Weightmans

Weightmans LLP
33 St Mary Axe
London, EC3A 8AA

Weightmans LLP & Insurance Day

Cyber Risk Survey Report

November 2015

Table of Contents

1.0 Methodology

The digital age which we operate in, constantly presents new challenges to the (Re)insurance market. This Cyber Risk Report was conducted by Weightmans' EC3 team to provide clarity on the extent to which (Re)insurers are ready for these challenges.

This report was prepared on the basis of a survey carried out over two weeks between 28 September and 9 October 2015. It canvassed insurance stakeholders in a set of 16 questions drawn up jointly with specialist magazine Insurance Day.

The 102 respondents were divided into three types: insurers, brokers and reinsurers. A number of questions were specific to one or two of these respondent groups only.

The answers were compiled and analysed by Weightmans' EC3 team. Their experience and input provided perspective into the survey results and were invaluable in helping shape both the main part of the Report and the comments under the answers to each individual question.

To supplement the survey findings, interviews were conducted with the following individuals:

- Niall Brophy, Technical Claims Manager, StarStone
- Graeme Newman, Chief Innovation Officer, CFC Underwriting
- David J. Shannon, Chair, Technology, Media & Intellectual Property; Chair, Privacy and Data Security, Marshall Dennehey
- Dominic T. Clarke & David Mackenzie, Blaney McMurtry LLP
- Francis Mackie, Partner, Weightmans LLP

Contributions were also made by the following individuals in Weightmans' EC3 team:

- Kieran Jones, Partner, Insurance Director, kieran.jones@weightmans.com
- Mike Grant, Head of Professional Risk, mike.grant@weightmans.com
- Edward Lewis, Partner, ed.lewis@weightmans.com
- Ling Ong, Partner, ling.ong@weightmans.com
- Colin Peck, Partner, colin.peck@weightmans.com
- James Denison, Associate, james.denison@weightmans.com
- Robert Crossingham, Partner, robert.crossingham@weightmans.com
- Ian Lavelle, Associate, ian.lavelle@weightmans.com

2.0 Foreword

The business world is transmogrifying before our very eyes, necessitating a wholesale re-think of the legal issues and risks surrounding it. The rise of technology is transforming manufacturing companies into software businesses, using increasingly digitised processes, with factories and plants controlled by computers - and mechanics gradually morphing into software technicians; services firms too are increasingly resembling software or data houses, now that so much business is conducted online and in the cloud.

The nature of crime is changing also. This October saw the Office for National Statistics showing cyber crime as a separate category of offence in the official crime figures, and the result is illuminating: whilst traditional crime is falling eight per cent, online fraud and cyber attacks now account for half of all crime.

The big question is: how prepared are we for this new cyber age? The challenges here are particularly acute for the (Re)insurance industry, responsible for underwriting these new risks for businesses and individuals. As the very nature of risk changes – or, in the words of Partner Ed Lewis, as old risks manifest in new ways – the industry needs to decide how it is going to measure them, and then how to provide cover.

The trouble is of course, that the bank of historical data needed to calculate risk in the future, simply doesn't exist. Indeed there is a paucity of data generally around cyber risk. This is why we decided to conduct this Cyber Risk Survey, as our contribution to the industry's discussion and debate. We hope you find this Report useful.

We believe the effects of the cyber revolution will be as transformative and far-reaching as those of the industrial revolution almost 200 years ago. We need to be ready for it.

Kieran Jones
Partner, Insurance Director
Weightmans LLP
kieran.jones@weightmans.com

The big question is: how prepared are we for this new cyber age?

Kieran Jones
Insurance Director

3.0 Overview – Cyber risk: from mystery to measurability

Options available to insurance professionals to ward against cyber claims are "very limited at this point", says one of the respondents to our Cyber Risk Survey, echoing a widespread belief in the sector that cyber risks are intractable as well as pervasive. But should that necessarily be the case?

The rise in high profile cyber attacks (The Ashley Madison and Talk Talk cyber breaches to name just two) has led to increased awareness of the risks as ones that can potentially affect any sector of industry and more than 80 per cent of respondents to the survey either collect, or plan to collect, cyber notification and claims data.

However, while data collection is an essential first measure in building up a knowledge base, 13.8 per cent of respondents do not analyse the data they have collected, 19.1 per cent merely anticipate collecting data in future and 18 per cent do not collect cyber notification and claims data at all and have no plans to do so. In total, over 50 per cent of insurance stakeholders are yet to take active steps to achieve a better understanding of cyber risks.

Cyber risk data depository

The systematic gathering and analysis of cyber notification and claims data should, in time, allow the sector to develop a historical data repository, enabling insurance professionals to draw up a clear picture and understand cyber risks, to design appropriate policies, to model their exposures accurately, and to set premiums at an appropriate price point. Ultimately of course, the more that insurers share this data, the clearer the picture will be for everybody. In practice this principle of sharing poses significant challenges, not least the need to stay within the confines of current data protection laws! This is undoubtedly going to be an interesting space to watch in the future, albeit one that for now is outside the scope of this Report.

In turn, data gathering should also help insurance professionals address a number of related issues such as fraudulent cyber claims. This is a concern to 80.6 per cent of respondents.

A more comprehensive cyber data repository should also assist in categorising cyber insurance products and in determining whether to address it as a risk in its own right or as the mere evolution of existing risks. Currently two thirds of respondents (62.9 per cent) categorise cyber insurance as a standalone product, which is in line with Lloyd's decision to give the class its own risk code. What the sector is yet to unravel is the impact of modern technology on 'old risks' and whether because of the new ways in which these can now manifest they should stack on more traditional forms of cover.

Options available to insurance professionals to ward against cyber claims are "very limited at this point."

50%

of insurance stakeholders are yet to take active steps to achieve a better understanding of cyber risks.

3.0 Overview – Cyber risk: from mystery to measurability

As things stand, only two thirds of respondents are confident they understand cyber risks and their impact on both the sector generally (64.3 per cent) and on their own business (66.7 per cent). It is unclear whether this reflects heightened awareness because of greater news coverage of cyber attacks, rather than genuine understanding of the nature and complexity of cyber risks.

Whilst understanding of cyber risks may be somewhat limited, respondents do appear to have grasped the pervasiveness of the risks to their policyholders: 85 per cent believe they affect all classes of insurance. However, there appears to be a disconnection between insurers' recognition of the threat to their policyholders and all classes of insurance on the one hand, and their perception of the threat to their own businesses on the other: only 52 per cent say that cyber risks are an issue for their own businesses too. The challenge, as in any business coming to terms with cyber threat, is to allocate clear responsibility for dealing with it. It may be that IT departments are ultimately those tasked with implementation but strategic decisions must be designed and developed in the boardroom.

"Whilst understanding of cyber risks may be somewhat limited, respondents do appear to have grasped the pervasiveness of the risks to their policyholders."

Major risks

It's not that the consequences of a cyber attack aren't fully understood. Reputational damage is perceived as a 'major risk' by more than 70 per cent of insurers, closely followed in the 'major risk' category by theft of personal data leading to a fine by regulatory bodies (68.1 per cent), and the risk also of theft of confidential information such as intellectual property leading to business interruption claims by policyholders (63.8 per cent).

