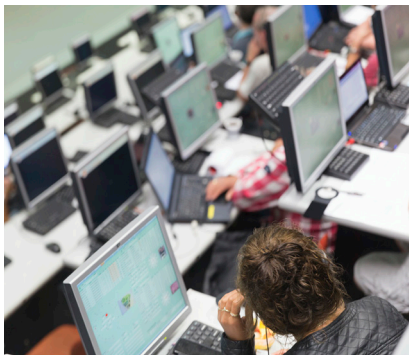
Fast growing demand for cyber insurance offers a huge commercial opportunity for insurers and reinsurers, but could also expose the industry to potentially devastating losses. How can your business develop the risk evaluation, risk pricing and risk transfer structures and capabilities to put cyber insurance on a sustainable footing?

Insurance 2020 & beyond: Reaping the dividends of cyber resilience



pwc

www.pwc.com/insurance

Contents

Introduction: Worth the risk?

Welcome to 'Reaping the dividends' of cyber resilience, the latest viewpoint in PwC's Insurance 2020 and beyond series.[1]

Cyber insurance is a potentially huge, but still largely untapped, opportunity for insurers and reinsurers. We estimate that annual gross written premiums are set to increase from around $2.5 billion[2] today to reach $7.5 billion[3] by the end of the decade.

Businesses across all sectors are beginning to recognise the importance of cyber insurance in today's increasingly complex and high risk digital landscape. In turn, many insurers and reinsurers are looking to take advantage of what they see as a rare opportunity to secure high margins in an otherwise soft market. Yet many others are still wary of cyber risk. How long can they remain on the sidelines? Cyber insurance could soon become a client expectation and insurers that are unwilling to embrace it risk losing out on other business opportunities if cyber products don't form part of their offering.

In the meantime, many insurers face considerable cyber exposures within their technology, errors & omissions, general liability and other existing business lines. The immediate priority is to evaluate and manage these 'buried' exposures.

Critical exposures

So why is there so much scepticism over cyber insurance? Part of the challenge is that cyber risk isn't like any other risk insurers and reinsurers have ever had to underwrite. There is limited publicly available data on the scale and financial impact of attacks. The difficulties created by the minimal data are heightened by the speed with which the threats are evolving and proliferating. While underwriters can estimate the likely cost of systems remediation with reasonable certainty, there simply isn't enough historical data to gauge further losses resulting from brand impairment or compensation to customers, suppliers and other stakeholders (as we explore later, new scenario-based techniques are needed). A UK Government report estimates that the insurance industry's global cyber risk exposure is already in the region of £100 billion[4] ($150 billion), more than a third of the Centre for Strategic and International Studies' estimate of the annual losses from cyber attacks ($400 billion)[5]. And while the scale of the potential losses is on a par with natural catastrophes, incidents are much more frequent. As a result, there are growing concerns about both the concentrations of cyber risk and the ability of less experienced insurers to withstand what could become a fast sequence of high loss events.

1 www.pwc.com/insurance/future-of-insurance and www.pwc.com/projectblue

2 Speech by John Nelson, Lloyd's Chairman, at the AAMGA, 28 May 2015 (https://www.lloyds.com/lloyds/press-centre/speeches/2015/05/vision-2025-and-aamga)'

3 PwC estimate (see page 10)

4 'UK Cybersecurity: The role of insurance in managing and mitigating the risk', UK Government, March 2015

5 'Net Losses: Estimating the Global Cost of Cybercrime', Centre for Strategic and International Studies, June 2014. The report estimates that the annual losses are between a "conservative estimate" of $375 billion and a "maximum" of $575 billion, giving a "likely" estimate of "more than $400 billion".

"…while the underwriting of cyber risks provides opportunities for Lloyd's syndicates, Lloyd's is concerned that without proper controls there exists a material risk of a dangerous aggregation of exposure in the market. Lloyd's is also concerned that cyber risk may not be being properly priced for, nor the exposures adequately quantified by managing agents".

Tom Bolt, Director, Performance Management, Lloyd's[6]

Insurers and reinsurers are charging high prices for cyber insurance relative to other types of liability coverage to cushion some of the uncertainty. They are also seeking to put a ceiling on their potential losses through restrictive limits, exclusions and conditions. However, many clients are starting to question the real value these policies offer, which may restrict market growth.

Sustainable footing

In this paper, we look at how cyber insurance could be a more sustainable venture that offers real protection for clients, while safeguarding insurers and reinsurers against damaging losses.

This includes more rigorous and relevant risk evaluation built around more reliable data, more effective scenario analysis and partnerships with government, technology companies and specialist firms. Rather than simply relying on blanket policy restrictions to control exposures, insurers would make coverage conditional on regular risk assessments of the client's operations and the actions they take in response to the issues identified in these regular reviews. The depth of the assessment would reflect the risks within the client's industry sector and the coverage limits.

