RACONTEUR

Mitigating Cyber Risk

JLT

JLT Specialty provides insurance broking, risk management and claims consulting services. Our success comes from focusing on sectors where we know we can make the greatest difference – using insight, intelligence and imagination to provide expert advice and robust, often unique, solutions.

www.jltspecialty.com

RACONTEUR

Publication sponsored by

Publisher Reuben Howard
Project manager Tom Andrews
Editorial consultant Gren Manuel
Editor Lindsay O'Hagan
Design Sara Gelfgren, Harry Lewis-Irlam
Head of production Justyna O'Connell
Digital marketing manager Elise Ngobi

Contributors

Gerrard Cowan
Writes about business issues including defence and cybersecurity. He was formerly a news editor at the *Wall Street Journal* and European editor of *Jane's Defence Weekly*.

Oliver Pickup
Multi-award-winning journalist who has written for publications including *The Times, Telegraph, Guardian*, and *FT Weekend*.

Ben Rossi
Formerly editor of *Information Age* and *Computer News Middle East*, he writes for national newspapers and business publications.

Sarah Stephens
Senior partner and Head of cyber at JLT Specialty in London.

Contents

Cyber insurance, once considered complex and unnecessary, has moved to the mainstream. This report explores how the market is evolving and why it is becoming an essential tool for large companies seeking to manage their exposure to digital threats.

04

In dangerous times, cyber insurance comes of age

06

Think your insurance covers cyber incidents? Think again...

09

Looking for the weak link in the chain

11

Five questions the C-suite needs to ask

13

When off-the-peg just won't fit

In dangerous times, cyber insurance comes of age

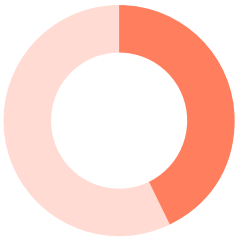
Once considered exotic and complex, cyber insurance is now an essential tool for large companies seeking to manage risk

OLIVER PICKUP

It is inevitable that every organisation, large and small, will suffer a data breach – and sooner rather than later in all probability. Indeed, all the companies that constitute America's Fortune 500 have been hacked, according to Mikko Hyppönen of F-Secure, a leading cybersecurity business. Closer to home, an estimated 43 per cent of UK companies were attacked or breached in 12 months, a government study published earlier in 2018 showed.

Since then the Europe Union's General Data Protection Regulation (which can fine organisations up to 4 per cent of annual global turnover) has come in to force, triggering a rush by C-suite executives to insist on adequate cyber insurance to mitigate or transfer this sizeable and multi-dimensional risk.

Cyber insurance has evolved quickly in the past few years and is no longer deemed exotic or over-complicated. "In the last five years we have seen the market adapt to the current climate," says Tom Huckle, a cybersecurity consultant and head of training and development at Crucial Group.



43%

of UK companies attacked or breached in 12 months

UK government/IPSOS Mori/University of Portsmouth study, 2018

"Cyber insurance is worth it. Despite adhering to every current best practice or investing in security hardware, if someone nefarious is desperate to hack you then they probably will, to some extent. The skill is in choosing the right coverage for your business, as the devil will be in the detail.

"With new regulations coming into force and the Internet of Things creeping into everyone's lives, it only increases the demand for people and businesses to take out cyber insurance."

Even a decade ago, the insurance industry had no way of predicting how cyber insurance would develop as a class. As of 2018, global cyber insurance premiums amount to $4.52 billion (£3.5 billion), calculates Orbis Research. And this figure is expected to quadruple to $17.55 billion in 2023.

A 2018 report for the UK government found that just 24 per cent of large businesses had specific cyber insurance policies. Many business leaders interviewed for the survey seem to have outdated views of the cyber insurance market, with the report saying "half of firm leaders we spoke to do not realise that cyber risks can even be insured."