More than half also considered business interruption as a 'major risk', both resulting from loss of essential data and while essential IT systems are down, (59.6 per cent and 55.3 per cent respectively), as well as the risk of claims arising out of the theft of personal data subsequently used to commit further crimes, principally fraud (57.4 per cent). These figures are reflected in the assessment made by brokers who took part in the survey, according to whom business interruption and data breach are key drivers in 30 per cent of cyber insurance purchase decisions, followed by data theft (20 per cent) and fraud (10 per cent).

Similarly, brokers place reputational damage at the top of the 'major risk' list for their clients' businesses, on a par with the risk of data theft for the purposes of committing crime (81.8 per cent), just before the risk of regulatory fine (72.7 per cent), with theft of business-sensitive data in equal third position with business interruption while IT systems are down (63.6 per cent).

The scale of regulatory risk – in practice, fines by the regulator for failure to comply with data protection law – is perhaps misunderstood in parts of the sector. Fines by the Information Commissioner's Office (ICO) are capped

It's not that the consequences of a cyber attack aren't fully understood. Reputational damage is perceived as a 'major risk' by more than **70%** of insurers.

3.0 Overview – Cyber risk: from mystery to measurability

at £500,000, much less than the average cost of a cyber attack on a large corporation, which the Association of British Insurers estimates at £1 million on average. However, a finding of regulatory breach may of course provide a platform for the victims of a data breach seeking to bring a separate civil claim.

Regulatory risk should also become a primary concern in anticipation of new European Union cyber security rules that are most likely now to arrive in 2017 (Network and Information Security Directive and new General Data Protection Directive).

In addition, two recent cases from the European Court of Justice should push the issue up the agenda for any entity operating in the European Union. On 1 October this year, the Luxembourg judges ruled that a company doing business in an EU member state came within the jurisdiction of that state's data protection authorities (Case 230/14 Weltimmo). Days later on 6 October, the court found the EU-US 'Safe Harbour' agreement (which gave special dispensation to US companies in certain circumstances to store European customers' personal data on American soil without interference from EU regulators) to be invalid (Case C-362/14 Schrems), a decision that will increase the level of data protection scrutiny in all EU member states.

Then there are the financial consequences of cyber attacks, with more than 90 per cent of respondents expecting claims payments on cyber insurance to increase in the next 12-18 months.

However, expectations of the possible increase in claims payments vary dramatically. Just over a third (36.6 per cent) expect these to rise between 1 and 25 per cent; just under a quarter (21.9 per cent) to rise between 26 and 50 per cent; less than ten per cent (7.3 per cent) to rise between 51 and 75 per cent; and one quarter (24.4 per cent) to rise by between 76 and 100 per cent. Such diversity could be the result of varied personal experience or of the jurisdiction in which respondents operate (insurers writing cyber risk in the US are notoriously more exposed). It could also suggest that no-one really knows how the cyber claims market will develop and that current risk models are failing to perform as they should. Further, it raises the question of how the sector could sustain a rise in claims without a rise in premium receipts. At the very minimum, every insurer should, as an immediate precaution, identify their cyber exposure and model their responses properly, as recently urged by Lloyd's. If an insurer cannot realistically produce an accurate model, then they should probably give serious consideration to whether it's appropriate for cyber cover to be given under their policies at all – the absence of clear modelling risks a shortfall in capacity to meet a systemic cyber loss spiralling through the market and financial catastrophe.

"Two recent cases from the European Court of Justice should push the issue up the agenda for any entity operating in the European Union... The cases of Weltimmo and 'Safe Harbour' will increase the level of data protection scrutiny in all EU member states."

At the very minimum, every insurer should, as an immediate precaution, identify their cyber exposure and model their responses properly, as recently urged by Lloyd's.

3.0 Overview – Cyber risk: from mystery to measurability

Taking precautions

Perhaps the greatest risk, lurking in the background is aggregation – the risk that an isolated incident, whether intentional or not, cascades through the whole sector. A simple example shows how quickly exposures can accumulate in cyberspace: imagine a cyber attack on a single Cloud provider that is under contract to a variety of insured businesses. The Cloud provider is hacked, compromising the security of all the companies' IT systems which are then exploited in a variety of ways, in turn resulting in large numbers of individual claims on a variety of policies and across a number of different classes. There are not only claims for business interruption and property damage, but also many against D&O policies where directors of affected companies are accused of failing to have had appropriate protection measures in place. Even personal injury claims are possible, including claims for emotional distress after the misuse of private information was "relabelled" a tort earlier this year by the Court of Appeal in Vidall-Hall v Google.

While anecdotally most professionals in the sector express grave concerns about aggregation, only two thirds of insurer respondents (65.8 per cent) say it is an issue for cyber policies. This brings up the classic insurance schoolbook problem: what precautions can you take to guard against a risk about which you know very little?

Concerns over systemic loss scenarios [are] a real issue, says one respondent, while others suggest careful review of policy wordings, [increasing] risk awareness, a deep dive in the covered value chains, and setting limits, including only covering attacks aimed at the insured alone.

Such comments should be given close consideration. They point at the lack of genuine understanding of cyber risk. They focus on restricting or limiting cover and could act as a disincentive for businesses to buy cyber policies. Why would a company buy cyber cover if the risk they hope to protect against manifests itself in such a way that the business will be left with no real protection? Or why would that same company take cyber cover if it can self-insure through appropriate risk management procedures? In practice, few are able to self-insure but many may be left high and dry with no choice but to find their own solution any way if the available cover is inadequate for their needs.

In fact, such is the cyber risk knowledge gap that less than half (45.4 per cent) of brokers in the survey think insurers understand the complexities involved in responding to a cyber attack.

What precautions can you take against a risk about which you know very little?

Why would a company buy cyber cover if the risk they hope to protect against manifests itself in such a way that the business will be left with no real protection?

Why would that same company take cyber cover if it can self-insure through appropriate risk management procedures?

3.0 Overview – Cyber risk: from mystery to measurability

They also report that while two thirds of insurers require their clients to have a cyber incident response plan, almost 55 per cent leave it to clients to judge when it should be triggered. More than a third, they say, do not insist on a response plan, and only nine per cent ask for regular monitoring of patterns so that aberrations can be detected. **Insurers may need to review their approach to the question of clients' response to cyber risk and be more hands-on.** This is not only because so little data is available about cyber risk but also, because the propensity for large scale loss is so much greater without risk management and incident response procedures in place and regularly rehearsed and tested. It also ought to provide reassurance that the sector understands the risk and has the ability to deal with it.

Reinsurers shared similar concerns in relation to levels of risk, with reputational damage and data loss featuring prominently as main risks, together with threats posed by complex viruses and the risk of aggregation. They also sounded further warnings, such as the detail of information they receive as being less than that available to insurers, and the possibility that cover for cyber-related events can unintentionally be included in traditional liability cover. Such were their reservations that a third did not provide reinsurance for cyber risk and had little interest in providing it in the near future.