This more informed approach would enable your business to reduce uncertain exposures while offering the types of coverage and more attractive premium rates clients want. Your clients would, in turn, benefit from more transparent and cost-effective coverage. As you look at how to strengthen balance sheet protection, we also discuss the options for more effective risk transfer built around a hybrid of traditional reinsurance and capital market structures.

Finally, we look at how your business could strengthen your own security in relation to cyber risk. Insurers hold considerable amounts of sensitive client data, so effective safeguards are essential in sustaining credibility in the cyber risk market and trust in the enterprise as a whole.

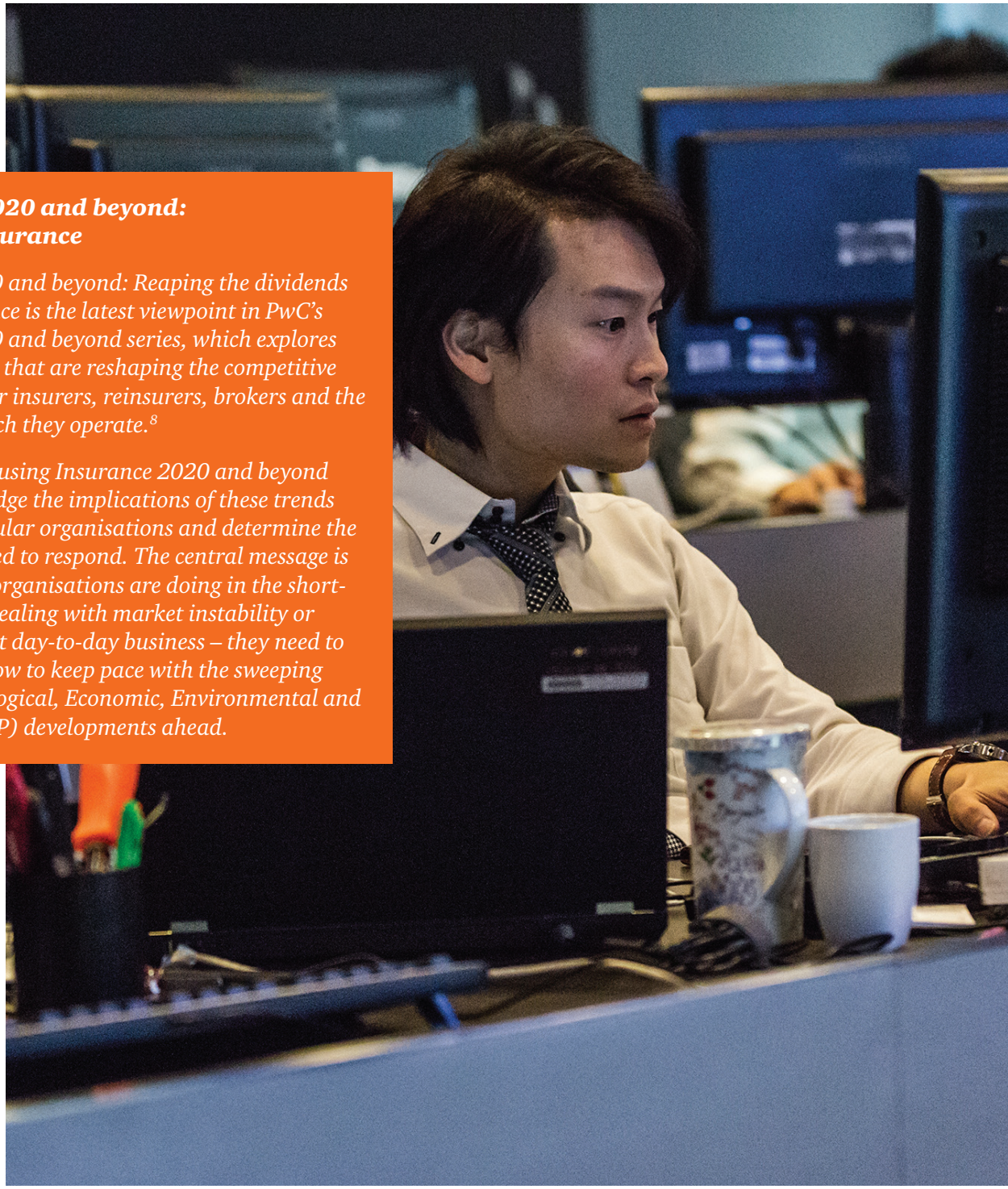
Cutting across this more sustainable approach is a holistic view of cyber risk, which looks at culture, people and processes, as well as technology. We call this cyber resilience.

If you have any queries or would like to discuss any of the issues in this paper in more detail, please speak to your usual PwC representative or one of the authors listed on page 18.

