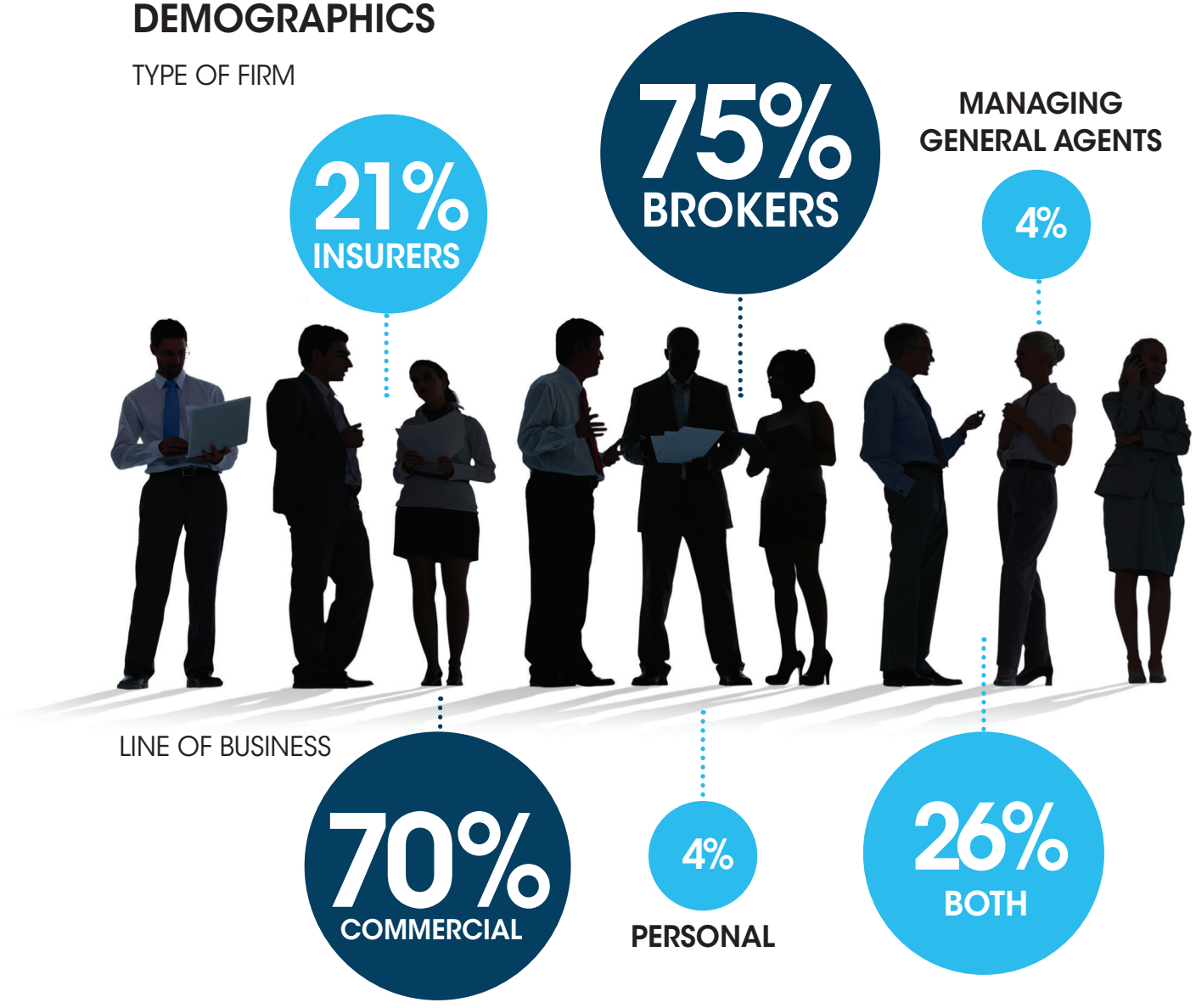
In total, 187 members of the insurance industry attempted to answer this survey, with 115 of these completing all the questions. All responses, complete and partial, have been included in the results.

Concurrently, a separate survey of the general public was carried out in December 2017 with the help of Consumer Intelligence. Over 1000 members of the public across the UK responded to the questions, the findings of which are presented in this report alongside results of the industry survey.

The data collected from the two surveys has been anonymised. ■

DEMOGRAPHICS

TYPE OF FIRM



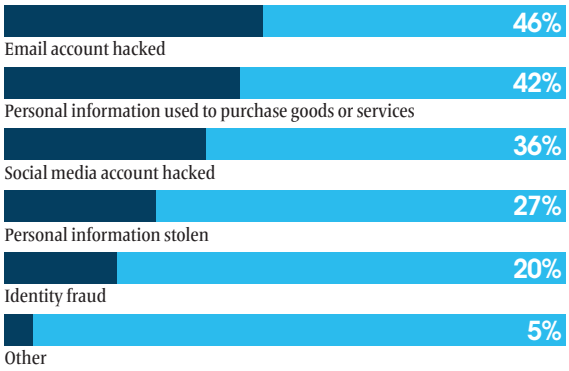
METHODOLOGY

CYBERSCOUT
WE'LL TAKE IT FROM HERE℠

GENERAL PUBLIC

Have you ever been hacked or suffered a data breach, whereby a third party has used your information for illicit purposes?

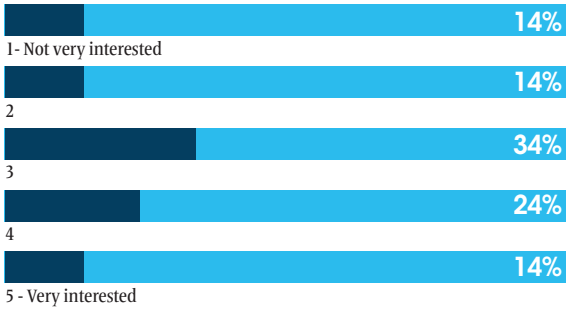
1. What type of hack or data breach have you been the victim of?



2. How many data breaches have you been the victim of?

3. Did you take steps to make sure your data was more secure in the future?

4. How interested would you be in advice from an insurance company's professional consultancy?



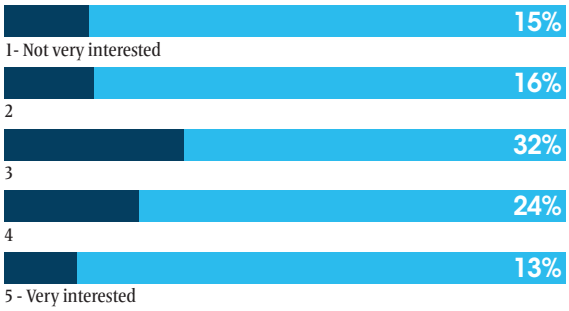
5. Would you be happy to pay for this service?

46%

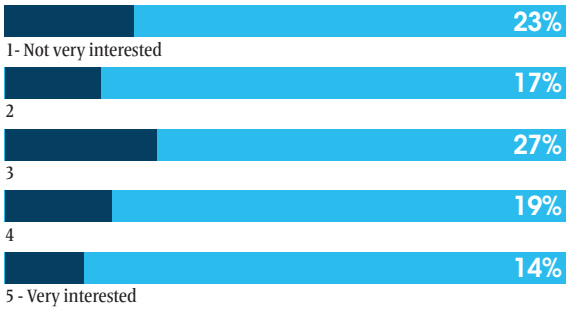
OF RESPONDENTS HAD BEEN A VICTIM OF EMAIL HACKING

6. How interested would you be in purchasing an insurance policy that reimburses you for lost funds?

7. How interested would you be in an insurance policy that rectifies damage to a computer or device?

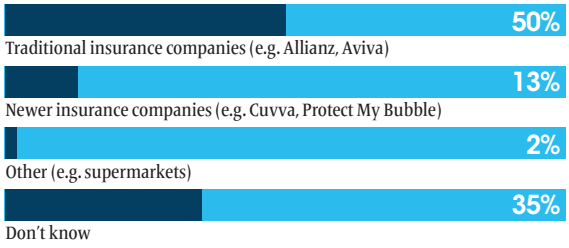


8. How interested would you be in purchasing an insurance policy that reimburses you for items ordered online that don't arrive or are not as expected?

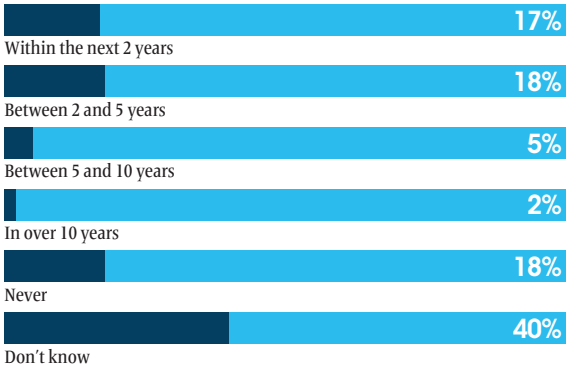


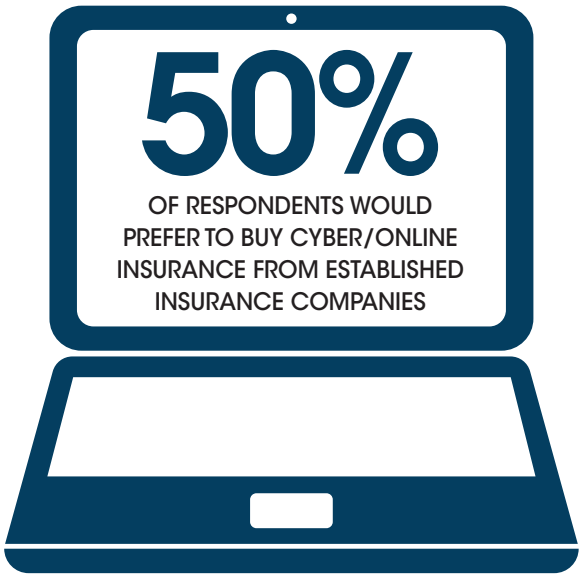
9. How interested would you be in an insurance policy that protects you from cyber bullying?

10. From which type of company would you prefer to buy cyber/online insurance?



11. In what timeframe do you see yourself purchasing some kind of cyber/online insurance?





SECTION ONE

CYBER LANDSCAPE TODAY

CYBER IS ALL AROUND US. We cannot see it, we cannot feel it; in fact we are unable to use any of our human senses to detect it. Yet it governs our lives and has the ability to enhance or ruin them. According to the Federation of Small Businesses, 66% of small businesses have been a victim of cyber crime and this research reveals 22% of insurers, brokers and managing general agents themselves already have suffered a cyber attack, with insurers having experienced a slightly higher number of incidents than brokers.

In reality, this figure most likely is higher. The propensity of phishing emails and emails with viruses sitting in the spam section of our inboxes is testament to the daily bombardment most internet users face when they log into their email account. This occurs to such an extent that some might not even call it a cyber attack.

Indeed, one respondent wrote: "Numerous occasions too many to mention. Every day I get an email with a list of emails that have been blocked from delivery due to phishing/malware/spyware etc."

Other named incidents by respondents include:

- Data encryption attempt
- Cyber extortion attack
- Attempts to access our system
- Ransomware in 2015
- Data stolen from service provider
- Website hacking
- Corruption of data

"The only surprise with these stats is that only 22% of companies have experienced a cyber related incident. The internet has revolutionised our lives but cyber crime is the dirty little secret that won't go away. What puzzles me is that this is still a class of cover that has to be sold. Why are clients not beating down our doors to buy the cover? How many more losses before this becomes a universal cover?" Howard Lickens, CEO, Clear Insurance Management

Another respondent wrote: "Email interception: A claims payment was sent to the wrong bank account following receipt of an email allegedly from the claimant with new bank details. It transpired that someone had intercepted emails and sent their own bank account details."