Protect and prepare

Only when stakeholders start collecting data and analysing it will they be able to grasp the nature of cyber risk. And that's only just the beginning. Because cyber risk constantly evolves and mutates, like a virus, insurance professionals must make sure that whatever methods and processes they adopt keep up with the changes in the nature and shape of the threat. It will involve taking a more scientific approach where statisticians will play a key part.

Like all risks, the occurrence of a cyber accident cannot be forecast with precision; however, the sector should be able to manage both the incidence and the consequences of cyber risk better if it starts taking positive action now.

Reviewing policy wordings, limiting claims to certain types only, and setting compensation maximums are a possible response. But these are very reactive measures, and possibly counter-productive. A more constructive approach is for stakeholders to take active steps to make sure they gain a deeper understanding of cyber risk and are nimble enough to respond to risk as it evolves. This means, inevitably, building and maintaining a data repository recording occurrences, causes and extent of cyber attacks. Only then will cyber risk become less of a mystery and more of a measurable phenomenon. It won't disappear but the sector will be able to manage it with much greater accuracy.

"Only when stakeholders start collecting data and analysing it will they be able to grasp the nature of cyber risk. And that's only just the beginning."

Because cyber risk constantly evolves and mutates, like a virus, insurance professionals must make sure that whatever methods and processes they adopt keep up with the changes in the nature and shape of the threat.

4.0 Interviews

The increased commoditisation of insurance services threatens to be a stumbling block in the industry's attempts to understand and address the new cyber threat. Whilst we continue to develop our knowledge of cyber risk, we must ensure that we devote proper time and attention to understanding the impact on the cover we provide to our insured clients - this is at odds with a commoditised approach. The industry needs to take the time to understand what insured clients' businesses are really all about: how they operate, what they are trying to achieve in their marketplaces, where their risks and exposures are as they do this, and what they need cover for.

This type of dialogue between Insurer and Insured was commonplace until technology enabled new methodologies in some parts of the market to increase volumes, reduce time input, lower costs (and of course ultimately the prices of premiums). Somewhere in this race to commoditise, in certain quarters we have lost the dialogue between Insurer and Insureds. In some instances, companies can now select their preferred product from a drop-down menu and buy the cover they want with the click of a button. Whilst this may be an acceptable, and indeed, practical approach in some parts of the market where risks are well known and products well established, (an arguable point in my view), in contrast it is wholly insufficient where providers and underwriters are grappling with new risks – or rather, in the words of Weightmans' Ed Lewis, 'old risks manifesting in new ways'.

Even as a clearer picture starts to emerge around the cyber issue, a further challenge is that this picture will keep changing. New technologies will emerge bringing different types of cyber threat; market dynamics will shift; and legal/regulatory frameworks will change too. [Indeed just this month two ECJ judgments (Safe Harbour and Weltimmo) disrupted the rules around which jurisdictions govern data breaches, for businesses trading online across borders.] So this 'deep listening' to insureds has to be more than just a one-off exercise if we are to understand the risks we are covering and protect our own businesses as well as our clients'. We need to rediscover this practice as an on-going habit.

So is the rise of cyber going to be our cue to return to those old-fashioned practices of insurers sitting down face-to-face with insureds, getting under the skin of their business to truly understand the risks they are covering? Now there's an irony...

Interview conducted with:
Niall Brophy
Technical Claims Manager
StarStone

"Somewhere in this race to commoditise, in certain quarters we have lost the dialogue between insurer and insureds."

" 'Deep listening' to insureds has to be more than just a one-off exercise if we are to understand the risks we are covering and protect our own businesses as well as our clients'."

STARSTONE

4.0 Interviews

A big question for the insurance industry is whether cyber risk is best dealt with by specialist cyber insurers, or by existing class specialists. The answer will be different for each category of loss. But for some, undoubtedly it's the class specialists that will have the edge when it comes to understanding the exposure. Here's why: when it comes to cyber, both halves of the risk assessment equation - the "likelihood" of an incident occurring and the "impact" (i.e. cost) if it does - are hard to fathom, simply because we don't have a bank of historical data to rely on. But within certain classes, particularly property damage for example, at least the "impact" side of the equation is more easily understood by the class specialists. Take for example a cyber attack on a manufacturing plant where processes are controlled by computer, so the attack causes a number of critical services to fail, including temperature control for example, resulting in property damage. Now, whilst it may have been impossible to predict the likelihood of the cyber attack in the first place, assessing the damage should be altogether easier for those familiar with property loss. However other categories of insurance will be better served by stand-alone cyber policies. In short, the point is that the property market is generally best positioned to deal with loss and/or damage to tangible property (regardless of how it is caused) and the cyber market is best positioned to deal with loss and/or damage to intangible property.

I do worry that many parts of the (Re)insurance industry are seeking to deal with cyber risk by focussing far too much on exclusions. This just isn't good enough if you want to be seen as an insurer that facilitates clients' business, rather than obstructs it. For example, a director of a financial institution may have job responsibility for implementing the organisation's data security policy – and if they fail in that duty for some reason, they will expect their D&O policy to cover them. If this sort of risk is routinely excluded, in an age where all business is increasingly being conducted in cyberspace, and often as much as 90 per cent of a director or officer's work is done over email or on the cloud, then insureds are going to query their D&O premiums more and more – and ask what their insurers are actually doing to earn them.

Insureds just want cover for what they do. They don't want to have to worry how their D&O policy interacts with a cyber policy; they certainly don't want duplication of premium costs; but equally, they don't want gaps in their cover. This is what the insurance industry needs to get its head around. And putting itself in the shoes of its insured clients would be a good place to start.

Graeme Newman
Chief Innovation Officer
CFC Underwriting

"I do worry that many parts of the re/insurance industry are seeking to deal with cyber risk by focussing far too much on exclusions. This just isn't good enough if you want to be seen as an insurer that facilitates clients' business, rather than obstructs it."

4.0 Interviews

Since the US insurance market has been writing cyber cover, if there's one single lesson we have learned that would benefit our UK cousins, it's that you need to assume there will be a cyber incident for any business you cover, to the same extent you assume now there will be a motor claim for example, a smashed truck in an insured's fleet. The questions to pay attention to are how to discern what's a good risk and how to limit your cover. As the market on this side of the Atlantic has become more used to writing cyber cover, it has learned to limit policies in terms of payouts, and also in prescribing ever more specifically what events will and won't be covered. Cyber policies have gradually become more and more specialised as time has gone on. If a policy lays out clearly what is included / excluded, what the limit is for each area of potential claim and how this interacts with other policies, you will have a much better understanding of the risk that you're indemnifying.

Just at the moment, the US insurance market is agog with news of an interesting model for cyber cover that has just reached the market: at a time when businesses are finding it hard to obtain the coverage they are looking for following the spike in high-profile data breaches, in September this year ACE brought out a $100 million primary policy for cyber coverage. In exchange, applicants have to open themselves up to unusually intense scrutiny of their data security policies, systems and compliance during the underwriting process, possibly even an on-site investigation by one of ACE's outside cyber security firms. It will be interesting to see how this sells.