Number 1 risk: Non-life insurers taking part in the latest Banana Skins survey ranked cyber risk as the biggest risk facing their businesses.[7]

6 Lloyd's Market Bulletin, 25 November 2014

7 806 industry participants from 54 countries were interviewed for Insurance Banana Skins 2015, a unique survey of the risks facing the industry, which was produced by the Centre for the Study of Financial Innovation (CSFI) in association with PwC (http://www.pwc.com/insurancebananaskins)



Insurance 2020 and beyond: Future of insurance

Insurance 2020 and beyond: Reaping the dividends of cyber resilience is the latest viewpoint in PwC's Insurance 2020 and beyond series, which explores the megatrends that are reshaping the competitive environment for insurers, reinsurers, brokers and the markets in which they operate.[8]

Our clients are using Insurance 2020 and beyond to help them judge the implications of these trends for their particular organisations and determine the strategies needed to respond. The central message is that whatever organisations are doing in the short-term – be this dealing with market instability or just going about day-to-day business – they need to be looking at how to keep pace with the sweeping Social, Technological, Economic, Environmental and Political (STEEP) developments ahead.

8 www.pwc.com/insurance/future-of-insurance and www.pwc.com/projectblue

1

Cyber vulnerabilities: A risk like no other

The challenges presented by cyber risk defy traditional risk evaluation, pricing and management.

The digital revolution has created a highly interconnected world that is awash with data, much of it sensitive, and much of it vulnerable to fraud, theft and compromise. Add to that malware, denial of service and other malicious attacks, and cyber risk emerges as one of the biggest threats of our age.

Cyber criminals are constantly probing for weaknesses and adapting their tactics. And while our image of the perpetrators often centres on activists or organised gangs, they could just as easily be employees. The targets are also broadening. A clear example came from the insurance sector itself when a company was hacked for the tracking data they held on cargo shipments.

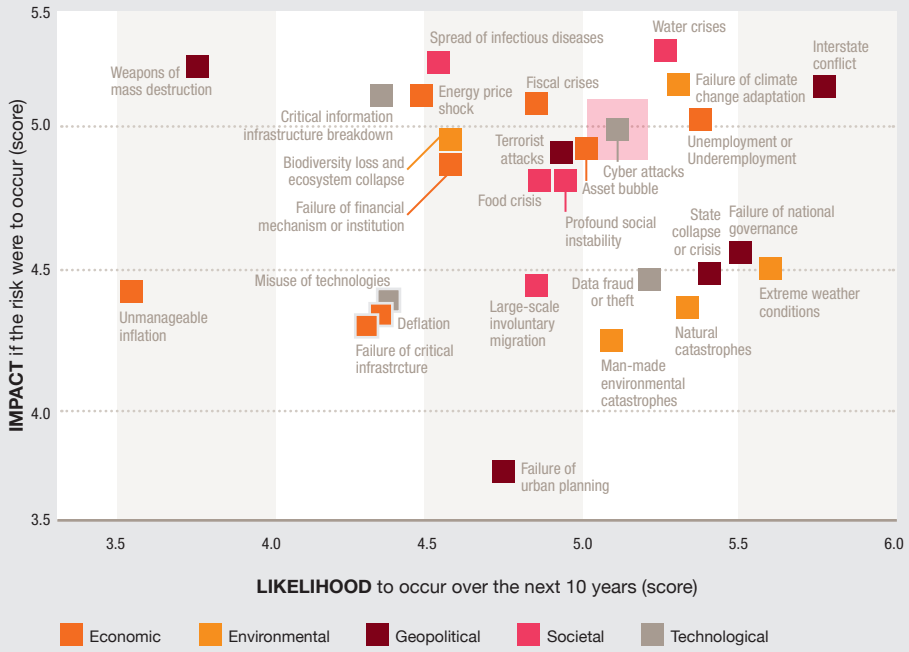
All these factors make cyber crime a costly, hard to detect and difficult to combat threat. From an insurance perspective, while analogies are often made with terrorism or catastrophe risks, cyber risk is, in many ways, a risk like no other.

Cyber crime costs the global economy more than $400 billion a year[9] and the costs will continue to grow

9 'Net Losses: Estimating the Global Cost of Cybercrime', Centre for Strategic and International Studies, June 2014. The report estimates that the annual losses are between a "conservative estimate" of $375 billion and a "maximum" of $575 billion, giving a "likely" estimate of "more than $400 billion".

71% of insurance CEOs, 79% of banking CEOs (the highest of any sector) and 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.[10]

Figure 1: Impact and likelihood of global risks



Note: Survey respondents were asked to assess the likelihood and impact of the individual risks on a scale of 1 to 7, 1 representing a risk that is not likely to happen or have impact, and 7 a risk very likely to occur and with massive and devastating impacts.