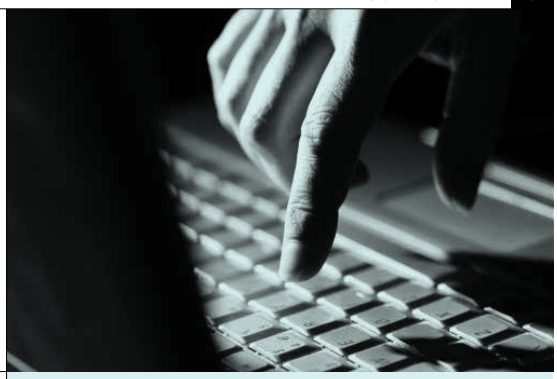
While cyber insurance has become more comprehensive and transparent, there is clearly room for a greater understanding, particularly around two key issues: the hidden risk posed by "silent cyber" and the potential damage of a low-probability, high-impact event sometimes dubbed a "cyber hurricane".

The former is, in simple terms, where an element of cyber insurance coverage is being provided unknowingly and unintentionally as part of a policy designed to cover other exposures.

As for the latter, in the same way that a natural disaster can lead to property insurers being challenged with thousands of claims from a single cause, a cyber hurricane would be exorbitantly costly.

"With more businesses connected to cloud servers and just a handful of service providers dominating approximately 80 per cent of the market, imagine if those servers were taken down," says Mr Huckle of a cyber hurricane. "It could affect up to 12.4 million businesses, who could be out of action for any length of time."

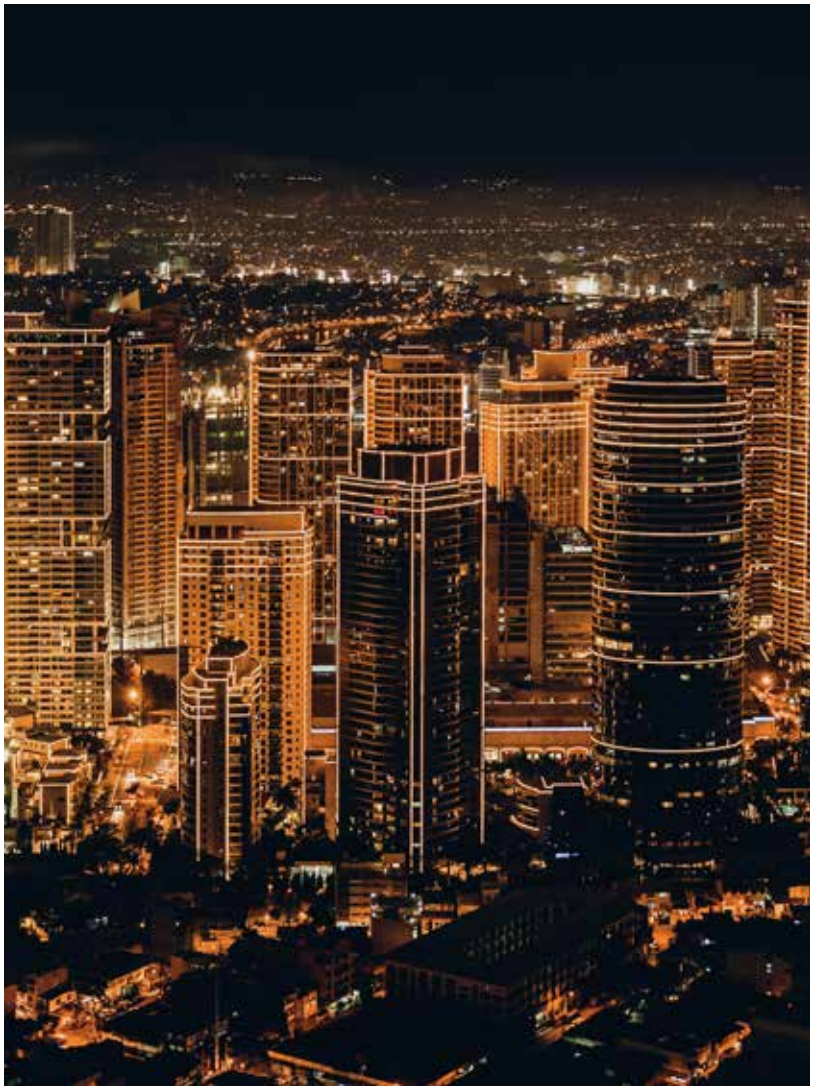
Nik Whitfield, chief executive of London-based cyber risk software company Panaseer, urges insurers to evolve their processes and embrace data to provide adequate cover and pricing. At present insurers typically assess risk using questionnaires and