When considering the increasingly various prongs of cyber attacks in existence today, it is perhaps difficult to imagine what is yet to come in the cyber world. Developing appropriate communication security strategies is of paramount importance for companies powered by communication over the internet, and insurance companies must be one step ahead at all times.

To successfully pre-empt their customers' needs and desires, the industry must invest time and resources to carefully establish what drives these emotions to appear in the first place.

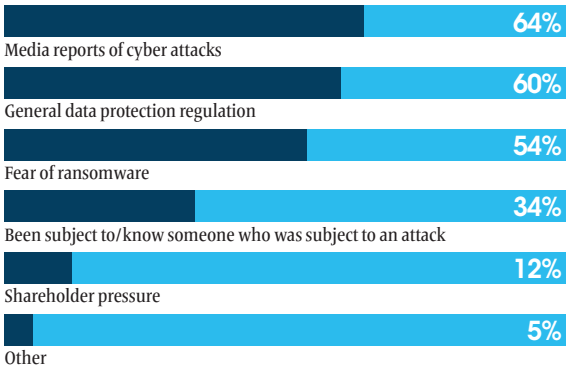
BIGGEST DRIVERS

According to PWC, 61% of business leaders across all industries see cyber attacks as a threat to growth, ranking it higher than shifts in consumer behaviour, the speed of technological change and supply chain disruption. Despite this, government figures suggest less than 10% of UK companies have cyber insurance protection.

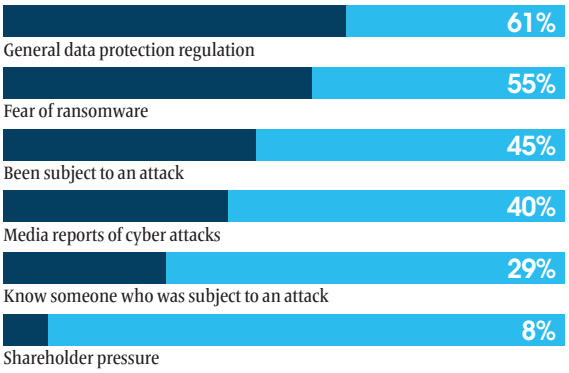
CYBER LANDSCAPE TODAY

BIGGEST DRIVERS FOR CUSTOMERS BUYING CYBER INSURANCE TODAY*

Brokers



Insurers



* Respondents were allowed to choose more than one option

This survey found brokers and insurers reveal slightly different views when considering what they believe to be the biggest drivers for customers buying cyber insurance today.

The major driver for brokers was media reports of cyber attacks, followed closely by the General Data Protection Regulation, and then, fear of ransomware.

Insurers cited the GDPR as the dominant force behind what they believe to be their customers' cyber insurance purchases, followed by fear of ransomware. Ranking in third place for insurers was the experience of having been subject to an attack themselves, which correlates with the statistic that more insurers than brokers had indeed already suffered a cyber- attack.

"Staff errors, including the loss of laptops and memory sticks as well as opening phishing emails, are major causes of cyber breaches, as well as hackers opportunistically exploiting security holes that appear in outdated legacy systems and/or a lack of patching. Insurers and businesses need to work together to identify and manage risks more holistically: focus on company culture – from continual training and education of all staff – to raising cyber risk management from the IT department to the boardroom." David Legassick, head of life sciences, technology and cyber, CNA Hardy

Shareholder pressure was rated very low, implying the drive for increased cyber insurance is a reaction to external events instead of internal red tape.

Other drivers listed by brokers and insurers were contractual requirements, business interruption events and social engineering, the term used to describe the psychological manipulation of a person to divulge confidential information.

BUSINESS INTERRUPTION

In terms of business interruption, a handful of respondents believe that if this has ensued from a cyber terrorism claim it should be covered, but not physical losses. As one respondent explained: "Physical loss has no place in a cyber policy. The limits that the market can offer are far too small to be meaningful."

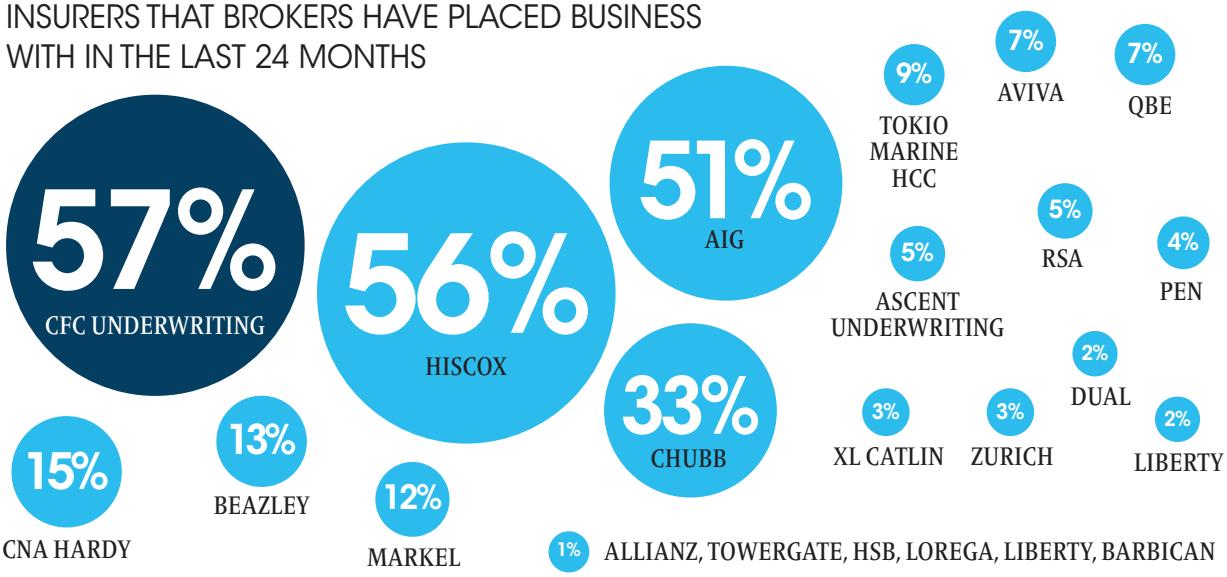
For the vast majority (90%), however, the consensus is that both business interruption and physical losses should be covered in the event of a claim due to cyber terrorism

– with one or two cautionary caveats. One respondent believed it would come down to: "appropriate security measures being followed prior to breach", and another stated: "This should not be standard within cyber policies and should be an optional extension for which a premium is charged, otherwise we could see insurers burn their books."

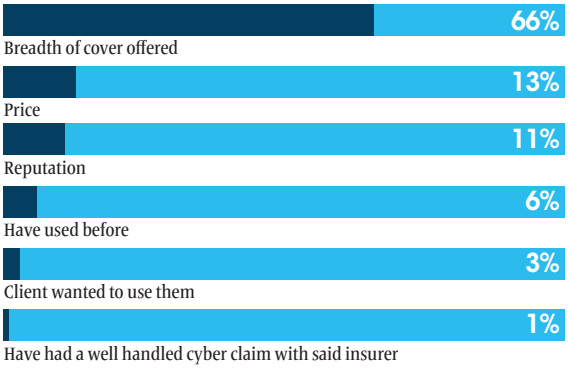
A concern of one respondent centred on the issue of attribution. "Cover is needed for these but really depends on the insured if this should be in their property damage, terror or a separate cyber PD policy. The biggest issue is one of attribution - if you can't confidentially attribute to either terror or malicious group - or even attribute to a cyber event, this is all moot."

Within cyber terrorism, another question beckons. For brokers, the majority believe individual insurers should be responsible for providing cyber-related terror insurance whereas the majority of insurers believe Pool Re, the Government-backed insurer of last resort, should be the responsible entity. A few respondents decided the task fell on both insurers and Pool Re to join together.

INSURERS THAT BROKERS HAVE PLACED BUSINESS WITH IN THE LAST 24 MONTHS



REASONS WHY BROKER PLACED CYBER BUSINESS WITH INSURERS



RANKING BY BROKERS OF INSURANCE FOR CYBER SECURITY INSURANCE*

* Insurers were scored by a weighted calculation. Items ranked first were valued higher than the following ranks, the score is the sum of all weighted rank counts.

CYBER LANDSCAPE TODAY

CYBERSCOUT
WE'LL TAKE IT FROM HERE™

BROKERS ON INSURERS

From an array of insurance companies [including MGAs], brokers were asked to list the ones their customers had used for their cyber cover in the past 24 months. CFC Underwriting, Hiscox and AIG were the top three insurance companies brokers turned to for cyber insurance purchases.

One-third of brokers had used Chubb, and CNA Hardy, Beazley and Markel were the next most popular.

The key driver for choosing to do business with these insurers was by far the breadth of cover offered: with 66% of brokers stating this to be the most important reason. Price and reputation come next, but only with 13% and 11% respectively. Previous work with an insurer or already having had a well-handled cyber claim with the said insurer was a deciding factor for only 7% of broker respondents. In 3% of cases, the client specifically had asked to use a particular insurance company.

RANKING INSURERS

When brokers were asked which insurers would be ranked top for their cyber security insurance, brokers were fairly unanimous in their decisions. Four insurance companies took prominent positions at the top.

CFC Underwriting came first on the list, followed closely by AIG, Hiscox and Chubb.

CNA Hardy was ranked a distant fifth followed by Beazley, QBE and Aviva.

Brokers clearly rate insurers according to their cover. Those insurers wishing to increase their cyber cover with brokers would do well to increase their breadth of cover to make themselves more attractive to the broker audience.

INSURERS ON BROKERS

Insurers were given the same task of naming the brokers whose customers have bought cyber cover from them in the past 24 months. Within the range of brokers listed, Aon was the most prolific broker at 55%, while Marsh and Willis Towers Watson are ranked joint-second, having placed cyber business with 45% of the insurer respondents. Arthur J Gallagher and Howden brokers are tied in fourth place, with JLT, Lockton and Towergate following closely behind.

A few insurers stated they used regional or independent brokers while a couple disclosed they were launching their own product so had no need for brokers.

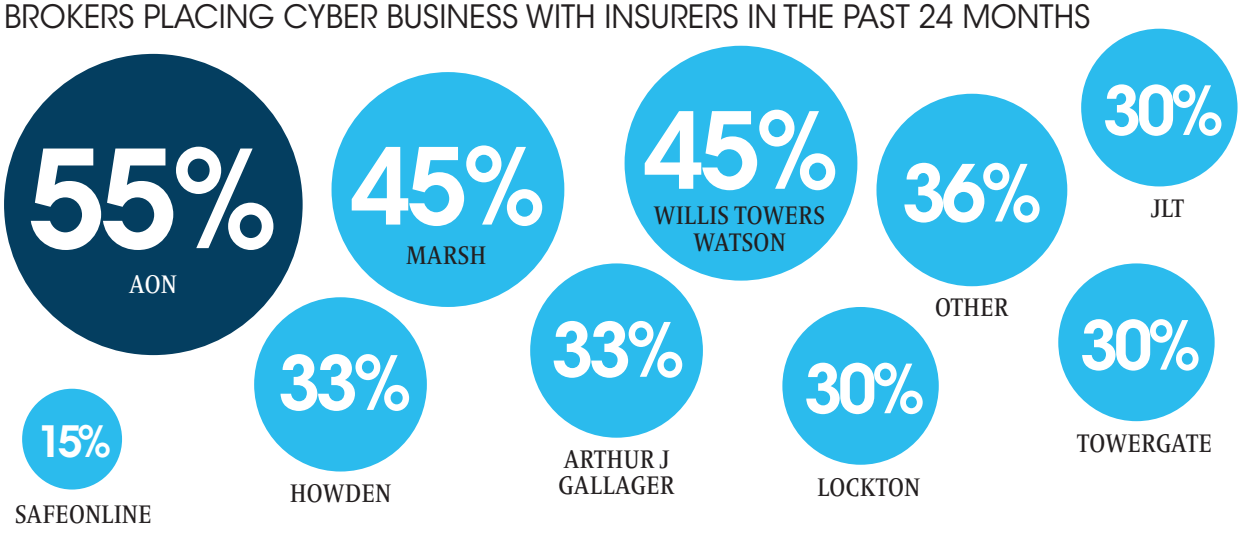
There are various reasons why insurers had chosen these particular brokers to work with on cyber cover, including the client's preference and having an existing relationship with the brokers, but there was no overriding sole key driver.