Certainly this new product shows the general direction of travel in the US, certainly amongst the larger insurers: if insureds want higher limits and more expansive coverage, (which they do), they are going to have to open themselves up to more examination and review of their policies and procedures concerning data security.

However, the smaller and mid-market insurers are still learning as they go. They have yet to work out exactly what is a good risk and what isn't – and it's quite possible they will get their fingers burnt in the process of their learning.

David J. Shannon
Chair of the Technology, Media & IP practice at Marshall Dennehey;
Chair Privacy and Data Security,
Marshall Dennehey

"If insureds want higher limits and more expansive coverage, (which they do), they are going to have to open themselves up to more examination and review."

MARSHALL DENNEHEY
WARNER COLEMAN & GOGGIN
ATTORNEYS-AT-LAW PA NJ DE OH FL NY

4.0 Interviews

In Canada, the insurance industry has been grappling with the challenges of cyber risk coverage for much the same length of time as has the UK market. Canadian insurers have not adopted a common approach, nor have they attempted to. There remains considerable inconsistency in the Canadian market as to how best to approach the information and technology insurance challenge. Disagreement extends even to the importance of cyber insurance: some believe it to be the single most important issue facing the industry, while others are yet to be convinced it is a key concern at all.

There is also a divergent approach in respect of underwriting. Some believe that it is best to chase the market as it develops, while others wish to hold back until the risks can be fully understood in actuarial terms. Clearly there are dangers in rushing in where others fear to tread. The fallout could be ugly. Many carriers are issuing broad coverage notwithstanding the limited information available pertaining to the scope and size of risk. This is done with reason, as broad cover is demanded by the Canadian market. Such carriers expect to learn through experience while building market share.

It is a difficult position for insurers. It will only be when losses begin to occur with regularity, and claims are denied, that policy wording will be tested in the courts. It is hoped that, over time, insurers will be able to start building real confidence in their models. Unfortunately, in this new insurance market, that time is some way off.

While Canadian carriers often look to the US market for claims experience, even the US provides little in the way of insight. Few claims have been litigated. What small amount of litigation has occurred has not been particularly instructive. Moreover, with the increased use of arbitration clauses, adjudication on coverage issues is not publicly available.

Eventually the metaphorical tide will finally go out. Only then will we see who's wearing swimming trunks and who isn't.

Dominic T. Clarke
Blaney McMurtry LLP

David Mackenzie
Blaney McMurtry LLP

"It will only be when losses begin to occur with regularity, and claims are denied, that policy wording will be tested in the courts."

"Eventually the metaphorical tide will finally go out. Only then will we see who's wearing swimming trunks and who isn't."

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

4.0 Interviews

This summer (June 2015) the LMA launched a new Cyber Business Panel "to identify issues of concern to Lloyd's underwriters relating to cyber risk". The first position of this new panel is one of natural caution: the LMA's current view of how best to tackle cyber risk is very much focussed on how to exclude it from policies. Given the LMA is a representative body, this is not surprising. From the many ongoing discussions we have with senior movers and shakers in the industry, it appears that the London market is presently very cautious about providing cover for anything cyber-related, other than for the more traditional areas such as privacy and data breaches. Their stance is simple: don't get involved in risks you don't know and are still developing – whatever the pressure from outside the market.

The latest string of high profile news stories of cyber attacks has brought home a new realisation that the fallout from these events could stretch far beyond what any of us could contemplate even just six months or a year ago: given it is so much easier than many thought for computer security systems to be breached and data stolen, it's not hard to envisage the possibility of hackers accessing computer systems to take over control of a factory, a power plant or on-board computers. Underwriters just don't have the appetite for this scale and complexion of risk – as the risk assessment is complicated, and third party liabilities, the consequential losses and the scale of the business interruption claims could be near-limitless. What we are seeing in society is that the very nature of cyber risk is changing, and growing in a way that means these sorts of attacks increasingly affect all our lives and in every aspect.

Although businesses want to buy this cover, the market presently doesn't want to offer comprehensive cover – and that must be right until the industry has got its collective head around the risks and understood them in full. For the present, until the true character of the risks we are talking about are properly understood, a cautious approach has some merit in it. In my view, the correct response to market pressure is to dedicate time, money and other resources to deepening our understanding of cyber risk and its assessment, until we can offer more constructive solutions to insureds. That's what we all need to commit to.

Francis Mackie
Partner
Weightmans LLP
francis.mackie@weightmans.com

"The latest string of high profile news stories of cyber attacks has brought home a new realisation that the fallout from these events could stretch far beyond what any of us could contemplate even just six months or a year ago."

Weightmans

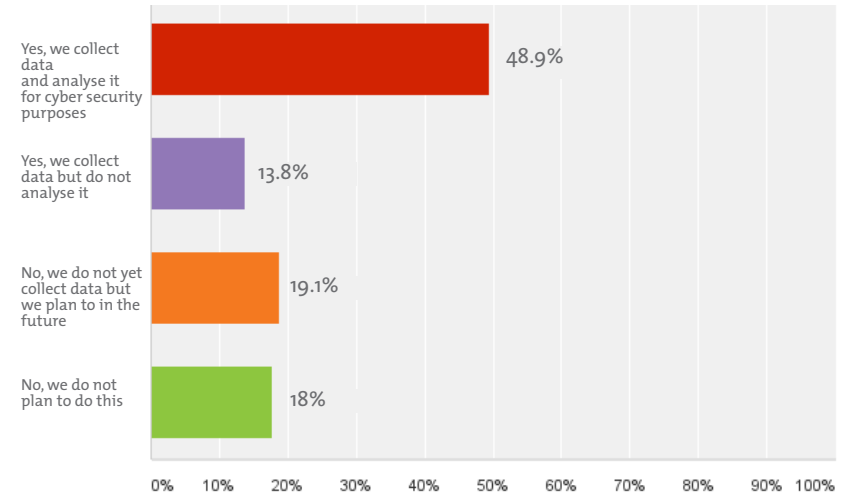
5.0 Close Up – Respondents' answers in detail

All respondents

Q: Are you, or do you plan to, collect data from cyber insurance claims?

A: Answers to this question suggest that the sector is keen to understand and prepare for cyber risk, with more than 80 per cent of respondents (81.8 per cent) saying they collect or plan to collect data from cyber insurance claims. However, there is still a significant amount of inertia. At the moment less than half (48.9 per cent) collect data in order to analyse it, while 13.8 per cent do not collect any data. Perhaps more worryingly, nearly one in five respondents (18 per cent) do not plan to collect cyber insurance notification and claims data in the future either. It is possible that these respondents do not write cyber policies but this is no less of a concern. Cyber risks can easily stack on other types of cover, so it's not only insurers writing cyber policies who can be affected by cyber risks. All insurers are potentially vulnerable and should start tracking that risk.

Do you collect data from cyber insurance claims?



Q: How concerned are you about fraudulent cyber insurance claims?