> **It is crucial that organisations do not look at cyber insurance as a silver bullet of protection**
>
> Nik Whitfield, Panaseer

other self-reported data, augmented with metrics from data providers. They usually won't directly analyse a firm's network or its data logs that may show, for instance, the severity of attacks it experiences.

Mr Whitfield says: "Unfortunately this is a very limited approach, akin to doctors evaluating patients without the benefit of x-rays, blood tests, MRI scans, and so on." He says direct data analysis could reveal insights in the same way that telematics is creating new insights into car insurance, creating "a far better evaluation of the enterprise's cyber hygiene and therefore risk position of the insured."



NotPetya damage leaves businesses with $10 billion bill

The world's most devastating cyber attack so far is arguably the NotPetya malware, which ripped through the internet in June 2017. The US government, pointing the finger of blame at the Russian military, called it "the most destructive and costly cyber attack in history". A White House assessment, reported by *Wired*, said the total damages would exceed $10 billion.

NotPetya caught nation states and leading businesses off-guard, and a raft of organisations – many without the requisite cyber insurance – were financially wounded.

"NotPetya is the most striking example, as the cyber attack is estimated to have inflicted nine-digit losses on many multinational companies," says Tim Smith, head of cyber and a partner at BLM, an insurance and dispute resolution law firm.

Pharmaceutical giant Merck was dented by a $460 million sales reduction, plus a further $355 million in additional expenses. Global courier service FedEx suffered $400 million in lost earnings, and was forced to halt shipping temporarily. Numerous other organisations incurred enormous losses as a direct result of the ransomware, including Maersk ($250-$300 million), Saint-Gobain ($220-$250 million) and Reckitt Benckiser ($114 million).

"It's important that organisations don't look to the NotPetya example as the norm," warns Piers Wilson, head of product development at cybersecurity organisation Huntsman. "If the same attack were to hit small to medium-sized enterprises who weren't covered by cyber insurance, many of them would likely be crippled and could even be forced to close their doors in the face of mounting costs, fines and loss of customer confidence."

Think your insurance covers cyber incidents? Think again...

Misconceptions about cyber insurance are widespread but business leaders must make sure their firms have the right cover

SARAH STEPHENS
SENIOR PARTNER AND HEAD OF CYBER, JLT SPECIALTY

No organisation in the world is 100 per cent secure from cyber attacks, and it follows that to mitigate the growing risk business leaders must ensure they have suitable cyber insurance.

87%

of global companies not yet funding cyber resilience to their desired levels

65%

of global companies will boost cybersecurity budgets in the next 12 months

EY survey, 2018

Although open and collaborative conversations about cybersecurity have matured at boardroom level in recent years, at JLT Specialty we observe a lack of understanding when it comes to cyber insurance – and this is why we take a measured approach, guiding our clients through a clear process that also helps educate the C-suite in this constantly evolving area.

In addition to becoming more knowledgeable about this hugely important subject, a mindset shift is required from business leaders. Traditionally, we insure what we can see and touch, and even today many on the C-level believe that their organisation is adequately protected against cyber attacks and/or data breaches when that is not always the case.

There are widespread misconceptions about what cyber insurance is, what it covers, and whether it is required. Indeed, at least half of the client meetings my team attend are on the topic of what cyber risks are covered under their current insurance, and there are plenty of 'aha' moments.

While there is more board-level awareness of cyber risk, the C-suite must start demanding confirmation that it is addressed adequately in the organisation's existing insurance arrangements, in the same way that tangible risks are. The attitude that "we buy all the normal insurances that companies like us buy, so we are fine" is not enough.