For just over one-third of insurers, clients had made specific requests to use certain brokers, and for one-quarter of the insurer respondents, they already had used the broker before.

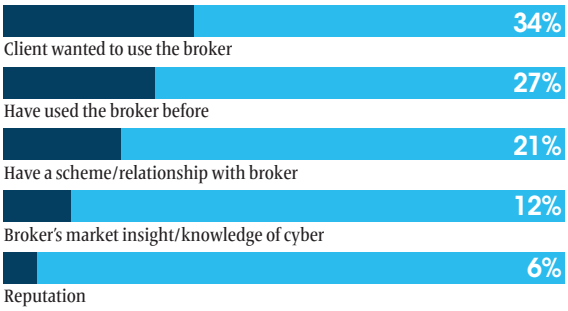
Insurance often has been described as a relationship industry, and for 21% of insurers, having a scheme or a relationship already in place with a certain broker resulted in more cyber cover business being sent to that broker.

Market insight or specialist cyber knowledge, together with a broker's reputation, counted for rather little when insurers had considered firms to work with for their cyber offering.

BROKERS PLACING CYBER BUSINESS WITH INSURERS IN THE PAST 24 MONTHS



REASONS WHY INSURERS CHOSE BROKER FOR CYBER BUSINESS



RANKING OF BROKERS BASED ON WHAT INSURERS HAVE SEEN AND KNOW IN TERMS OF CYBER SECURITY*

* Insurers were scored by a weighted calculation. Items ranked first were valued higher than the following ranks. The score is the sum of all weighted rank counts.

RANKING BROKERS

The ranking of brokers chosen by insurers, based on what they have seen and know in terms of cyber security insurance, was very close, unlike the brokers' ranking of insurers, which had four top insurers stand out above the crowd.

In line with the list of brokers that had placed cyber cover with insurers over the past 24 months, Aon and Marsh were ranked first and second.

However, Lockton has been ranked by insurers in third place – before Willis Towers Watson – despite only 30% of insurers having used this brokerage to sell cyber cover for them, implying a huge majority of this 30% would have needed to rank Lockton first or second.

JLT, Arthur J Gallagher and Howden resume the rankings order, with Towergate and Safe Online bringing up the rear. ■

SECTION TWO

RISK MANAGEMENT AND COVERAGE

RISK MANAGEMENT AND COVERAGE

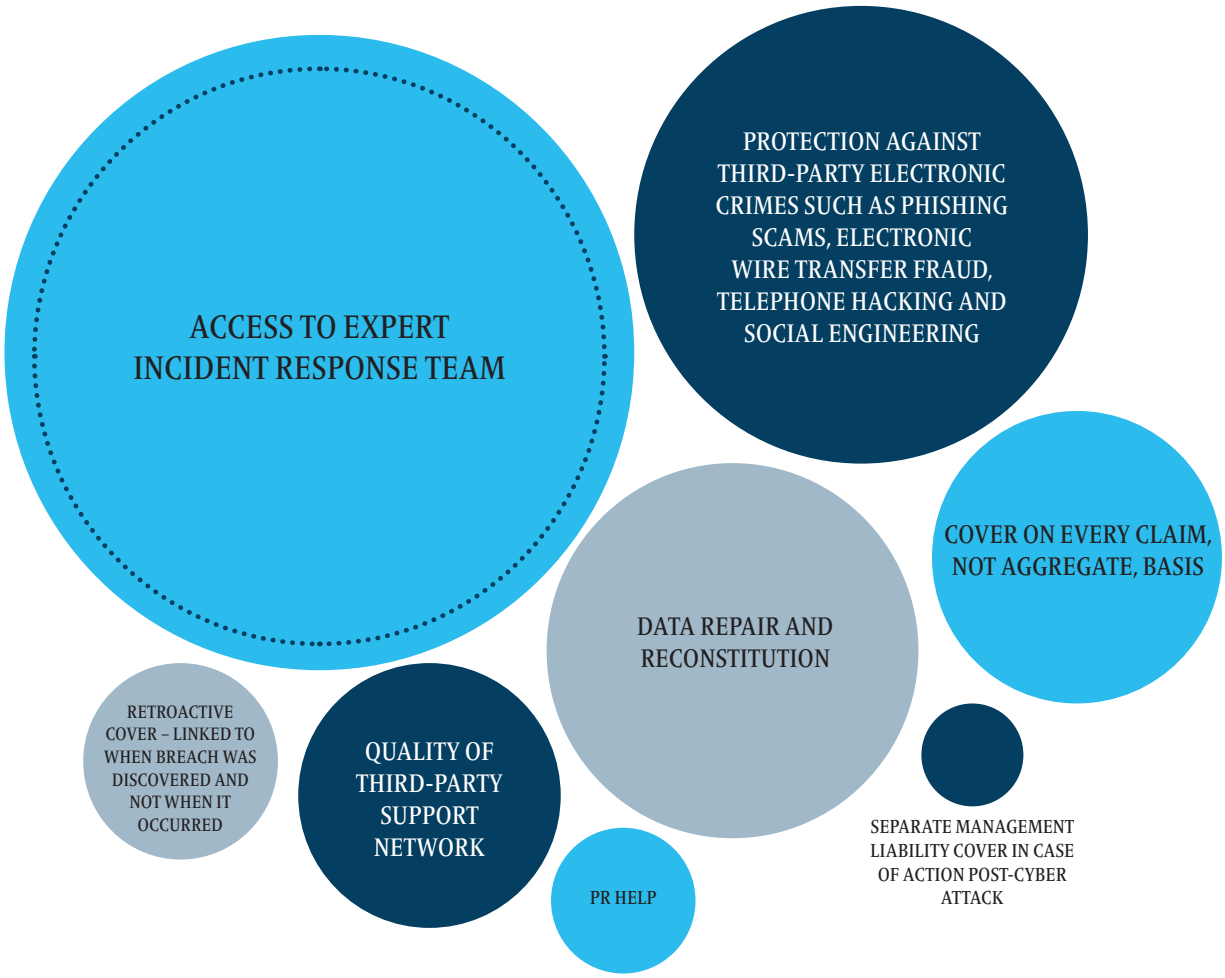
CYBER POLICIES ARE STILL IN THEIR INFANCY compared to many other aspects of the insurance industry and are still rapidly evolving to meet ever-changing client needs. But are these cyber policies fitting the bill of requirements presented by the customer?

According to brokers, the two most important factors in a cyber policy are access to an expert incident response team and protection against third-party electronic crimes such as phishing scams, electronic wire transfer fraud, telephone hacking and social engineering.

Data repair and reconstitution cover on an individual rather than aggregate claim basis, and quality of third-party support networks were deemed the three next most important factors.

Public relations help and separate management liability cover in case of action post-attack were not considered very important, ranking seventh and eighth respectively.

THE MOST IMPORTANT FACTORS FOR A CYBER POLICY



RISK MANAGEMENT AND COVERAGE

CYBERSCOUT
WE'LL TAKE IT FROM HERE™

PREPARED FOR ATTACK

Brokers and insurers generally do not feel companies' risk management departments are prepared for a cyber attack.

Only 1% of broker respondents believe companies are well prepared for an attack. A small majority – two-fifths – of brokers felt companies were prepared "to a lesser extent". Responses were then divided predominantly between "to some extent" and "not a lot", with 6% of the broker population stating companies were "not at all" prepared for an attack.

"This highlights deficiencies in understanding of the risk of a cyber attack, and potential gaps in communication lines between risk managers and the C-suite. Cyber-specialist brokers and underwriters in the insurance industry can help support businesses with their knowledge in this area. However, all stakeholders need to be open to understanding the potential impact an incident could have on their company, and the results from the survey indicate this isn't the case in many businesses."
Peter Hawley, underwriter, cyber, HDI Global

None of the insurers felt companies were well-prepared for a cyber attack, although insurers do appear to have more faith than their broker counterparts in either companies' risk management departments or in the advice they are receiving: 41% believe companies are prepared for a cyber attack "to some extent".

The remaining insurer votes were fairly equally divided between 'to a lesser extent' and 'not a lot', with 6% again stating companies were 'not at all' prepared for an attack. In total, the majority response taken from insurers and brokers is that companies are prepared 'to a lesser extent'.

With brokers often on the frontline of relationships with company risk managers, this insight must surely compel an urgent action on this front.

EDUCATION

For companies to become more, or better, prepared against cyber attacks, it would seem that two things need to happen in conjunction: companies must become somehow better educated about the risks of the cyber world in order to protect themselves against it, and insurers must find better ways to accurately predict these risks in order to educate their customers.

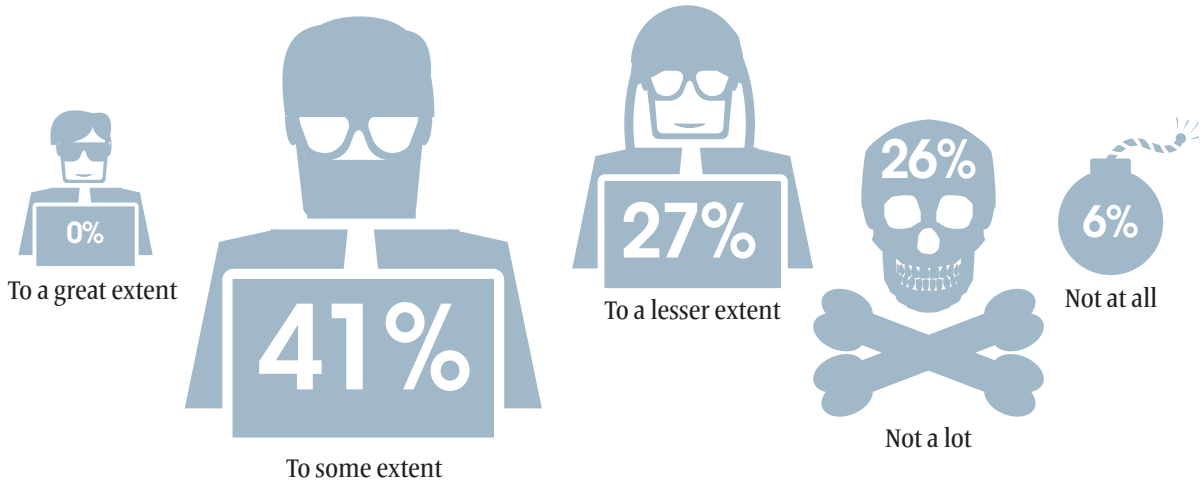
There is no question that educating clients on cyber insurance is vitally important. Nearly three-quarters of the total respondents gave this a 10 out of 10 as a priority, and the remaining quarter listed this between seven and nine out of 10.