Source: World Economic Forum 'Global Risks, 10th Edition', 2014

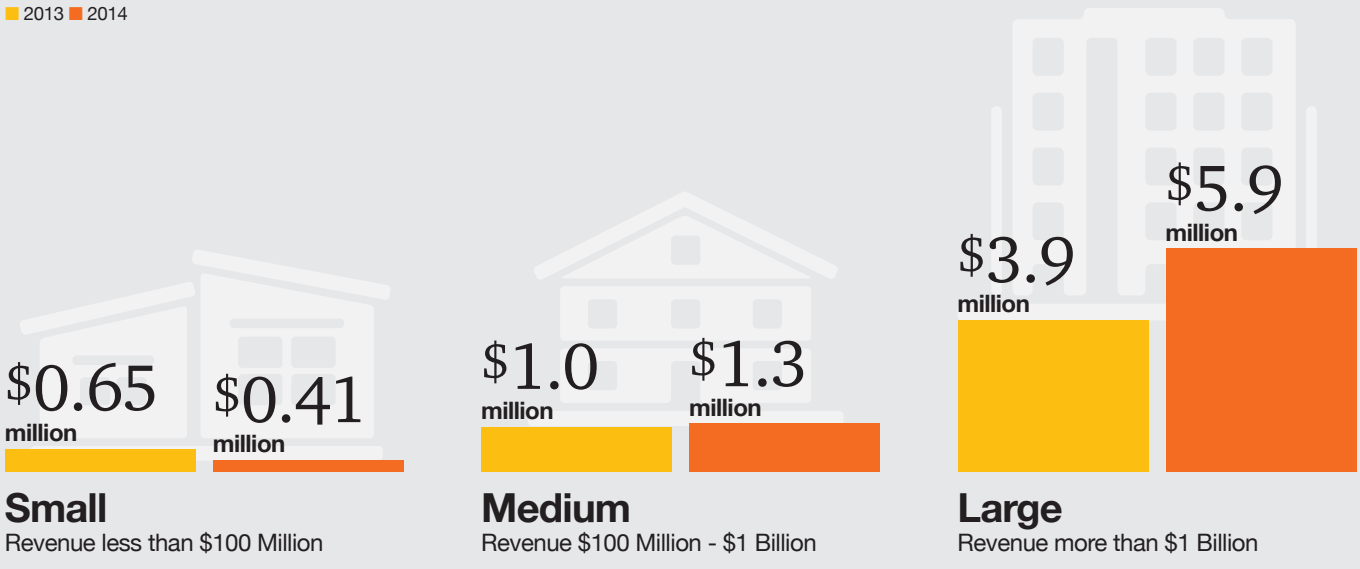
1 Both frequent and severe

As Figure 1 indicates, cyber risks score highly on both impact and likelihood.

Our annual survey of security, IT and business executives shows that there were nearly 43 million global security incidents detected in 2014.[11] This is the equivalent of more than 100,000 attacks a day. The financial impact keeps rising (see Figure 2) and has, in some cases, run into tens of millions of dollars. Insurers could face a rapid succession of severe losses, making it harder to absorb the impact or subsequently rebuild the balance sheet in the same way as following a catastrophe event.

Figure 2: Incidents are more costly for large organisations

Average financial losses due to security incidents, 2013–2014



Source: 'Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015', PwC[11]

2 Loss contagion is hard to contain

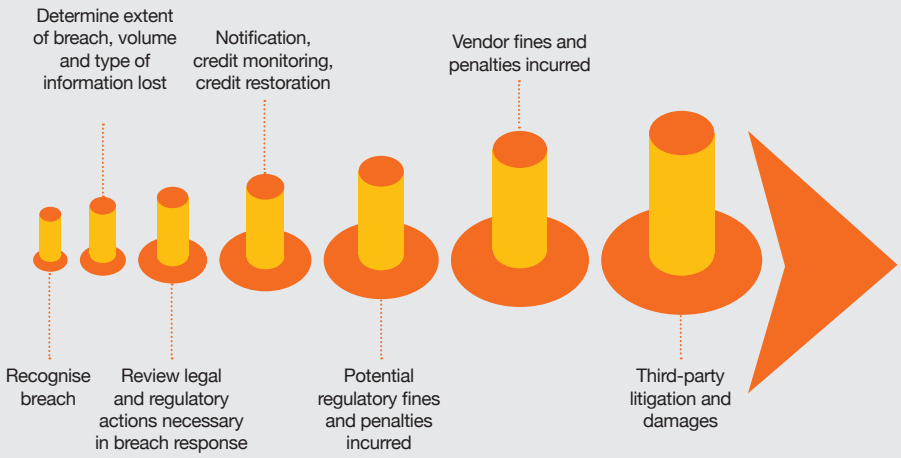
The impact of business interruption and systems remediation is compounded by knock-on losses including fines, litigation and reputational damage. Figure 3 outlines the long and unpredictable fallout from a cyber breach. All businesses operate within an increasingly interconnected and interdependent ecosystem, in which it is not just their own systems and data that are vulnerable, but those of their suppliers, customers and strategic partners. The Internet of Things has heightened the connectivity and associated vulnerability further still.[12] Businesses are also concerned about the threat of attacks on the infrastructure they rely on.