The number one reason business leaders don't take out cyber insurance is because they believe they will not be affected. They think: "We aren't a bank, so there is no cyber risk. Also, we outsource services, so that transfers our risk to someone else." Moving beyond this dangerous approach is vital. For one thing, a majority of recent breaches in the news have been caused through third parties, so thinking that the supply chain is safe, or not your responsibility, can be a fatal business mistake.

The C-suite needs to realise the potential short- and long-term impact cyber risks can have. What would it mean not to have email for days, or if there was no access to the business-critical system that deals with transactions? Moreover, what if all the data in that system was compromised? The knock-on effect on the business, including reputational damage, has to be taken into account.

The second barrier to adequate cyber insurance is the applicability challenge, the belief that "the cyber insurance that exists in the market now is not right for me". Business leaders sometimes think that these policies are mostly bought by financial institutions, which implies they are not appropriate for their own organisation and industry. They may also believe that they do not need insurance because they do not hold large quantities of personal data. For reasons like these almost all the companies that meet my team insist at first that the market can not meet their needs.

However, when we sit down and go through what clients want and need, around 90 per cent of the issues that cause concern can be covered, often by careful tailoring of policies. Of the remaining one in ten, many of these risks will one day soon be insurable as the market rapidly evolves. Much of the disconnect in perception

> **Companies have been denied coverage for cyber claims because they have taken out a general, non-cyber policy**

about what the market can offer arises when clients have not worked with a capable cyber broker who can show them the full art of the possible.

The third hurdle they must overcome is the opinion that, because the cyber insurance market is so new and cyber underwriters don't know what they are doing, cyber insurers can't possibly pay out all their claims without collapsing. Even though cyber insurance is relatively new to the C-suite, it has been evolving for decades. Furthermore, it uses the same principles and methodologies applied in other forms of insurance.

One of the reasons that some people have in their heads that cyber insurance companies don't pay claims is the unhelpful and misleading headlines in the media. If you dig a little deeper, though, companies have been denied coverage for cyber claims because they have taken out a general, non-cyber policy. There are so many examples of this in the press, but the reality behind the headlines is that they have been trying to fit a square peg into a round hole with no proper cyber insurance and have been caught out.

5x

growth projection for global cyber insurance premiums from 2018 to 2025

Munich Re

Given that big corporates are struggling to deal with cyber risk, it is unsurprising that smaller companies are way off the pace of change. Small companies do have one advantage in that they are not weighed down by legacy computer systems prone to disruption and attack. It is essential for organisations of all sizes to have cyber insurance, as hackers target system vulnerabilities regardless of company size.

The cyber insurance market may be relatively young, but it is growing quickly. At JLT we take a measured approach and believe that the process should be as clear and straightforward as possible. That way, more of the C-suite will understand the expanding and wide-reaching nature of cyber risk, and mitigate it.

“Hackers target system vulnerabilities regardless of company size

Looking for the weak link in the chain

Outsourcing to the cloud and elsewhere creates new risks that can be uncovered during the insurance process

GERRARD COWAN

Mitigating risks from outsourcers and suppliers is a key focus of cyber insurance. However, the process of acquiring that insurance could also offer practical benefits, helping identify potential dangers in the supply chain.

It is increasingly difficult for companies "to build an information security fortress", says Jimaan Sane, an underwriter at Beazley, a specialist insurer focused on the cyber market. Because of the way companies interact with their suppliers – as well as consumers and employees – they must allow access to their systems to varying degrees, depending on the individual user or the nature of the data. This raises the importance of robust due diligence, "because if you allow access to your systems and networks to a third party provider whose level of security is lower than your own, they become the weakest link in the chain".

However, it is not enough to rely on information security standards like ISO 27001, says Mr Sane. Security is about culture: reviewing and testing processes and procedures, and constantly ensuring that appropriate security measures and employee training are in place. The ultimate responsibility here lies with the company, but it can be supported through the process of acquiring insurance, Mr Sane says, as insurers go through risk information and ask questions or benchmark against industry standards, which in some cases can help highlight weaknesses.

Cloud computing: a concentrated risk?