A: The possibility of fraudulent cyber insurance claims is a concern for a large majority of respondents (80.6 per cent) but this concern is relative: 43 per cent are 'very concerned' and 37.6 per cent only 'slightly concerned'. (Only one in five is not concerned.)

One of the difficulties fuelling this concern could be that, unlike motor insurance and personal injury (Employer's Liability and Public Liability) – the two most prevalent areas for fraudulent claims – the location and identity of a cybercriminal at the moment of an attack are notoriously difficult matters to pinpoint, making it even harder still to distinguish between fraudulent claims on the one hand from legitimate ones on the other.

At the moment less than half collect data in order to analyse it, while 13.8% do not collect any data. Perhaps more worryingly, nearly one in five respondents do not plan to collect cyber insurance notification and claims data in the future either.

5.0 Close Up – Respondents' answers in detail

Q: How are you categorising cyber insurance products?

A: Only two answers were possible: respondents either categorised cyber insurance products as standalone or as part of other policies. Nearly two thirds said they categorised it as a standalone product, with the remaining third categorising it as part of other policies. The split in the response is symptomatic of the state of flux in the sector. Cyber risk, while rightly regarded by most operators as pervasive and potentially affecting all areas, is still mostly viewed as a separate risk when it comes to categorisation. Strictly, true cyber risk is limited. It refers to non-physical damage such as loss or destruction of data or IT systems. But, in practice, cyber is often just a wrapper for a multitude of other risks, like crime, that have until now manifested in other ways. In 2007, for instance, hacker Alberto Gonzales broke into Heartland Payment Systems and stole credit card details allowing him to steel $171 million. He carried out the theft from the comfort of his bedroom. Fifty years earlier, it took Ronnie Biggs months of planning and 16 men to attack a Royal Mail train and make off with a paltry £2 million. Cyber crime has not changed the nature of crime – theft is still theft – but it has allowed criminals to carry out their deeds on a much larger scale and with greater ease.

For businesses affected by cyber crime, the risk remains the same: it involves property theft – usually data or cash. Directors could be held liable for failing to understand the risk and protect against it; the company could be fined by the regulator; and policyholders whose data was lost could sue for consequential losses (for instance if valuable intellectual property was stolen). So while cyber cover can be an offer on its own, cyber risk needs to be considered in the context of a wide range of other policies too.

In practice, cyber is often just a wrapper for a multitude of other risks, like crime, that have until now manifested in other ways.

Insurers

Q: How confident are you that you understand 'cyber risk' and how it impacts?

A: The sector may be apprehensive about cyber risk, but the answers to this question as to whether respondents are confident they understand cyber risk provides an optimistic basis to start tackling it. About two thirds of insurer respondents said they are either 'very confident' or 'confident' that they understand cyber risk and its impact, on both insurances and their own businesses (eg if their own IT system was hacked). More, however, are not as confident (merely 'confident' rather than 'very confident') that they understand how it would affect their own business. What's more, it leaves more than one third being 'not confident'. In addition, one should be cautious when interpreting these results. Confidence on the part of respondents is a positive

5.0 Close Up – Respondents' answers in detail

finding but it could nevertheless conceal a lack of genuine understanding. This could be especially so, given many insurance businesses regard themselves as 'not being at risk'.

Q: You believe that cyber risk is an issue for: a) cyber-specific insurances only, b) all classes of insurance, c) insurers' own businesses too (may tick more than one).

A: The rise in cyber attacks or IT malfunctions across all business sectors probably explains the apparent heightened awareness of the problem as one that could affect anybody. A very large number of insurer respondents (85.7 per cent) said cyber risk was an issue for all classes of insurance. There could be some complacency, however, with significant numbers saying this was an issue for 'cyber-specific insurance only' (35.7 per cent) and only half (52.4 per cent) saying it was an issue for their own businesses as insurers too. The answers to the next question provide further insight in relation to the latter.

Q: What is the level of risk to insurers' own businesses of a cyber-attack on their own systems?

A: Following on from the previous question, insurers were asked specific questions about cyber risk in respect of their own business. Only half said cyber risk was an issue for them as a business, but more detailed questioning here shows a much greater appreciation of the risk. All the risk levels mentioned, from business interruption to loss of confidential information, attracted more than 91 per cent acknowledgment as a risk to insurers' businesses (either 'major risk' or 'minor or limited risk'). The greatest risk was deemed to be reputational damage, with more than two thirds (70.2 per cent) seeing it as a 'major risk', followed by trouble with the regulator ('theft of personal data leading to a fine by the regulator'), with 68.1 per cent seeing it as a 'major risk'. In third place as a 'major risk' is 'theft of confidential information (e.g. intellectual property) disclosed to policyholders leading to a claim for associated loss' (63.8 per cent).

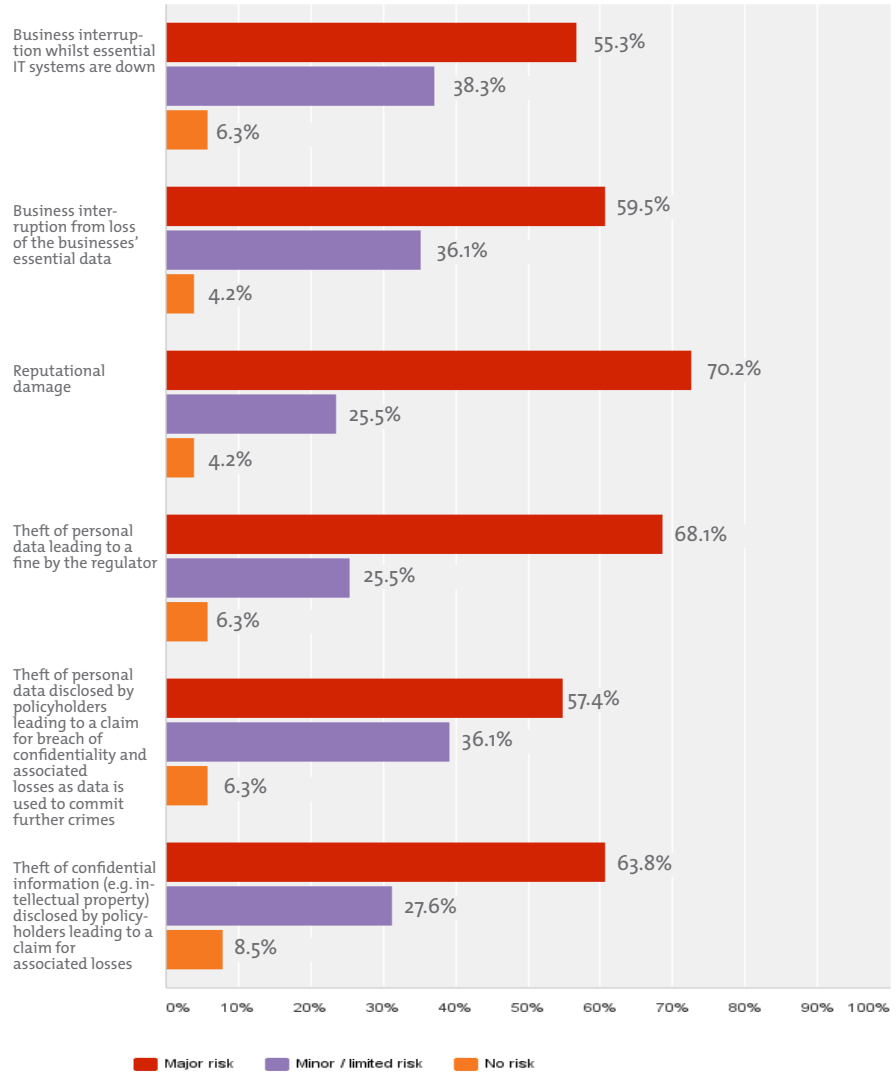
Reputational damage remains the most significant perceived threat when looking at 'major risk' and 'minor / limited risk' together, on a par with business interruption resulting from loss of data (95.7 per cent). This finding is perhaps at odds with everyday IT practice, where business interruption is more likely to result from a system's outage than loss of data. Instead, this high number is perhaps more an amalgamation of two distinct issues: the concerns surrounding data loss on the one hand and the damage caused by business interruption on the other.