3 Risks are difficult to detect, evaluate and price

There is limited actuarial data on the financial impact of cyber attacks, which makes this a difficult risk to evaluate or price with any precision. While underwriters can estimate the cost of getting IT systems back up and running in the same way as if they were put out of action by fire or flood, there simply isn't enough data to estimate the further losses resulting from brand impairment or compensation payments to customers, suppliers and other stakeholders. The uncertainty is compounded by the fact that cyber security breaches can remain undetected for several months, even years, which opens up the possibility of accumulated and compounded losses down the line.

Even if your business offers no standalone cyber coverage, it needs to gauge the exposures that exist within your wider property, business interruption, general liability and errors & omissions coverage. There may be exclusions that limit the potential for claims (e.g. the need for physical damage to trigger business interruption), but this should be thoroughly checked.

Figure 3: A cyber breach has a long and unpredictable tail



Source: PwC

Insurers are expected to lead

Who will take ultimate responsibility for the management of this growing, uncertain and costly risk?

Boards are coming to realise the need for safeguards against the most damaging cyber attacks. Cyber insurance is one risk transfer option. Yet, while many insurers have eagerly embraced the revenue growth opportunities opened up by cyber insurance products, others believe that this is too big a risk for them to take on. There has also been some talk about whether governments would be prepared to step in as an insurer or reinsurer of last resort, as they have with terrorism and some hard to place flood coverage. However, our own discussions with a number of governments indicate that their preferred solution would be commercial insurance, which would be structured and governed by defined government-set standards. Even where the cyber attacks are state-sponsored, there would be a reluctance to declare this as an act of war and hence invoke certain exclusion clauses.

Your business could choose not to underwrite cyber risks explicitly, but as highlighted earlier, the exposure may already be part of existing policies. As cyber coverage moves into the mainstream, there could also be direct or implicit pressure from longstanding clients or brokers to offer it. Therefore, like it or not, cyber risk coverage would need to form at least some part of your business plans.

10 1322 CEOs interviewed for PwC's 18th Annual Global CEO Survey (www.pwc.com/ceosurvey)

11 'Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015', PwC (http://www.pwc.com/gx/en/consulting-services/information-security-survey)

12 'Insurance 2020 and beyond: Necessity is the mother of reinvention', PwC, 2015 (www.pwc.com/insurance2020reinvention)

2

Cyber insurance market growth: The need for a more sustainable solution

Insurers are relying on tight policy terms and conditions and conservative pricing strategies to limit their cyber risk exposures. But how sustainable is this approach as clients come to question the value of their policies and market bodies begin to express concerns about the level and concentration of cyber risk exposures?

There is no doubt that cyber insurance offers considerable opportunities for revenue growth.

An estimated $2.5 billion in cyber insurance premium was written in 2014.[13] Some 90% of cyber insurance is purchased by US companies,[14] underlining the size of the opportunities for further market expansion worldwide. In the UK, for example, only 2% of companies have standalone cyber insurance.[15] Even in the more penetrated US market, only around a third of companies have some form of cyber coverage.[16] There is also a wide variation in take-up by industry, with only 5% of manufacturing companies in the US holding standalone cyber insurance, compared to around 50% in the healthcare, technology and retail sectors.[17] As recognition of cyber threats increases, take-up of cyber insurance in under-penetrated industries and countries continues to grow, and companies face demands to disclose whether they have cyber coverage (examples include the US Securities and Exchange Commission's disclosure guidance[18]). We estimate that the cyber insurance market could grow to $5 billion in annual premiums by 2018 and at least $7.5 billion by 2020.

There is a strong appetite among underwriters for further expansion in cyber insurance writings, reflecting what would appear to be favourable prices in comparison to other areas of a generally soft market – the cost of cyber insurance relative to the limit purchased is typically three times the cost of cover for more established general liability risks.[19] Part of the reason for the high prices is the still limited number of insurers offering such coverage, though a much bigger reason is the uncertainty around how much to put aside for potential losses.

Many insurers are also setting limits below the levels sought by their clients (the maximum is $500 million, though most large companies have difficulty securing more than $300 million[20]). Insurers may also impose restrictive exclusions and conditions. Some common conditions, such as state-of-the-art data encryption or 100% updated security patch clauses, are difficult for any business to maintain. Given the high cost of coverage, the limits imposed, the tight attaching terms and conditions and the restrictions on whether policyholders can claim, many policyholders are questioning whether their cyber insurance policies are delivering real value. Such misgivings could hold back growth in the short-term. There is also a possibility that overly onerous terms and conditions could invite regulatory action or litigation against insurers.

13 Speech by John Nelson, Lloyd's Chairman, at the AAMGA, 28 May 2015 (https://www.lloyds.com/lloyds/press-centre/speeches/2015/05/vision-2025-and-aamga)'

14 Fortune, 23 January 2015

15 Reuters, 23 March 2015

16 Aon Benfield Insurance Risk Study 2014

17 Willis Insights, March 2014

18 https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

19 'UK Cybersecurity: The role of insurance in managing and mitigating the risk', UK Government, March 2015

20 Financial Times, 18 February 2015

Growing concerns

Even with the limits, conditions and exclusions being used to curtail potential losses, many regulators and market bodies are still concerned about the accumulation and concentration of cyber exposures.