Many insurers claim to be taking steps to address education but brokers believe some are more proactive than others.

Brokers ranked XL Catlin as the No. 1 insurer for educating SMEs on cyber risks. Zurich takes second place, followed by CNA Hardy, Tokio Marine HCC and CFC Underwriting, respectively. Bringing up the rear of the table with a ranking of five or less out of 10 for their efforts to educate SMEs on cyber are Aviva, Markel and QBE.

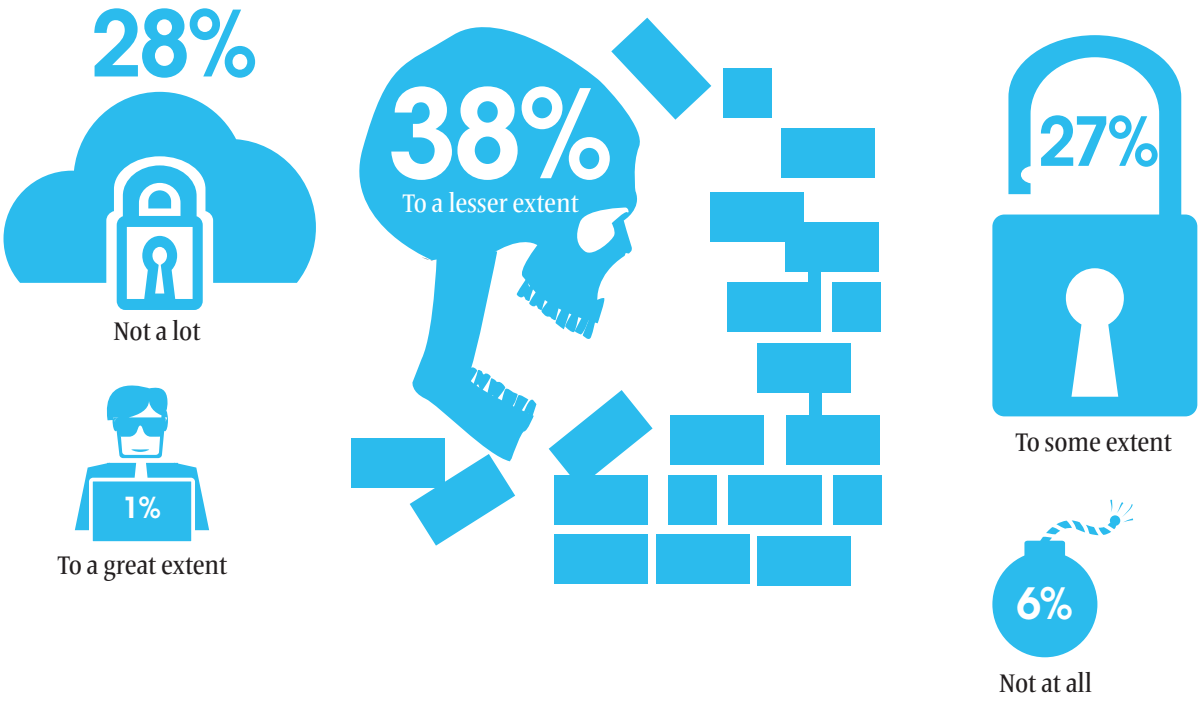
INSURERS' RESPONSES

TO WHAT EXTENT DO YOU FEEL COMPANIES' RISK MANAGEMENT DEPARTMENTS ARE PREPARED FOR A CYBER ATTACK?



BROKERS' RESPONSES

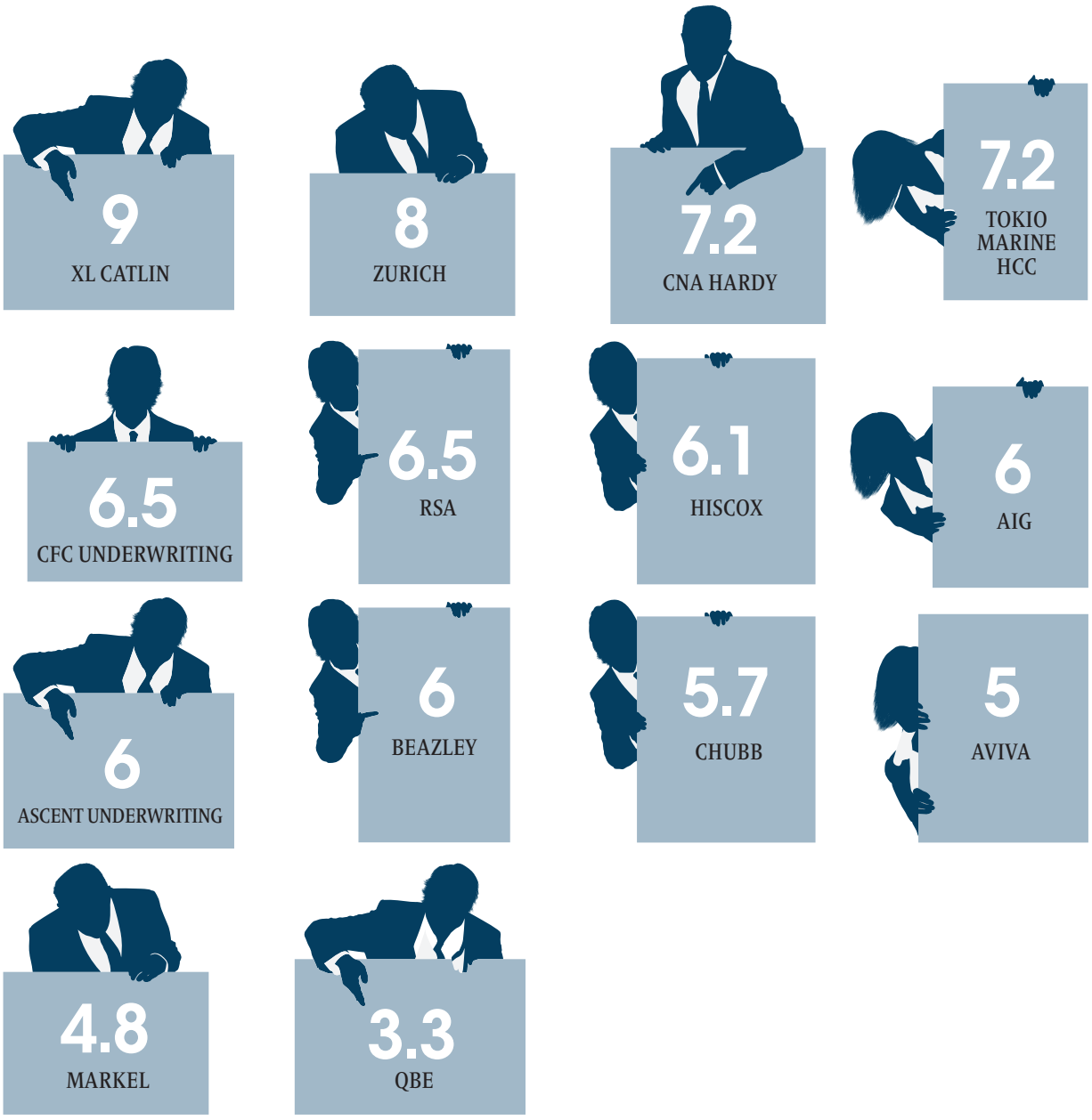
TO WHAT EXTENT DO YOU FEEL COMPANIES' RISK MANAGEMENT DEPARTMENTS ARE PREPARED FOR A CYBER ATTACK?



RISK MANAGEMENT AND COVERAGE

CYBERSCOUT
WE'LL TAKE IT FROM HERE℠

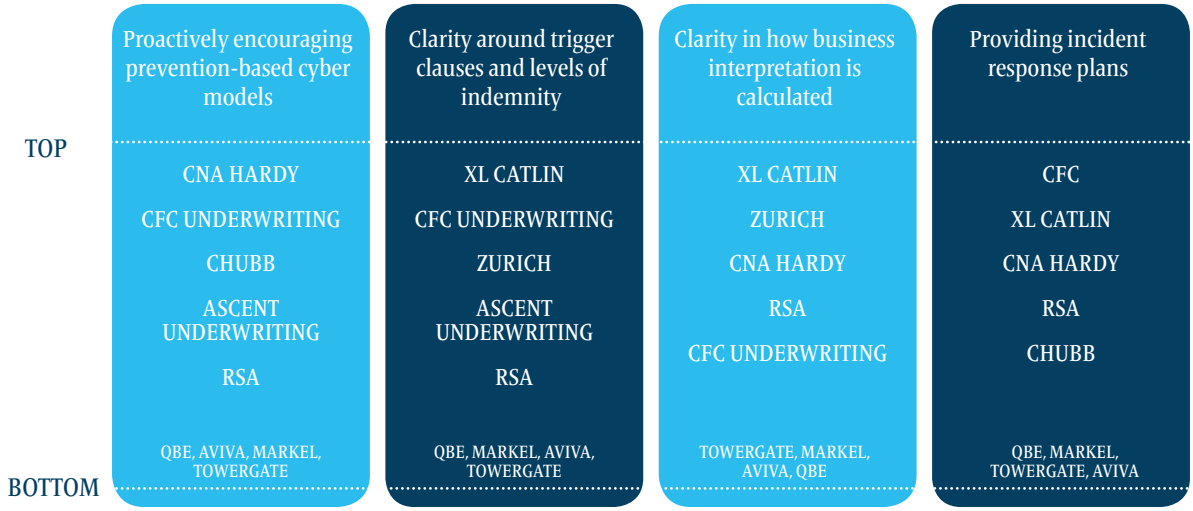
INSURERS' RANKING OUT OF 10 FOR EDUCATING SMES ON THE RISKS OF CYBER



Yet when considering cyber policies, many factors come into play before a customer decides which insurer to do business with. Proactively encouraging prevention-based cyber models, supplying incident response plans, or providing clarity around trigger clauses, levels of indemnity and business interruption calculations are all indicators of how strong an insurer's offering may be, and brokers ranked insurers accordingly.

CRC Underwriting and RSA consistently were in the top five for these policy elements.. XL Catlin and CNA Hardy are the next most highly ranked in terms of these policy elements, followed by Zurich, Ascent Underwriting and Chubb.

RANKING OF INSURERS BY BROKERS



DECLINED PAYMENTS

Even when cover is in place, not all policies have paid out. The reasons given by brokers for why cyber-related claims had been declined by insurers were varied, ranging from poor risk management and security, theft of physical goods, noncompliance with IT security, no telecoms cover, access records to the server room, to incorrect cover or cover exclusions. This nonexhaustive list highlights how important it is for the insurance industry to educate companies on policy wording, as well as as more effective risk management strategies.

MODELLING TRENDS

But does the industry have enough data with which to educate their customers? Brokers were asked how much effort they felt their insurers were putting into modelling trends to produce more accurate policies in the cyber arena.

Nearly 60% of all broker respondents said insurers are not putting in enough effort, while just under one-quarter felt insurers were putting in "a lot" of effort to model trends and find ways to produce more accurate policies. An even smaller percentage, not even one-fifth of respondents, were happy with insurers' efforts to address pricing policies.

If a policy is comprehensive enough, detailed enough and accurate enough to appeal to a customer and pay out in the future, its worth will be hugely apparent in the event of a claim following a cyber breach, and the insurers that have devised it will see brokers flocking to their door. ■

CLAIMS: WHAT TO DO AFTER A BREACH

INSURER RATINGS

Brokers were asked to name the insurers with which their customers had made a cyber claim within the past 24 months.