Only half said cyber risk was an issue for them as a business, but more detailed questioning here shows a much greater appreciation of the risk.

5.0 Close Up – Respondents' answers in detail

Several risk levels came second when considering major and minor risks together: business interruption while IT systems are down; theft of personal data leading to regulatory fine, and theft of personal data disclosed by policyholders leading to a claim for breach of confidentiality and associated losses as data is used to commit further crimes (93.5 per cent). Theft of business sensitive information ('theft of confidential information such as intellectual property disclosed by policyholders leading to a claim etc.') came third but nonetheless scored a 91.4 per cent rate.

Perceived risk to insurers' own business of a cyber attack on their own systems



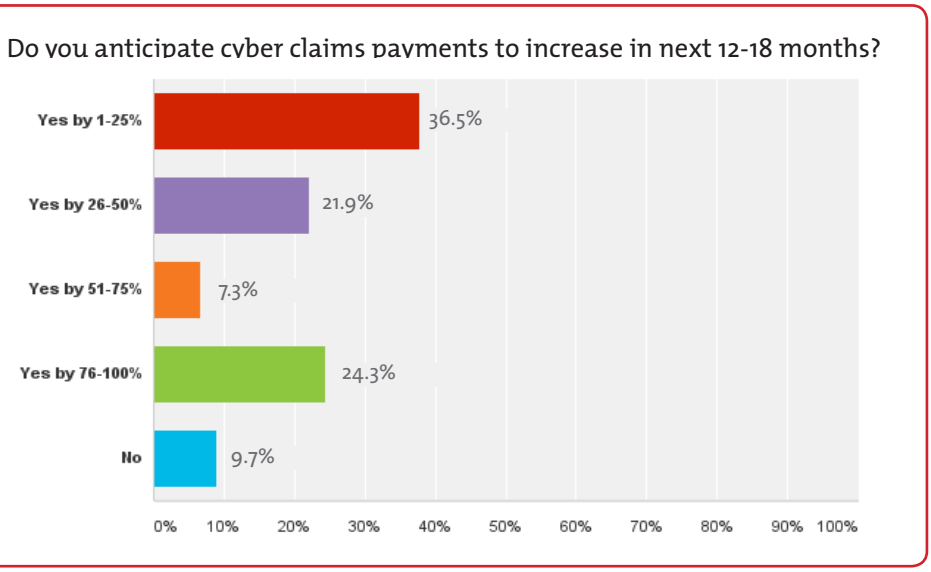
The risk of fines by regulators is likely to become a more pressing issue following a recent European Court of Justice decision rendering any organisation operating in the European Union subject to the jurisdiction of the authorities of the member state where it is doing business (Case C-230/14 Weltimmo).

5.0 Close Up – Respondents' answers in detail

This will be especially relevant for insurers selling cover online across the EU. Another ruling which found the EU-US 'Safe Harbour' agreement invalid is also likely to intensify the scrutiny by national data protection authorities on the way US businesses operating in the EU deal with customers' details (Case C-362/14 Schrems).

Q: Do you anticipate that claims payments on cyber insurance will increase in the next 12-18 months?

A: In a further illustration of the concern over cyber risks, more than 90 per cent of insurers say they expect claims to go up in the next 12-18 months. However, the disparity of the answers in relation to the scale of the increase could be a hint about the lack of information about the risks. Alternatively, this disparity could arise from a difference in the jurisdictions where cover is written, with insurers writing US business probably anticipating a far greater incidence of claims than their UK counterparts. More than a third of respondents (36.5 per cent) expect the increase to be between 1 and 25 per cent, and just over one fifth (21.9 per cent) to be between 26 and 50 per cent. Few expect the increase to be between 51 and 75 per cent (7.3 per cent), but nearly a quarter (24.3 per cent) fear it could double (between 76 and 100 per cent). Such variations are difficult to interpret. While well over half of the respondents (58.4 per cent) anticipate an increase of as much as half of current payment levels, would some respondents rather prepare for the worst by thinking in terms of payments doubling over that period? Or it could simply be that operators are trying to model for cyber exposure as accurately as possible in the absence of any reliable data?



In a further illustration of the concern over cyber risks, more than 90% of insurers say they expect claims to go up in the next 12-18 months.

5.0 Close Up – Respondents' answers in detail

Q: Do you consider aggregation to be an issue for cyber policies, whether as insurers, or insureds? And, if so, what precautions are you taking?

A: Aggregation is widely believed to be one of the most significant challenges for the sector. The potential for systemic risk arising from cyber attacks is just as real, as it is unlike anything the insurance market has seen before. But responses to this question were perhaps not as clear-cut as observers would hope. A comparatively low two thirds of respondents (65.8 per cent) see it as an issue, leaving just over one third (34.1 per cent) who don't.

There was a range of responses to the related question of what precautions insurers are taking in respect of aggregation, reflecting the complexity of the challenges set by the problem. One respondent even says that the precautions are "very limited at this point."

Looking at responses by type, one strand relates to education, with respondents talking about greater risk awareness, analysis, and understanding the covered value chains. Immediate action is another strand: some respondents say they are reviewing the wording of policies and tracking cyber exposure across all classes to set criteria. A third strand suggests that thought is also being given to setting limits, including only covering attacks targeted at the insured alone.

From a business perspective, there is undoubtedly a need for cyber insurance to be an enabler – a means to make businesses confident that they can operate in the digital age with protection against cyber threats. However, businesses also have to take steps to protect themselves by other means as well. The argument for cultural and behavioural change regarding the use of technology, as well as good governance, is compelling. Meanwhile, from the market's perspective, it is unlikely that the sector could sustain a worldwide cyber epidemic without limits on aggregation in some areas. One such area is business interruption (BI). Because insurers cannot expect to know all their clients' customers or trading partners over the period of a policy, it is therefore practical to expect limits on contingent BI exposure.