The regulatory response has been particularly prominent in the UK, where many of the biggest cyber underwriters are based. In November 2014, Lloyd's introduced new measures to strengthen the monitoring of risk aggregation and management processes, which will "allow for more targeted interventions, where required".[21] In July 2015, the UK Prudential Regulation Authority (PRA) asked more than 60 insurers to carry out a scenario analysis based on a series of simultaneous cyber attacks on multinationals, leading to data breaches and subsequent class actions.[22]

The clear indication is that regulators could step in to curtail or even stop further cyber insurance policies being written by companies that don't sufficiently understand, or could struggle to withstand, the potential losses.

Losing the cushion

Cyber insurance capacity will continue to increase over the next few years, which is likely to put downward pressure on premium rates and encourage some insurers to relax limits, exclusions and other terms and conditions as they compete for business.

Looking further ahead, the market will eventually reach the data maturity needed to price more accurately and hence reduce the need for a premium cushion. The key questions include how long this will take and whether it could be accelerated. If the industry takes too long, there is a risk that a disruptor could move in and corner the market by aggressively cutting prices or offering much more favourable terms.

21 Lloyd's Market Bulletin, 25 November 2014

22 General Insurance Stress Test 2015

3

Cyber sustainability: Genuine protection at the right price

Capitalising on the cyber risk opportunity, while simultaneously managing the exposures, demands a fresh approach to risk evaluation, risk pricing and risk transfer.

We believe there are eight ways insurers, reinsurers and brokers could put cyber insurance on a more sustainable footing and take advantage of the opportunities for profitable growth:

1 Judging what you could lose and how much you can afford to lose
Pricing will continue to be as much of an art as a science in the absence of robust actuarial data. But it may be possible to develop a much clearer picture of your total maximum loss and match this against your risk appetite and risk tolerances. This could be especially useful in helping your business judge what industries to focus on, when to curtail underwriting and where there may be room for further coverage.

Key inputs include worst-case scenario analysis for your particular portfolio. If your clients include a lot of US power companies, for example, what losses could result from a major attack on the US grid? A recent report based around a "plausible but extreme" scenario in which a sophisticated group of hackers were able to compromise the US electrical grid, estimated that insurance companies would face claims ranging from $21 billion to $71 billion, depending on the size and scope of the attack.[23] What proportion of these claims would your business be liable for? What steps could you take now to mitigate the losses in areas ranging from reducing risk concentrations in your portfolio to working with clients to improve safeguards and crisis planning?

2 Sharpen intelligence
To develop more effective threat and client vulnerability assessments, it will be important to bring in people from technology companies and intelligence agencies. The resulting risk evaluation, screening and pricing process would be a partnership between your existing actuaries and underwriters, focusing on the compensation and other third-party liabilities, and technology experts who would concentrate on the data and systems area. This is akin to the partnership between CRO and CIO teams that are being developed to combat cyber threats within many businesses.

23 'Business Blackout: Emerging risk report 2015', Lloyd's, 7 July 2015

3 Risk-based conditions

Many insurers now impose blanket terms and conditions. A more effective approach would be to make coverage conditional on a fuller and more frequent assessment of the policyholder's vulnerabilities and agreement to follow advised steps. This could include an audit of processes, responsibilities and governance within your client business. It could also include threat intelligence assessments, which would draw on the evaluations of threats to industries and/or particular enterprises, provided by government agencies and other credible sources. It could also include exercises that mimic attacks to test weaknesses and plans for response. As a condition of coverage, you could then specify the implementation of appropriate prevention and detection technologies and procedures.

Your business would benefit from a better understanding and control of the risks you choose to accept, hence lowering exposures, and the ability to offer keener pricing. Clients would in turn be able to secure more effective and cost-efficient insurance protection. These assessments could also help to cement a closer relationship with clients and provide the foundation for fee-based advisory services.

4 Share more data

More effective data sharing is the key to greater pricing accuracy. Client companies have been wary of admitting breaches for reputational reasons, while insurers have been reluctant to share data due to concerns over loss of competitive advantage. However, data breach notification legislation in the US, which is now set to be replicated in the EU, could help increase available data volumes. Some governments and regulators have also launched data sharing initiatives (e.g. MAS in Singapore or the UK's Cyber Security Information Sharing Partnership). Data pooling on operational risk, through ORIC, provides a precedent for more industry-wide sharing.

5 Real-time policy update

Annual renewals and 18 month product development cycles will need to give way to real-time analysis and rolling policy updates. This dynamic approach could be likened to the updates on security software or the approach taken by credit insurers to dynamically manage limits and exposures.

6 Hybrid risk transfer

While the cyber reinsurance market is less developed than its direct counterpart, a better understanding of the evolving threat and maximum loss scenarios could encourage more reinsurance companies to enter the market.