AIG and CFC Underwriting were the two insurers that had the most claims. Almost one-fifth of brokers have had cyber claims with Hiscox, and nearly one-fifth with CNA Hardy.

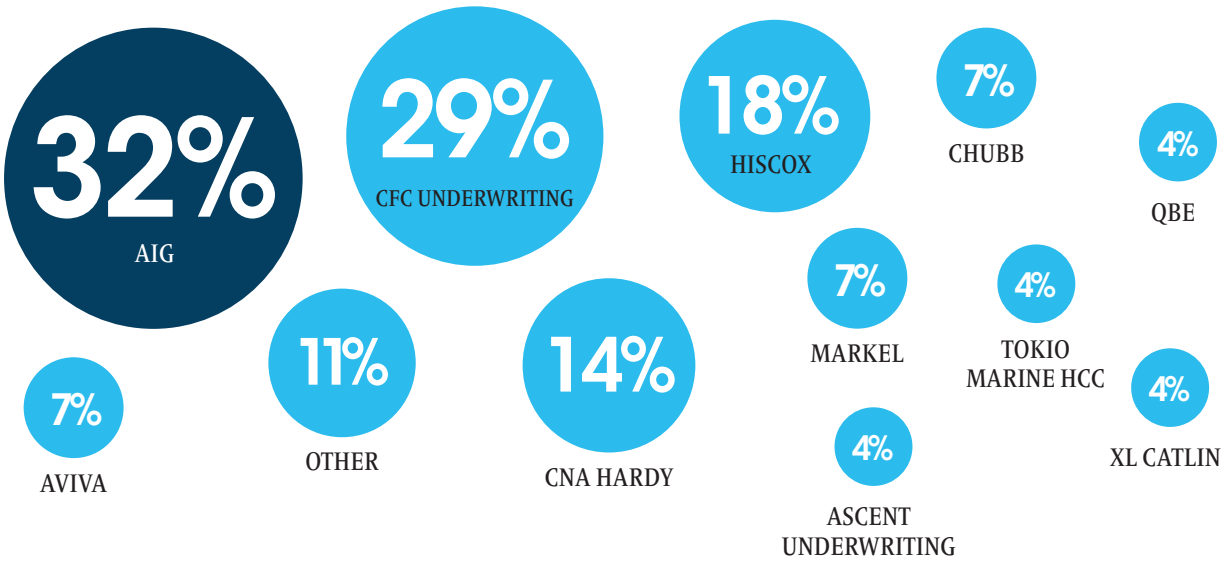
When asked to rate the insurers they had dealt with based on the claims service received, brokers, under the veil of anonymity, were able to give frank answers. At the bottom end of the scale, Aviva's pre-pilot product had offered limited support, brokers said, and the company showed lack a "lack of understanding when needed and didn't pay the claim in full," while QBE was described as having a slow response.

AIG scored a fairly healthy 7.4 through timely client support. Prompt settlement and value for money were the reasons Hiscox was awarded a slightly higher ranking.

Interestingly, Tokio Marine HCC, Ascent Underwriting and Chubb, which had seen fewer claims, received a higher overall score than AIG, suggesting these companies possibly may emerge to become future leaders if policies are placed according to service.

AIG was described as having an excellent blue-light response, with one broker writing: "Excellent third-party suppliers; nil excess for 48-hour first response." However, one bad experience may be responsible for AIG's lower-than-expected ranking: a broker commented that the company had "more interest in the physical claim repudiation than the risk factor of a client database server being stolen".

INSURERS WITH WHOM BROKERS HAVE HAD A CYBER CLAIM WITHIN THE PAST 24 MONTHS



RANKING OF INSURERS BY BROKERS BASED ON THE CYBER CLAIMS SERVICE RECEIVED

Unfortunately, one bad experience is all that is needed to shunt an insurer down the ranking scale and force a broker to cut ties and move on.

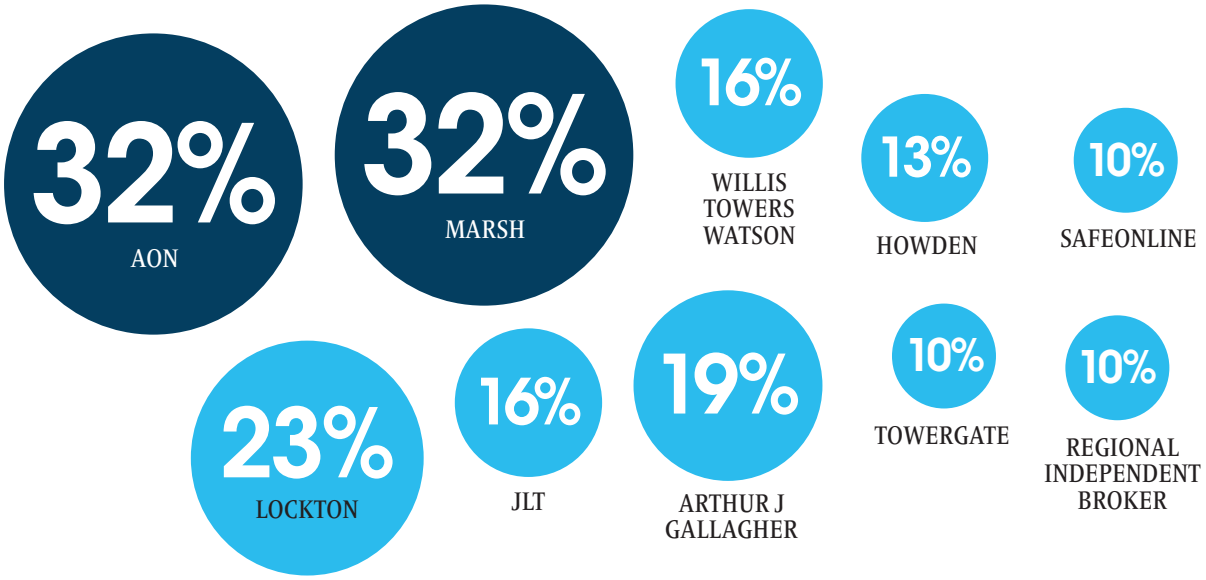
Another surprising statistic is that CNA Hardy, while having worked with only 14% of brokers on cyber claims over the past 24 months, was awarded second place in the overall rankings on cyber claim services received. Excellent cover and third-party support, combined with access to experts, propelled this insurer into a leading position, only slightly below the overall rankings winner CFC Underwriting. CFC Underwriting received an impressive nine out of 10 and comments such as “proactive and professional service”; “initial response very good, made client feel reassured throughout”; and “good technical knowledge”. Speed of response also was listed.

MITIGATION TESTING

In addition to enacting policy requirements in the event of a cyber-related breach, some insurers are quick to offer scenario testing or mitigation exercises, a service increasingly requested by brokers and their clients.

Arguably, these should have been carried out prior to any cyber incident, but in this relatively new and ever-evolving line of insurance, such exercises may prove difficult to execute due to lack of

WHICH OF THE FOLLOWING BROKERS HAVE BEEN INVOLVED WITH A CYBER CLAIM WITHIN THE PAST 24 MONTHS?



historical data and absence of specialist expertise. However, this is changing – with every new cyber attack comes new data.

Currently, one-third of brokers have experienced AIG offering such services, while one-fifth of brokers cited CNA Hardy's services. CFC Underwriting, RSA and Markel were named by nearly 15% of the respondents as offering mitigation testing. Brokers had little experience with Aviva, Chubb or Hiscox offering post-event mitigation exercises or scenario testing.

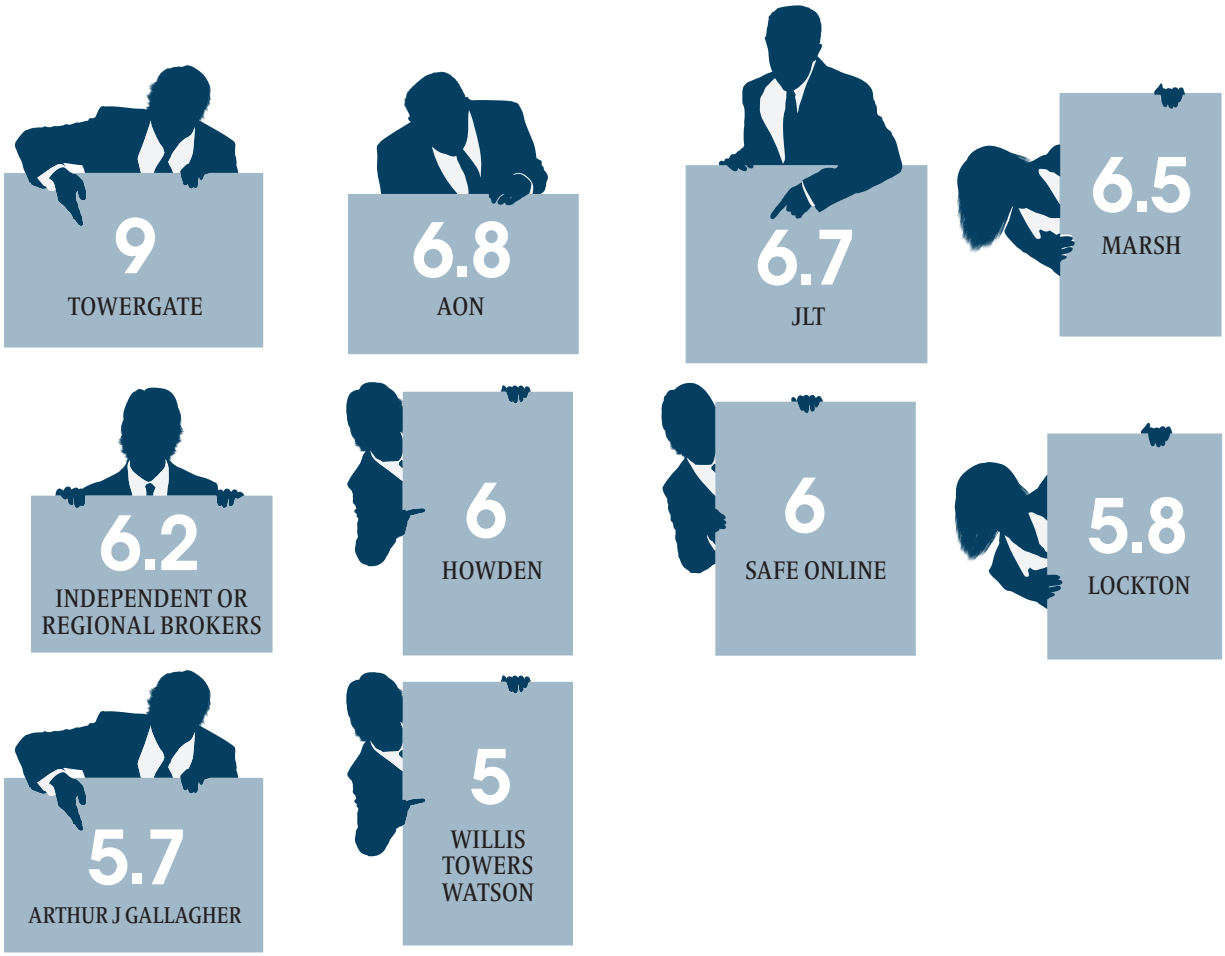
BROKER RATINGS

When insurers were asked to name the brokers through which their clients had notified a cyber claim within the past 24 months, two names were more prominent than the rest: Aon and Marsh, which is unsurprising due to their size.

10% of cyber claims were notified through an independent or regional broker.