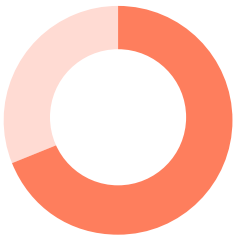
Many companies now rely on the cloud for essential services. With the market dominated by a handful of suppliers, how would insurers fare if one of these giants suffered a cyber breach?

The broad issue was highlighted in a January report from Lloyd's of London: Cloud Down – The impacts on the US economy. This found that an extreme cyber incident that takes a top cloud provider in the US offline for three to six days would result in economic losses of $15 billion, and up to $3 billion in insured losses. Businesses outside the Fortune 1000 are at the highest risk, the report stated, with this group carrying 63 per cent of economic losses and 57 per cent of insured losses.

The dominance of a small number of providers creates a trade-off, says Beazley's Jimaan Sane. On the one hand, clusters of clients in a portfolio are likely to rely on an individual provider: if that provider suffers a failure or a breach, the insurer could face multiple claims related to loss of data or an inability to trade, for example. On the other hand, the more that companies depend on the services of a Google or an Amazon, the more their security will increase on a day-to-day basis, given the high standards at such providers.

"You're probably trading frequency – because individual levels of security are higher – for severity, because if one provider goes down you'll have multiple clients having issues at the same time."

Insurers are well aware of the issue, Mr Sane says, and each knows the payouts it would face if the worst were to occur. However, because the market is relatively young, it will take time before enough data is available to understand what a severe incident could mean in terms of long-term damage, he says.



69%

of executives cite data security as a top concern when moving to the cloud

Deloitte Global Outsourcing Survey 2018

The insurer will conduct a "mini-audit" or "request for information" focused on "getting a sense of where the risks are and what they're doing to mitigate them". The answers will inform the type of cover an insurer like Beazley will offer and the terms and conditions attached, and will change in complexity depending on the size of the client. However, the ultimate goal is the same, Mr Sane says: "The insurer and the company will get a sense of where their risks lie, and what they're doing to mitigate those risks."

Most insurance policies cover the risk from the technology supply chain as standard, says Laila Khudairi, cyber divisional head of enterprise risk at Tokio Marine Kiln, an insurer. This works on two levels, she says. First, there is the danger to data. A company has responsibility for its customers' data, "even if it is hosted on an outsourced provider's platform", or if it is passed to a supplier through day-to-day business. Second, cyber policies cover business interruptions that could be caused by an outage of their own system or an outsourcer (for example, a cloud provider).

Companies are growing more aware of the risks from outsourcers and suppliers, says Scott Kannry, chief executive of Axio, which helps clients quantify their cyber risks through a variety of models, methodologies and other tools. Axio is increasingly helping its customers assess their supply chains, including their insurance provisions.

"We look at the supply chain and ask, 'if there's an event, what could the impact on the business be?'"

It is crucial that insurance policies cover outsourcers, and that companies focus on their suppliers, because that is simply the way business is evolving, says Mr Sane.

"Most companies tend to outsource things where they can – that's the way the world is going."

> **"We look at the supply chain and ask, 'if there's an event, what could the impact on the business be?**
>
> Scott Kannry, Axio

What the C-suite needs to ask about cybersecurity

The issue is now too important to delegate. Time to ask these tough questions

OLIVER PICKUP

1

What is our risk from cyber attack, and how can we reduce this?

"Organisations can never be 100 per cent secure, but they can be 100 per cent sure of their position," says Nik Whitfield, chief executive of London-based cyber risk software organisation Panaseer. "With that in mind, this is the first question the board must direct to their security team. By being clear on the risks, the conversation can then move on to the cybersecurity insurance policy, for which the C-suite must ask for clear details on the scope and specifics, so that they can make sure that they are adhering to the policy in place and that it protects them from any damaging cyber events."