Ready to respond

A bead of sweat rolls down the CEO's forehead as her screen flashes red. An alert warns her that IT sensors have detected the launch of a cyber attack against her company by an organised crime group. The CEO and her team have to quickly work out how to block the attackers, before bracing themselves for the next possible hit. The CEO's mind begins to race. Will the security systems the company implemented keep the criminals at bay? She watches with her executive team as the attackers repeatedly try to penetrate the company's cyber defences. Each attack comes up on the screen as denied. In a last-ditch effort, the criminals attempt to launch ransomware against the company. The CEO and her team quickly reverse-engineer the malware and defeat their adversaries. The CEO exhales and collapses into her chair.

That was just a simulation, but one day it could be real. Such virtual exercises are an increasingly common and effective way to gauge vulnerability and readiness to respond within a business. The simulation exercises we at PwC have developed for use with our clients build the scenarios around the latest threat intelligence assessments for their particular industry or business.[24] The objective is to enable boards to test and strengthen their cyber defence skills, while discovering how the nature and sequence of their decisions make a difference; a difference that could very well be strategically critical. The combination of improved client intelligence and protection would enable insurers to improve their client risk assessments and offer more targeted terms and conditions, while reducing their own exposure to cyber-related losses.

24 PwC Game of Threats http://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.jhtml)

If your business can't protect itself, why should policyholders trust you to protect them?

Risk transfer structures are likely to include traditional excess of loss reinsurance in the lower layers, with capital market structures being developed for peak losses. Possible options might include indemnity or industry loss warranty structures, and/or some form of contingent capital. Such capital market structures could prove appealing to investors looking for diversification and yield. Fund managers and investment banks can bring in expertise from reinsurers and/or technology companies to develop appropriate evaluation techniques.

7 Risk facilitation

Given the ever more complex and uncertain loss drivers surrounding cyber risk, there is a growing need for coordinated risk management solutions that bring together a range of stakeholders, including corporations, insurance/reinsurance companies, capital markets and policymakers. Some form of risk facilitator, possibly the broker, will be needed to bring the parties together and lead the development of effective solutions,[25] including the standards for cyber insurance that many governments are keen to introduce.

8 Build credibility through effective in-house safeguards

The development of effective in-house safeguards is essential in sustaining credibility in the cyber risk market, and trust in the enterprise as a whole. If your business can't protect itself, why should policyholders trust you to protect them?

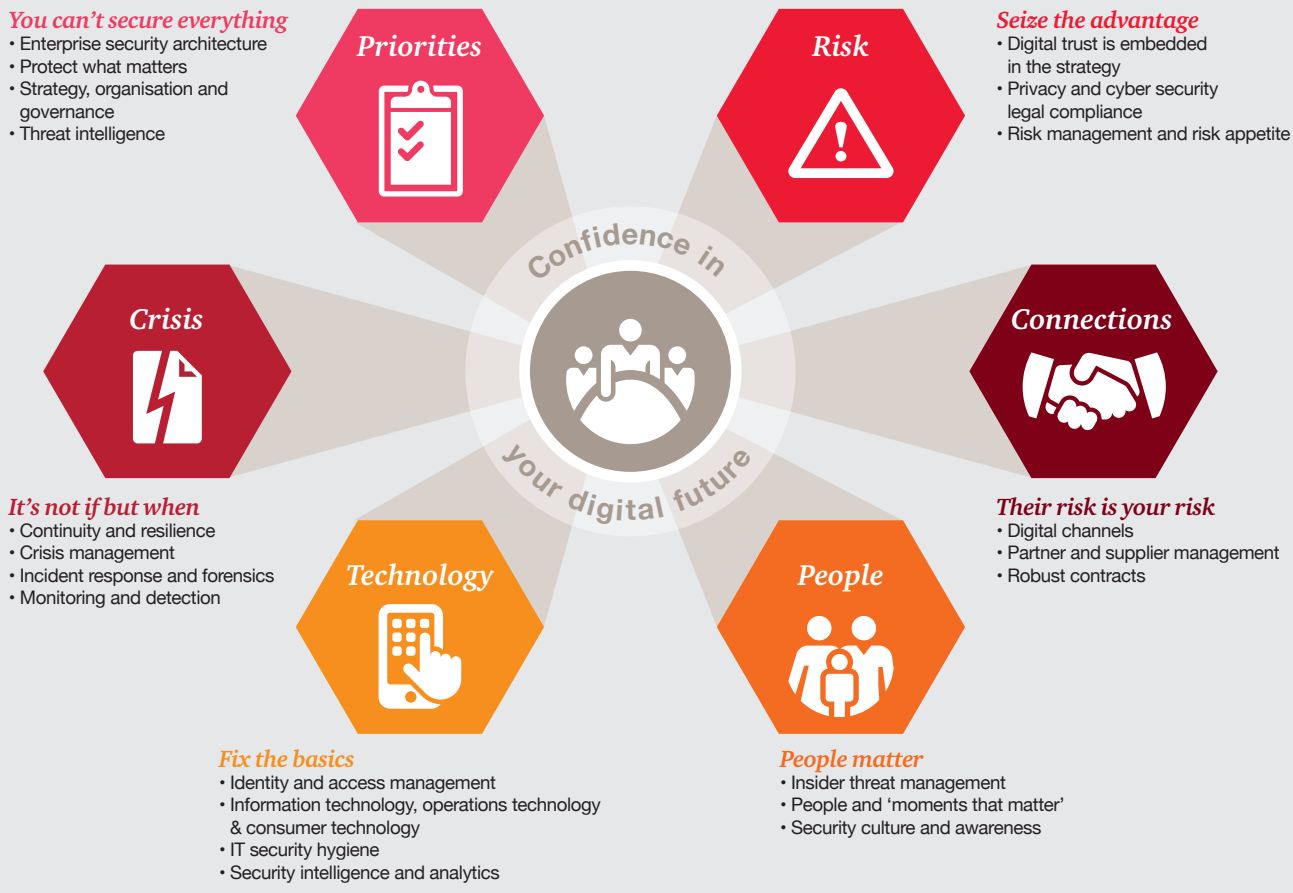
Banks have invested hundreds of millions of dollars in cyber security, bringing in people from intelligence agencies and even ex-hackers to advise on safeguards.[26] It is insurers also need to continue to invest appropriately in their own cyber security given the volume of sensitive policyholder information they hold which, if compromised, would lead to a loss of trust that would be extremely difficult to restore. The sensitive data held by cyber insurers that hackers might well want to gain access to includes information on clients' cyber risks and defences.