In terms of communication throughout a claim, Towergate received the highest score, nine out of 10. Aon was in second place, followed by JLT. Marsh was in fourth place. Independent and regional brokers came next, ranking above industry giants, such as Willis Towers Watson and Arthur J Gallagher, and landing in the UK's top five. ■

HOW INSURERS RATE COMMUNICATION REGARDING CYBER CLAIMS WITH BROKERS



SECTION FOUR

THE FUTURE

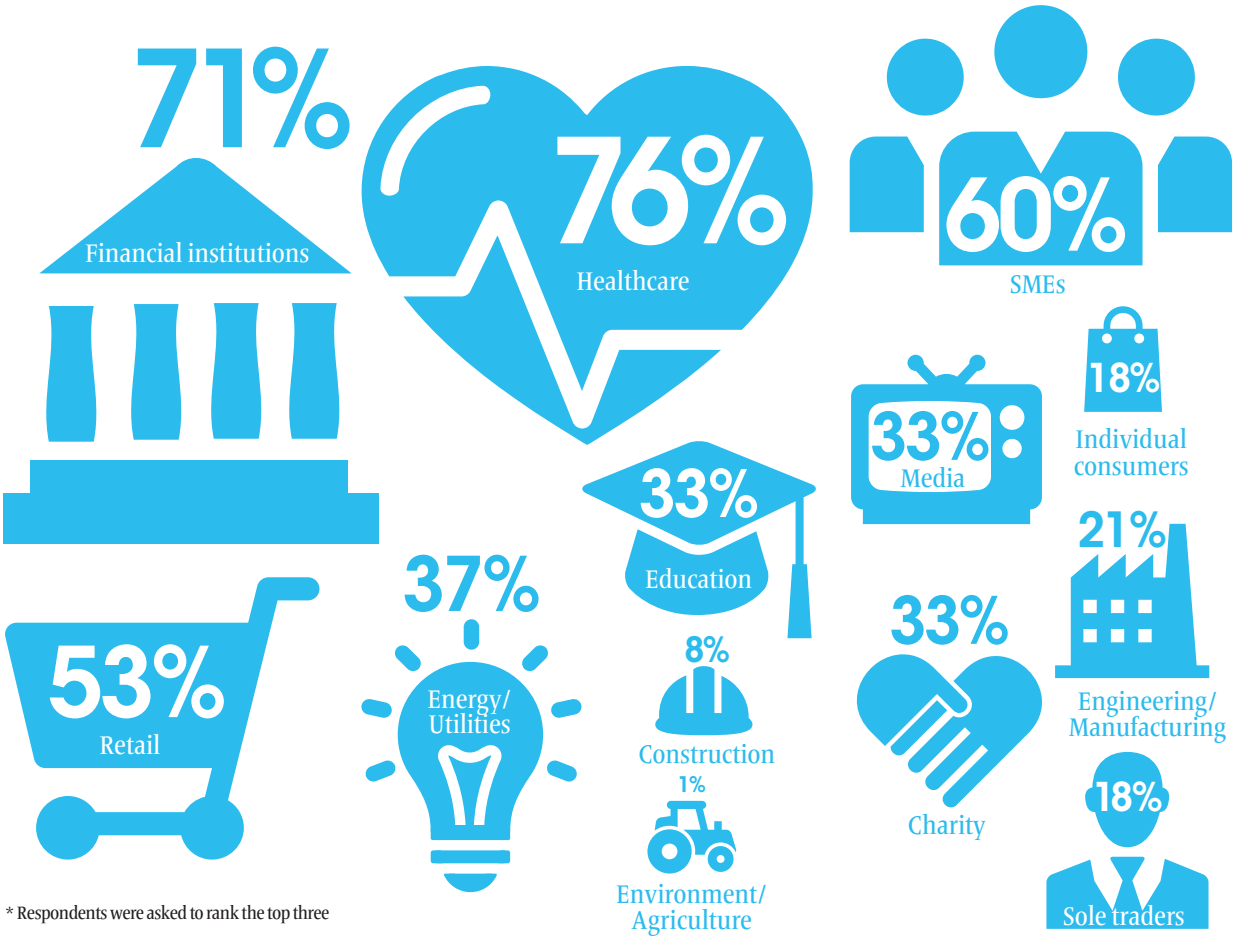
THE FUTURE

IT ALREADY IS CLEAR THAT WHATEVER TYPES of cyber attacks companies and individuals currently are experiencing, these will become more prolific as cyber hacktivists and organised criminals learn new tactics to break past firewalls, gain access to confidential information and wreak havoc.

The healthcare sector and financial institutions stood out as the top two sectors most likely to be vulnerable to cyber attack,, with healthcare slightly in the lead. For brokers, these two sectors drew just over 75% of votes, while for insurers, healthcare was almost 20 percentage points more likely to be vulnerable to an attack.

SMEs came in third place by brokers and fourth by insurers, revealing a real urgency, sensed across the entire insurance industry, to address and manage the cyber vulnerability of the UK's smaller companies. Next in order of perceived vulnerability by brokers and insurers is the retail sector. But after that there is less agreement. Energy, utilities, engineering and manufacturing are deemed more vulnerable by insurers than by brokers, while the latter ranks education and media sectors next. Overall, by brokers and insurers, energy and utilities were ranked fifth.

WHICH OF THE FOLLOWING SECTORS ARE MOST VULNERABLE TO A CYBER ATTACK*



* Respondents were asked to rank the top three

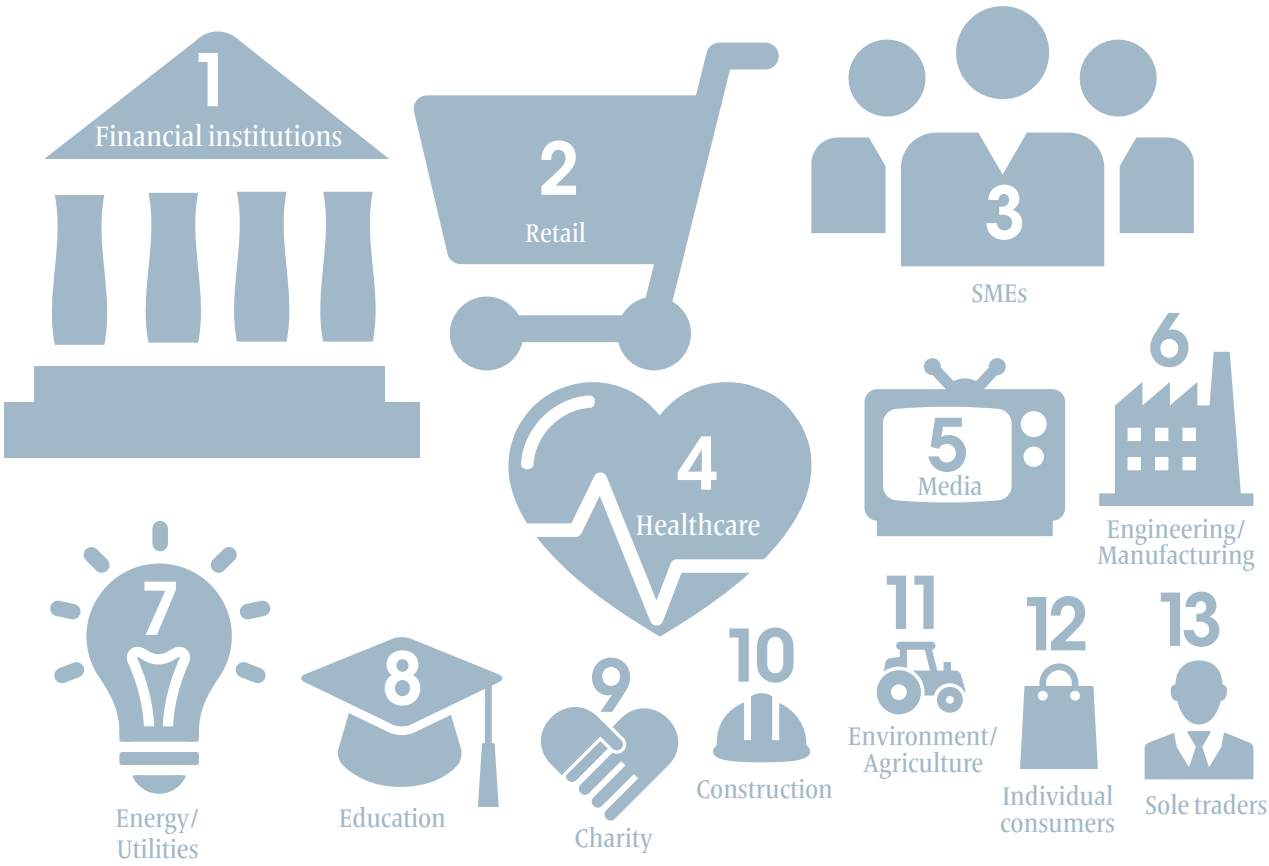
"The sectors purchasing cyber cover seem to have cyber risk because they hold financial information (retail), sensitive information (healthcare) or have a higher legal regulation (financial institutions). I would have expected sectors that are wholly reliant on electronic systems to function, such as telecommunications or technology companies, to feature more highly." Hans Allnutt, head of cyber and data risk, DAC Beachcroft

The environmental and agricultural sectors were deemed the least vulnerable of sectors as far as cyber events were concerned. These did not attract any votes from brokers and just a handful from insurers, while the construction industry was ranked second to last. This implies either these industries are seen as unworthy of cyber attacks or as having strong security measures in place, for now.

Perhaps brokers are more attuned to their customers than insurers. When examining which sectors currently are purchasing cyber cover, brokers' predictions regarding the cyber attack vulnerability of companies correlates more closely with purchasing figures than insurers' predictions do.

Far in the lead, by over double the ranking score for the second-largest sector buying cyber insurance, are the financial institutions, followed by retail in second place, then SMEs and healthcare, respectively.

BASED ON EXPERIENCE, WHICH SECTORS HAVE BOUGHT THE MOST CYBER COVER?*



* Respondents were asked to rank the top three

THE FUTURE

"We are seeing a pronounced increase in cyber cover enquiries and the percentage of those converted into policies. We note a particular awareness of cyber cover from the professional services sector, which is a key buyer of cover." Andrew Lewis, cyber expert, QBE European Operations

According to both brokers and insurers, financial institutions are buying nearly four times more cyber cover than the healthcare sector. Yet, as the insurers pointed out, healthcare is in a potentially dangerous position, seemingly not buying enough cyber cover to counteract its level of vulnerability.

Sole traders and individual consumers are the two sectors buying the least amount of cyber cover yet figure higher on the vulnerability list, suggesting the insurance industry could do more to encourage these sectors to act against the potential perils of cyber. The same applies to the energy and utilities sector: brokers and insurers placed this fairly high up in terms of vulnerability to a cyber attack, yet this sector is not buying the corresponding amount of cover. If prevention is the best cure, this sector perhaps needs to be targeted with extra resources and campaigns to highlight the severity of the problem.

In line with the steadily increasing cyber attacks reported in the media, cyber policy purchases also have been on the increase over the past 12 months, with over one-quarter of brokers reporting an increase of more than 50% in numbers of policies sold. One-fifth say the number of sold policies had increased by between 26% and 50%. Only 12% said they had seen neither an increase nor a decrease in this number.

This sharp increase in companies buying cyber policies will only accelerate over the next 12 months, according to respondents in this research. When asked to predict how many policies they expected to sell in the next year, nearly one-third of respondents believe their figures will increase by over 50% and over three-tenths have predicted an increase of between 26% and 50%.