> **"Aggregation is widely believed to be one of the most significant challenges for the sector. The potential for systemic risk arising from cyber attacks is just as real, as it is unlike anything the insurance market has seen before."**

Brokers

Q: What threats are perceived to be the biggest driver for buying cyber insurance?

A: Business interruption and data breach were the two most significant drivers for buying cyber insurance, according to broker respondents (30 per cent each), just before data theft (20 per cent). Aside from the practical and regulatory implications, one possible explanation is that these have tended to be in the news more than other threats so far. This ought to be contrasted with insurers' response in relation to what they saw as the greatest risk – reputational

5.0 Close Up – Respondents' answers in detail

damage – and is not immediately reflected in brokers' appreciation of purchase drivers.

Fraud – perhaps surprisingly – was not regarded as a key driver (10 per cent), but this is consistent with the overall low level of perceived risk of fraudulent claims, as highlighted above.

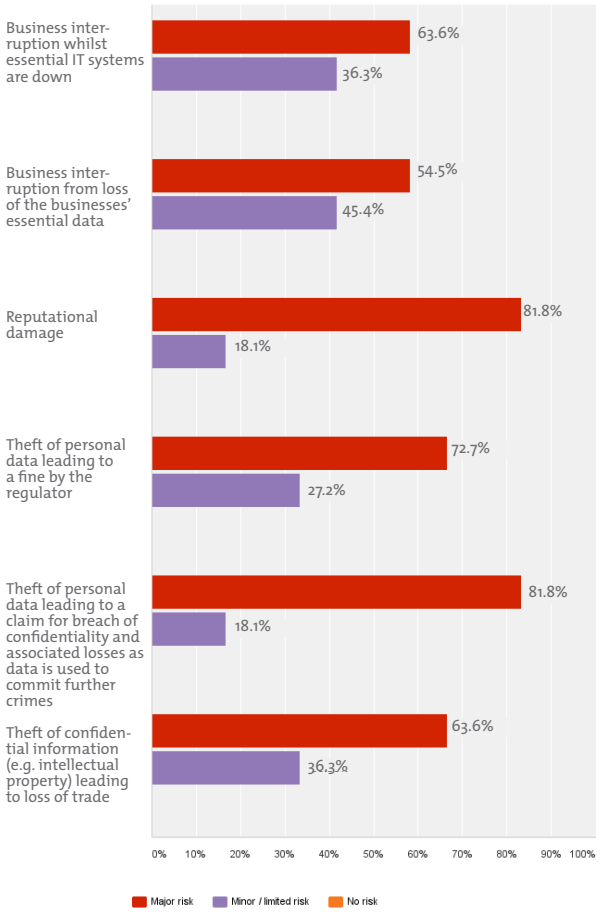
Intellectual property theft and libel via digital media were not seen as key drivers by any of the broker respondents. This, however, does not necessarily mean that protection against industrial espionage is not a consideration.

State-sponsored hacking, in particular, has featured regularly in news reports recently and has to be a major concern for any business whose assets are digitally stored IP and/or trade secrets.

Turning to brokers' assessment of the level of risk to their clients' businesses of a cyber attack, all felt that clients were vulnerable in some way.

Q: What is the level of risk to your clients' businesses of a cyber-attack?

Perception of risk to clients' business of a cyber attack



A: Turning to brokers' assessment of the level of risk to their clients' businesses of a cyber attack, all felt that clients were vulnerable in some way.

Much like insurers, brokers saw reputational damage as a 'major risk' (81.8

per cent), on a par with theft of personal data leading to a claim for breach of confidentiality and associated losses in cases where data is used to commit further crimes.

The closely related risk of theft of personal data leading to a fine by the regulator came second (72.7 per cent). In third position were business interruption while systems are down; and theft of confidential information such as intellectual property leading to loss of trade (63.6 per cent). Business interruption from loss of data scored a relatively low (54.5 per cent). This may not be a surprise finding, as loss of data is perhaps not as much of an interrupter as a systems outage. Variations on the loss concept, such as attacks via ransomware, however, should be ranked high on the list of concerns.

Variations on the loss concept, such as attacks via ransomware... should be ranked high on the list of concerns.

Q: Are your clients confident that insurers understand the complexities involved in responding to a cyber-attack?

A: Whether the sector as a whole and individual operators understand the nature of cyber risk is a recurrent question. Some admit to their lack of knowledge – usually based on the absence of any historical data – while others simply cannot say. This question was set in terms of trust and perception: do brokers think clients are confident that insurers understand the complexities involved in responding to a cyber attack? Just under half thought so (45.4 per cent). But that comparatively reassuring assessment left more than half (54.5 per cent) either not knowing (27.2 per cent) or answering no to that question (27.2 per cent). The purpose of insurance is to provide peace of mind, so these numbers would need to improve if clients are to feel confident that the knowledge chain going from insurers to brokers and back actually achieves this.

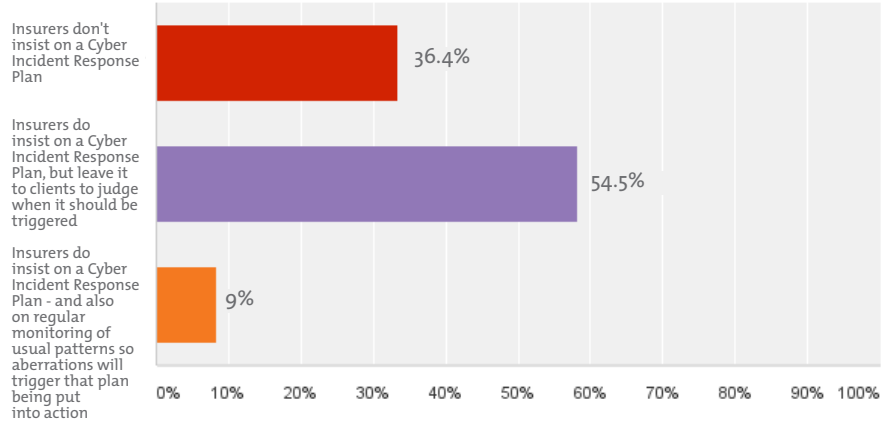
Whether the sector as a whole and individual operators understand the nature of cyber risk is a recurrent question. Some admit to their lack of knowledge... while others simply cannot say.

Q: If their insurers require a Cyber Incident Response Plan before agreeing cover, are you confident your client knows when it should be triggered?

A: A significant majority of broker respondents (63.6 per cent) say insurers insist that their clients must have a cyber incident response plan before agreeing cover. More than half, however (54.5 per cent), leave it to clients to decide what the trigger point should be for the plan being put into action. In addition, fewer than one tenth (nine per cent) of insurers require clients to undertake regular monitoring of usual patterns so that aberrations activate the response plan. A sizeable minority of insurers (36.4 per cent) do not require a plan. This is at odds with advice given by the Information Commissioner's Office and should be cause for concern amongst this cohort of respondents. Without such plans in place organisations are left at the mercy of cyber criminals, exposing board

members to personal liability for failing to protect their companies' and their companies' customers' interests properly.