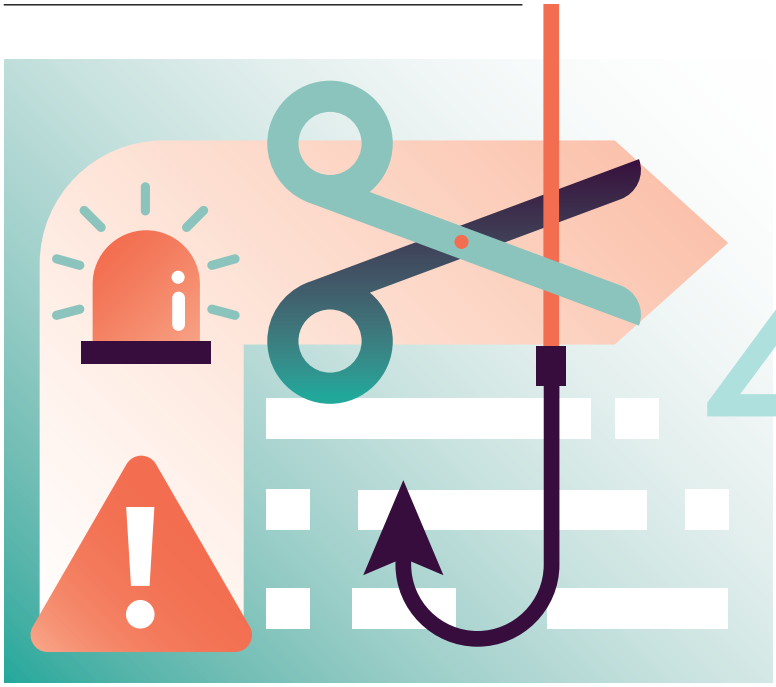
2

Does our organisation's cyber insurance policy cover us adequately and are our cover limits structured in the right way?

Much media coverage of cyber insurance focuses on how companies with catastrophic losses have failed to recoup them from their insurer, which implies that policies fail in the hour of greatest need. The reality is more prosaic: the company, most likely, was underinsured with a low ceiling on damages. Deborah Chang, vice-president of business development and public policy at bug bounty platform HackerOne, says that when boards grill the chief information security officer (CISO), or chief technology officer (CTO) about new risks, these answers should inform not only the technical response but also discussions about cover. "Companies should talk to an insurance broker to determine what the best coverage is for them."

What might invalidate a cyber insurance claim?

"Companies taking out cyber insurance need to know what they are talking about and to be able to answer questions accurately from the insurer about their risk profile, security infrastructure, and policies and processes," says Mark Taylor, managing consultant at NTT Security. "Inaccurate information can void a policy, with claims denied because information provided is inaccurate. Our Risk:Value 2018 report reveals that many business leaders are unaware of what might invalidate their insurance. Half of respondents admit that a failure to maintain or apply updates to existing IT systems could invalidate an insurance policy; 38 per cent point to the lack of an incident response plan, and 37 per cent believe that lack of compliance with regulations, including GDPR, could affect a claim."



How do we defend our organisation against phishing attacks?

"Many cyber attacks experienced by business are very basic in their nature, and not the advanced threats from major nation states that the media tends to depict as the main risk," says Graeme Newman, chief innovation officer at CFC Underwriting. He believes good company-wide cyber hygiene is essential, and in the boardroom this topic must be addressed – and regularly. "Rather than asking about specific point-in-time security measures, boards need to ensure there is a structured IT security program in place that follows an established framework."

How would a cyber attack impact on the way we do business, and how much might it cost?

"If your organisation is breached, can it still trade without a website or access to other systems?" asks Sarah Adams, a cyber risk specialist at insurance intermediary PolicyBee. She says research by insurance group Hiscox estimates that the average cost of an attack for smaller businesses is around £26,000. "Can you survive without email? Do you take payments online? Do you hold particularly sensitive customer data or images? What will be the consequences for both you and your customers if you're hacked or held to ransom?"

When off-the-peg just won't fit

Variations in exposure and risk profile mean that large firms need a customised approach to cyber insurance

BEN ROSSI

As the threat of cyber attacks and data breaches continues to grow, insurers have honed their cyber policies, and brokers are putting cyber nearer the top of the agenda when reviewing an organisation's risk profile.