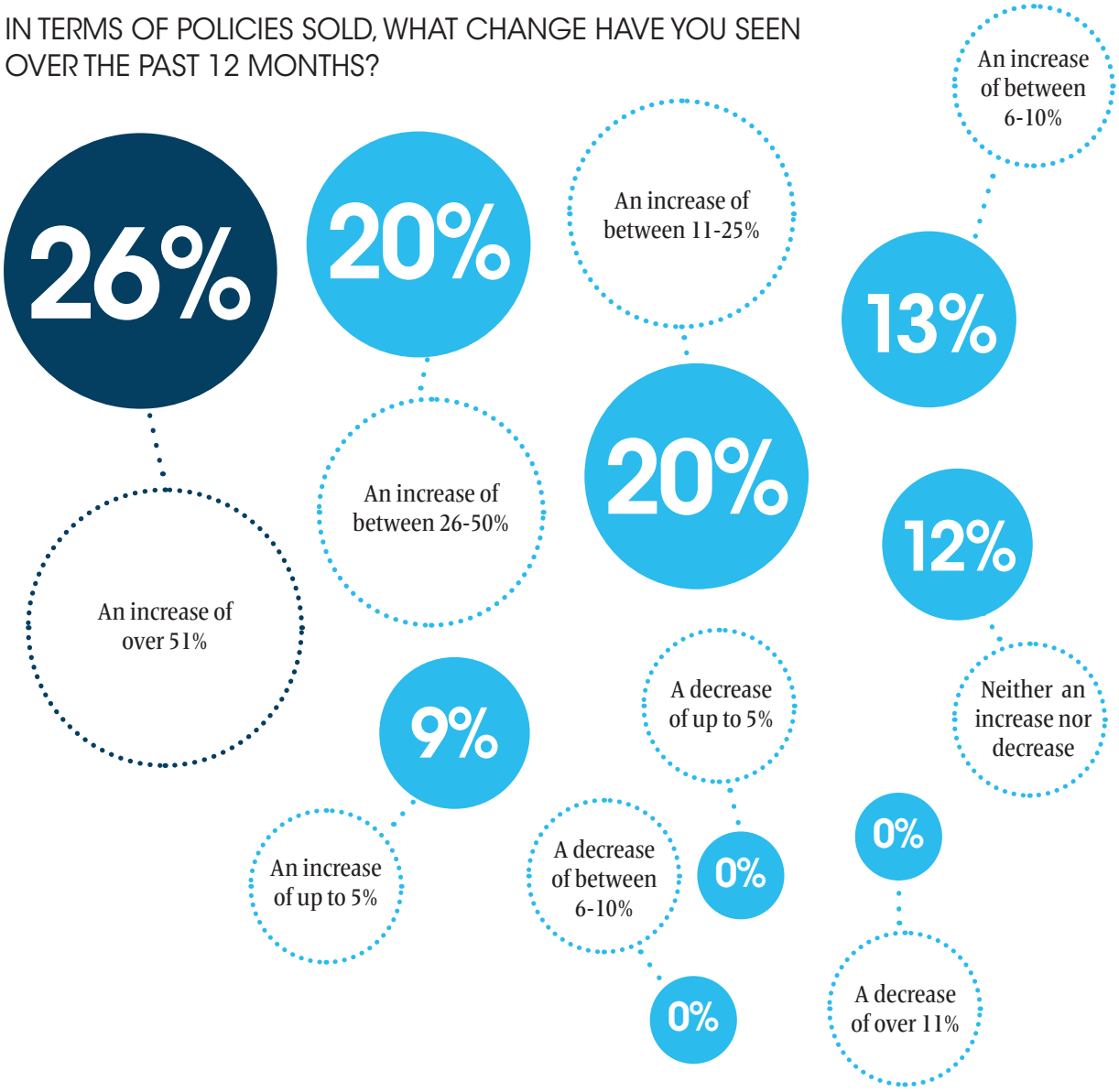
Only 6% professed to predict neither an increase nor a decrease in cyber cover purchase. Even the most cautious of respondents expect a considerable increase in cyber policy purchases over the course of 2018, and the industry has the challenge to ensure these policies truly are cyber-proof.

Evidently the challenges of cyber insurance are many. From modelling trends to pricing policies, it is imperative the insurance industry foresees challenges and risks before its customers, but sometimes the problem is not so much external sources but internal company habits and an unwillingness to embrace change.

Education was listed as the most challenging aspect of cyber insurance – educating clients, explaining the need for cyber cover, raising awareness of risks. As one respondent explained: "The smaller SME market will continue to see this product/cover as something which isn't applicable to them." Another respondent commented: "Continuing to educate customers – lots are much more interested in having discussions after something has happened."

Clients demand to make informed choices for their purchases. Currently, this is not the case with cyber as the historical data upon which these choices can be made is still filtering in. The second most challenging aspect for insurers and brokers is understanding cyber themselves and keeping apace with different cyber attack trends. One respondent said one issue is "keeping up to date with the advances in technology and advances made by cyber criminals, as we will always be a step behind them".

IN TERMS OF POLICIES SOLD, WHAT CHANGE HAVE YOU SEEN OVER THE PAST 12 MONTHS?

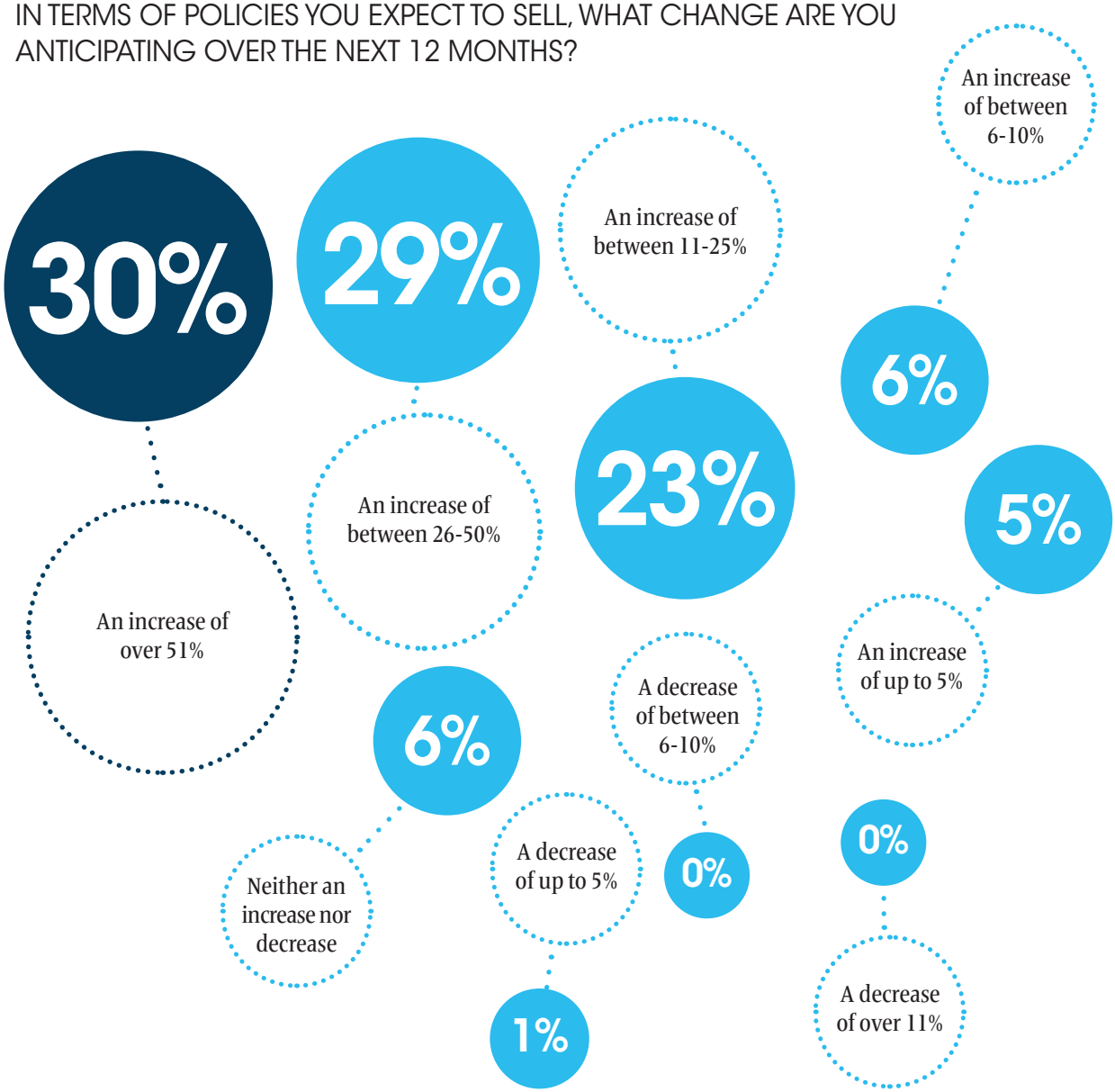


GDPR compliance is a less-pressing concern, on a par with pricing and cost. Policy wordings and the anticipation of huge claims occupy the minds of several respondents, while for brokers, specifically, the uniformity of coverage from insurers appears to be a concern. Insurers also would be happier with simpler policies, according to one respondent whose cyber-related challenge was described as "brokers understanding the cover and being able to confidently sell it to their clients. There are too many policies on the market with different wordings, clauses and conditions".

The crossover between cyber and crime was mentioned by several respondents as "clients expect crime to be covered, and insurers need to come up with a suitable solution". ■

THE FUTURE

IN TERMS OF POLICIES YOU EXPECT TO SELL, WHAT CHANGE ARE YOU ANTICIPATING OVER THE NEXT 12 MONTHS?



SECTION FIVE

PERSONAL LINES

PERSONAL LINES

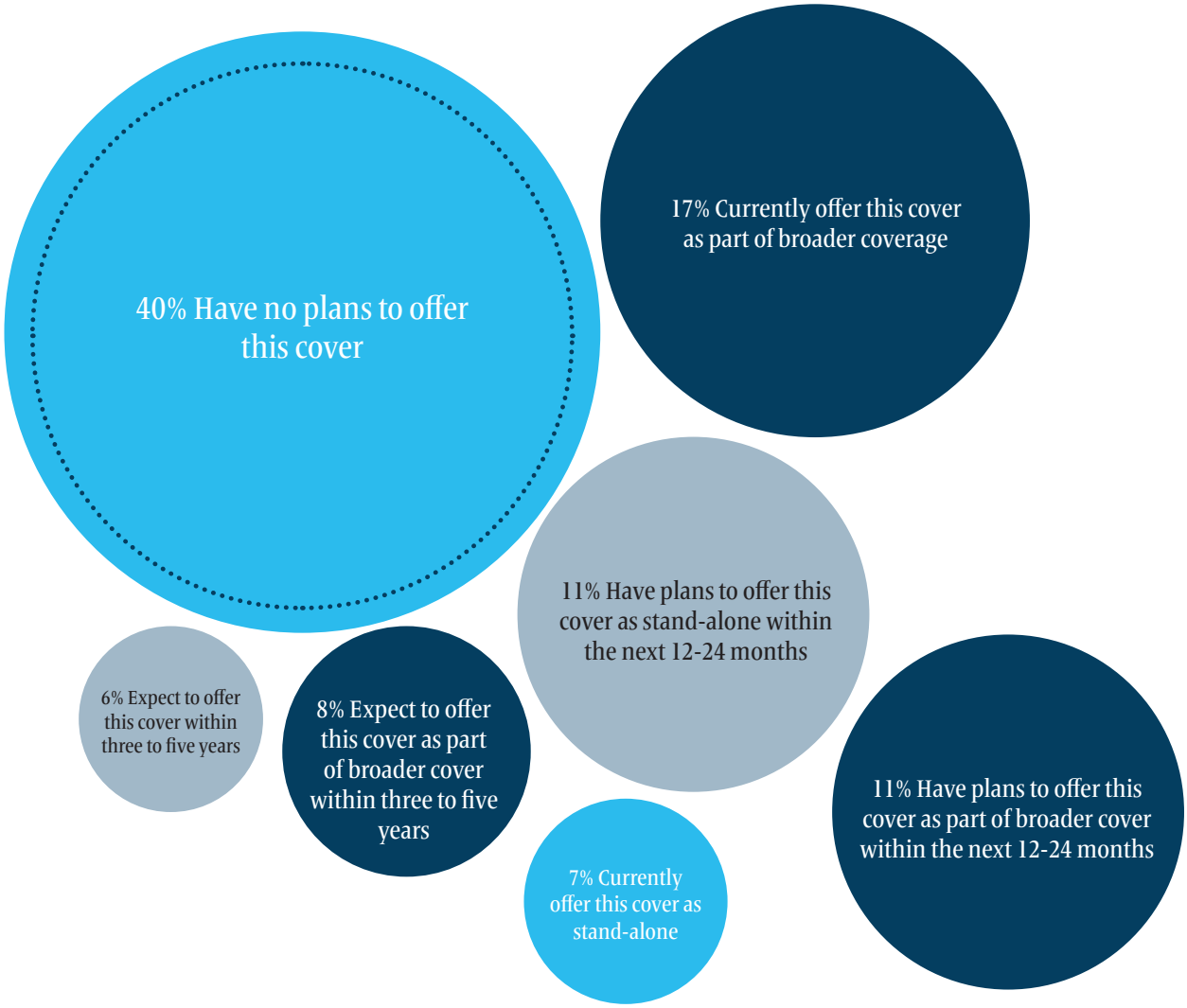
WITH CYBER PROTECTION INCREASINGLY ON the minds of companies in the UK, how long until it preoccupies the minds of individual consumers?