Brokers: are you confident your clients know when their Incident Response Plan should be triggered?



Reinsurers

Q: Which class of business do you reinsure?

A: Of the reinsurers who took part in the survey, nearly all (90.9 per cent) reinsure professionals. The second largest market in which they are active is directors' and officers' (D&O) liability (54.5 per cent). These are classes where cyber is a particular threat and risks can attach to underlying policies even if they are not cyber-specific policies. Such findings reinforce the need for stakeholders to ask themselves more pressingly whether they are confident they understand the complexities of cyber risk and take steps accordingly. Marine and Energy came third and fourth respectively (36.4 and 27.3 per cent).

Q: From a reinsurance perspective, what do you consider to be the biggest risk posed by cyber threats?

A: This was a qualitative question, leaving respondents to come up with their thoughts, unprompted. Reputational damage and loss of personal data were mentioned, as were the risks posed by aggregation and attacks using malware and ransomware. One respondent mentioned Stuxnet, the 'worm' believed to have been developed by US secret services, that caused widespread malfunction at Iran's first nuclear plant. Some observers suggest that the story could now be written in reverse following the UK government's decision to grant China contracts to build new nuclear power stations in Britain. Further points more

> **The information a reinsurer receives is below the level of detail the primary insurer will benefit from.**

5.0 Close Up – Respondents' answers in detail

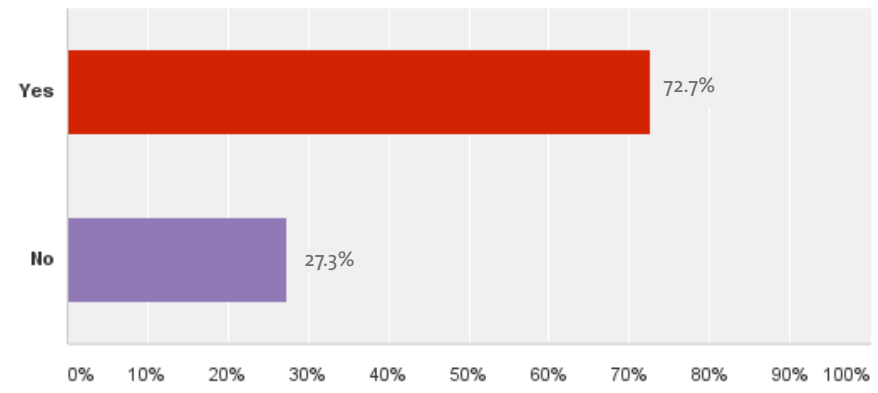
specific to reinsurers included concern that they would receive less detailed information than that available to insurers; and the unintentional inclusion of cyber cover in more traditional forms of insurance. There could, for instance, be claims under Public Liability policies following the decision in Vidal-Hall v Google. In this case the misuse of private information was relabelled a tort by the Court of Appeal and the recovery of damages for emotional distress were permissible. Following the ruling, some Public Liability policies now actively include cover for cyber liability, albeit without any apparent appreciation for the full extent of the exposure that creates. The danger is that ubiquitous "cyber cover" ends up being added automatically without further thought being given to consequences. Policies such as Public Liability are usually occurrence-driven, and insurers could be warehousing a whole range of exposures for which neither they nor their reinsurers are properly prepared.

The danger is that ubiquitous 'cyber cover' ends up being added automatically without further thought being given to consequences.

Q: Do you currently provide reinsurance for cyber risk? And if not, do you plan to?

A: Reinsurers may be just as concerned about cyber risk as other operators, but the market is not showing any signs of attracting new entrants. This possibly signals a more cautious approach and perhaps a greater appreciation for the uncertainty of the risks involved. Only two thirds (72.7 per cent) currently provide reinsurance for cyber risk. Further, none of those who do not currently provide cyber risk reinsurance intend to do so within the next six months, and a third do not intend to provide it at all (27.3 per cent). Of those considering providing it, one third plan on doing so within a year - and the remaining third within two years.

Do you currently provide reinsurance for cyber risk



6.0 Concluding thoughts

When we first conceived the idea of a survey exploring the (Re)insurance industry's preparedness for Cyber Risk, little did we realise just how timely this would prove to be. As we sat around a boardroom table in our new EC3 offices over the Summer, discussing with our friends at Insurance Day how best to investigate attitudes and capture opinion on the new demands for cyber cover, the latest headlines on high profile data breaches - at TalkTalk and Morrisons - had yet to break. And the Office for National Statistics had not yet made public its decision to include cyber as a separate category in the annual crime figures for the first time, as the very nature of crime itself is deemed to have changed.

Before long my colleagues and I found ourselves hauled into the centre of a very public debate about cyber risk and the law - at one point fielding questions from businesses and consumers live on national TV and radio following the TalkTalk breach. Their concerns told an interesting story: the public's belated appreciation of the value of their personal information and its attraction to criminals; the lack of consistency in protections employed by businesses against the risk of theft, loss or destruction of personal data; and an absence of specificity within the current legal framework as to standards of protection that businesses are required to have in place.

What we said then, we hold to now: the real lesson about these high profile stories, is less about what one individual company may have done wrong, and more about how these issues affect every business - indeed including the businesses of insurers themselves. Of course it's the cyber attacks on household consumer brands that will always grab headlines, so data breach is what we read about most in the newspapers. But this is by no means the only cyber threat to which businesses and their insurers need to be alert. What these stories really show is just how easy it is for computer systems anywhere to be hacked. The threat is all-pervasive. Ubiquitous even. And in turn that means losses arising from cyber related incidents are potentially capable of attaching to the full spectrum of insurance covers currently available, not just cyber-specific policies.

At the time of writing, news is just breaking that 14 other high street names have been subject to cyber attacks since TalkTalk's in October. The likes of Amazon, BBC Sport, Halifax, Sky TV, O2, TicketMaster, Uber, Visa, Vodafone - even sandwich chain Subway – have all been implicated, to name just a few. By the time you are reading this, who knows how many more headlines will have made even this copy out of date. The picture is moving fast and businesses – and their insurers – need to catch up. We hope this report at least helps you put the central issues in focus.

Ed Lewis
Partner
Weightmans LLP
ed.lewis@weightmans.com

Weightmans

Meet the team

Kieran Jones
Partner, Insurance Director
DD: 0151 242 7967
kieran.jones@weightmans.com

Mike Grant
Head of Professional Risk
DD: 0151 242 7956
mike.grant@weightmans.com

Ed Lewis
Partner
DD: 020 7882 1992
ed.lewis@weightmans.com

Ling Ong
Partner
DD: 020 7822 1985
ling.ong@weightmans.com

Colin Peck
Partner
DD: 020 7822 1984
colin.peck@weightmans.com

James Denison
Associate
DD: 020 7822 1943
james.denison@weightmans.com

Robert Crossingham
Partner
DD: 0207 822 1991
robert.crossingham@weightmans.

Ian Lavelle
Associate
DD: 0776 162 5139
ian.lavelle@weightmans.com

Weightmans

weightmans.com