However, just engaging an insurance broker doesn't guarantee access to effective and competitive coverage. The threat landscape is changing at a fast pace, leaving many brokers with insufficient knowledge of the impact a successful cyber attack could have. Meanwhile, insurers still lack an industry-standard approach to cyber policies.

Risk typically varies by industry, making some types of coverage more relevant than others. "There are a lot of brokers that just sell generic, off-the-shelf policies with seven or eight different types of basic cover," says Andrew Lewis, cyber lead underwriter at Hiscox London Market. "But if you have a business with high privacy risk then there will be parts of a policy that are more relevant than if you're a manufacturer and business interruption exposure is significant."

Off-the-shelf policies can also be vague and many insurers and brokers lack experience in this area. Businesses should, therefore, carefully evaluate whether they can identify exposure that is specific to them.

While smaller companies can often find adequate coverage in off-the-shelf offerings, the absence of an industry standard means larger organisations must seek customisation. Research on the major risks they face is vital.

"It's extremely important that mid-sized and large businesses evaluate where they think their exposure is," says Mr Lewis. "The really good brokers will work with clients before they come to market to understand their exposure and focus on perhaps two or three things that are really important to them. The cover is then tailored to deal with that."

Credit reporting agency Equifax expects costs relating to its mammoth data breach last year to total at least $439 million. That doesn't account for the $5 billion that was erased from its market capitalisation in the aftermath of the breach, yet the company bought a policy with a maximum payout of just $125 million.

Incidents of this kind are still rare, so it is challenging for insurers to assess the potential scope and damage of a cyber attack. This will become easier as the market evolves and more data becomes available but, until then, claims assessors are attempting to conduct scenario modelling of the cyber threats a firm faces.

"This is a complicated area but well worth the effort," says Steven Nock, partner at Harris Balcombe, an insurance assessor that offers this service. "Often it identifies areas of risk that would otherwise have been overlooked."

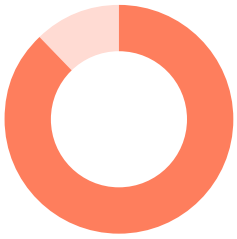
However, Francisco Sanches, director of IT internal audit at accountancy firm Mazars, cautions: "Insurers will be able to improve their predictive models, but the cyber world is surrounded by high uncertainty and disruptive events still happen frequently."

> **"Businesses need to understand what their specific policy covers**
>
> Steven Nock, Harris Balcombe

What is often neglected, yet is arguably more harmful than financial losses to an organisation that suffers a high-profile data breach, is the impact on its reputation. This kind of damage is almost impossible to quantify accurately, but some policies attempt to offer cover for it and demand is likely to grow as insurers are able to draw more insights from companies that have experienced it.

Such damage is typically addressed by paying for PR experts to minimise the impact on a company's reputation or for promotional activity that restores favourable views towards the business. "This is quite different to quantifying and indemnifying for resultant loss of profit that may flow from reputational damage," says Mr Nock. "Businesses need to understand what their specific policy covers."

As cyber threats continue to evolve at a rapid pace, insurers face the task of staying abreast of the latest attack mechanisms while maturing their approach to offering cyber policies. Cyber is racing towards being a mainstream business threat more quickly than directors can understand how to protect their organisation from possible losses. It falls to insurers and brokers to fill this critical knowledge void.



88%

of FTSE 350 companies are increasing spending to mitigate cyber risks

FT/ICSA survey, August 2018

Hidden under the hood

Specialist cyber underwriters determine whether companies are taking security seriously during their risk assessment and actuarial process. If a cyber policy is being sought to insure the poor state of an organisation's security, insurers may offer to help with risk reduction. "It makes real sense to use this service as it will help substantiate any future claim," says Ken Munro, partner at Pen Test Partners, which does penetration testing of IT systems.

While small and medium-sized firms are typically receptive to these offers, many large companies decline. Bigger organisations are naturally more likely to have IT security and response teams to deal with risk, although there may be other reasons at play.

"There is probably some notion that they don't want their insurers knowing what's going on under the hood for fear of increased premiums or declination of coverage," says Chris Bayley, co-founder and head of new products at insurtech firm Cover Genius.

RACONTEUR