For insurance companies working in the personal lines sector, the cyber scene is still awakening. Brokers do not appear to have concrete or pressing plans to take cyber cover to the masses, with the majority – nearly two-fifths – of respondents saying they had "no plans" to offer this cover. For insurers, half are not considering bringing cyber into the personal lines space.

In the long term, offering stand-alone policies to individuals appears to be the less popular way forward. But brokers believe they will get more traction with stand-alone policies in the short term, rather than with policies that include cyber as part of greater cover.

For insurers, offering cyber as a package is deemed more appealing to customers than stand-alone policies. Only time will tell. Currently, the cyber offering is still relatively new, and stand-alone

IN TERMS OF PERSONAL LINES [INDIVIDUAL] CYBER COVER, DO YOU



"As this fascinating survey demonstrates, cyber crime is not a theoretical threat or a 'panic story'. For many millions of people, it is already an unpleasant and unwelcome reality. Getting the terms of the policies just right will never be easy, but for both insurers and brokers, a new risk invariably creates a new opportunity." Lord Hunt of Wirral, chairman, British Insurance Brokers' Association

policies may be more appropriate as new data is collated and analysed.

DATA BREACHES

Nearly two-fifths (37%) of the general public, when questioned about their online security, stated they had been hacked or suffered a data breach, whereby a third party had used their information for illicit purposes. Londoners are by far the most likely respondents to have suffered a breach, as is the 25-34 age group bracket, 50% of whom admitted to having been hacked four times.

Having an email account hacked is the most common type of data breach among respondents (46%). This is followed by the use of personal information to purchase goods and service, the option chosen by 42% of the sample group. A further 27% had their personal information stolen, while 36% had experienced the hack of a social media account. Londoners experienced on average twice as many social media hacks as the rest of the country. Identity fraud affected 20% of respondents, although the majority reside in London and Yorkshire and the Humber.

Other types of data breaches include credit card cloning, having an online bank account hacked, or having a Playstation or Paypal account hacked. One respondent had their eBay account hacked and used to sell products the person didn't own.

FEMALES FAIL WITH ONLINE SECURITY

Those living in Scotland and the South East accounted for half of all respondents who had been hacked or suffered a data breach more than five times. Equally, those in the 45-54 age bracket comprised 50% of those who had been hacked or suffered a breach.

While half of the population had only been hacked once, almost one-third confessed to having been a victim of a data breach or hack twice. Londoners and those in Yorkshire and the Humber made up 56% of those who had had four cyber-related negative experiences.

Women may not be taking online security seriously enough. Three times more women than men admitted to having been hacked more than five times, an astonishing figure highlighting the need to address women's online security knowledge.

However, women showed themselves to be far more proactive than men in taking security steps following an attack, with over three times more mensaying they had "carried on as before" and not taken any extra steps to secure their data. Almost twice as many men as women admitted they had only taken "a few steps but nothing wholesale".

After experiencing a cyber attack of any sort, an overwhelming majority of 80% took steps to ensure their data would be more secure in the future and still profess to be "very careful". Another 11% took security-enhancing steps for a while but "not so much now", while 6% admitted they had taken a few steps, but nothing of much substance.

PUBLIC CYBER POLICIES

Professional consultancies advising on prevention measures against cyber attacks already are present at the commercial level of insurance. Offering such a service to the personal lines market also may be a viable option. Nearly 40% of the general public respondents are interested or very interested in this service, with men slightly more interested than women.

Those within the 25-44 age group showed more interest than the other age groups. More than 60% of Londoners and Northern Ireland inhabitants would be interested or very interested in cyber-attack consultancy services, while Scotland, Wales and the South East showed the least, middling at around 30% interest.

When asked whether they would be happy to pay for this service, 42% replied yes, indicating a growing realisation of the importance of cyber protection.

Men were more likely than women to pay money for advice in all age groups except one. Those unhappy to pay outweighed those prepared to pay for such a service, usually by more than 50%.

In the 25-34 year age group, 52% were willing to pay for a service. Similar responses were seen for geographical areas: in all areas except one – London – the refusals vastly outnumbered those willing to pay. For the capital, 66% of the population would pay.

Wales was the area least likely to pay, with only 28% stating they would.

The 25-34 age group was the most likely to purchase an insurance policy that reimbursed for lost funds due to a data breach or cyber attack, with nearly 50% saying they were either interested or very interested in being reimbursed after a financial breach.

On the whole, the public is not very interested in purchasing an insurance policy that protects against cyber bullying and is only fairly interested in being reimbursed for items ordered online that do not arrive in time or are not as expected.

Of greater note, nearly two-fifths expressed possible interest in an insurance policy that rectifies damage to a computer or device, for example, locating and removing a computer virus.

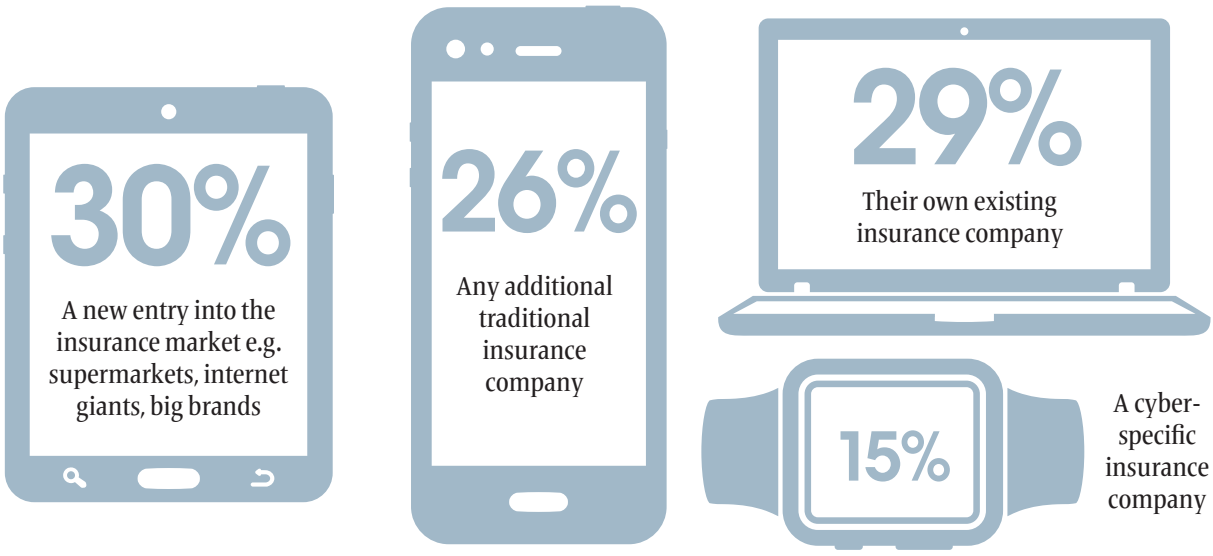
The 40% of insurers and brokers who do not intend to offer personal cyber cover may be missing an opportunity, especially since there are other avenues for the public to procure insurance than through a traditional insurance company.

THE BUYING MARKET

For 32% of the insurer respondents, start-ups or “new” insurance companies pose a fairly strong threat in terms of offering cyber insurance in the commercial lines market.

In the personal lines space, the threat may not be present yet, but is likely to emerge. The majority of public respondents saw themselves purchasing some kind of cyber or online insurance within the next five years, with just under one-fifth believing they would never have the need to purchase such a product. Admittedly, most of these responses came from the older population.

DO INSURERS BELIEVE THE PUBLIC WOULD PREFER BUYING CYBER INSURANCE FOR THEIR PHONES AND GADGETS FROM TRADITIONAL OR FROM 'NEW' INSURANCE COMPANIES?



Insurance companies may rest assured, however, that regardless of the start-up explosion or sharing economy, the general public would still prefer buying their cyber or online insurance for their phones or gadgets from traditional insurance companies.

Exactly half of respondents chose traditional companies over newer ones, which attracted only 13% of responses.

Insurers, however, are not convinced. Nearly 15% believe the public will turn to a cyber-specific insurance company, while almost 30% feel a new entry into the insurance market, such as supermarkets, internet giants or big brands, might scoop up the customers. The same percentage are certain the public will turn to their own existing insurance company.

Whatever happens in the near future, the public will make better and more informed cyber choices about cyber thanks to data scientists' and experts' analysis and models.. The landscape is still very much being drawn.

Overall, the relatively high number of "unsure" answers from both the industry and general public surveys confirms the cyber revolution has just begun.

In the invisible, borderless cyber world, almost anything is possible.

Cyber is about communication and control. With technology in the wrong hands, it can have

devastating results, ruinining many lives. Yet there is a consensus within the insurance industry that many amble through life with an attitude of "it won't happen to me".

Who better to inform them that "it just might" than the people striving to deliver the best possible protection: the insurers, brokers and managing general agents. ■

AUTHOR

MICHÈLE BACCHUS

As former research and commercial projects editor for *Post*, Infopro Digital's flagship insurance magazine, freelance journalist Michèle Bacchus brings a wealth of proofreading and editing experience from various sectors, including property, finance and construction. Recent research projects include the State of the Risk Management Nation, Lloyd's & the London Market, and *Post*'s biennial census.

Michèle is half-French and lives in Somerset with her two children.

WE'LL TAKE IT FROM HERE™

CYBERSCOUT sets the gold standard for identity and data defense services – from proactive protection to education to successful resolution.

For more than 13 years, **CYBERSCOUT** has combined on-the-ground experience with high-touch personal service to help commercial clients and individuals minimise risk and maximise recovery.

CYBER RESEARCH 2018

Insurance POST

In association with CYBERSCOUT®

WE'LL TAKE IT FROM HERE™