The starting point is for boards to take the lead in evaluating and tackling cyber risk within your own business, rather than simply seeing this as a matter for IT or compliance (see Figure 4).

25 For a more detailed exploration of the issues please see 'Broking 2020: Leading from the front in a new era of risk' (http://www.pwc.com/gx/en/insurance/reinsurance-rendezvous/insurance-2020.jhtml)

26 Cyber insecurity: When 95% isn't good enough, Financial Times, 28 July 2015

Figure 4: Cyber security isn't just about technology



Source: PwC

Key questions your board should be asking as it looks to strengthen protection include:

- *Who are our adversaries, what are their targets and what would be the impact of an attack (see Figure 5)?*
- *We can't lock down everything, so what are the most important assets ('crown jewels') we need to protect?*
- *How effective are our processes and assignment of responsibilities, as well as our systems safeguards?*
- *Are we integrating threat intelligence and assessments into proactive cyber defence programmes?*
- *Do we assess vulnerabilities against known tactics and tools used by perpetrators who might target them?*

The answers to these questions would help your business develop the risk awareness and organisation-wide response that are the hallmarks of cyber resilience. This resilience will in turn enable you to safely realise the benefits of technological advances to enhance innovation, collaboration, productivity and customer experience.

Figure 5: Assessing threats and vulnerabilities

	Motives	*Targets*	*Impact*
Nation state	• Economical or political advantage	• Trade secrets • M&A information • Critical financial systems and information	• Loss of competitive advantage • Regulatory investigation/penalty • Disruption to critical infrastructure
Organised crime	• Immediate financial gain • Collect information for future financial gains	• Financial/payment systems • Personally identifiable or sensitive information • Payment card information • Protected health info	• Regulatory investigation/penalty • Law suits • Brand and reputation • Loss of consumer confidence
Hacktivists	• Influence political and/or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Critical financial systems • Personally identifiable/sensitive information	• Regulatory investigation/penalty • Law suits • Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Bribery or coercian	• Sales, deals, market strategies • Corporate secrets • Business operations • Personally identifiable/sensitive information • Administrative credentials	• Trade secret disclosure • Operational disruption • Loss of consumer confidence

Source: PwC

4

Conclusion: Sharpening differentiation and return

In a market with relatively flat pricing and restrictive terms, better understanding and control of cyber exposures would offer both clear competitive differentiation and more sustainable returns. Key advantages include the ability to offer more attractive prices, conditions and exclusions to your clients, as well as the development of more effective risk transfer solutions.

The initial priority is to identify the specific triggers for claims, and the level of potential exposure in policies that may not have been written with cyber threats in mind.

You can then look at how to develop the scenario analysis, dynamic threat intelligence and more active mitigation of client risks that would allow you to evaluate and control exposures more effectively.

It will still be difficult to price with anything like the confidence and precision of more mature liability business lines. But a more informed and sustainable cyber insurance model would enable you to reduce the cushion in your pricing, allocate capital more efficiently and seek out efficient reinsurance and capital market risk transfer. You would also be in a better position to know when to turn on and off the tap of underwriting and target specific market openings.

Your own cyber security is crucial in capitalising on the benefits of digitisation and becoming leaders in the fast growing cyber insurance market. The key is looking at this as an enterprise rather than systems/technology risk and encouraging the board to take the lead in integrating cyber resilience into business operations.

Some insurers and reinsurers may still be wary of cyber risk. At the other end of the spectrum, some may be opening themselves up to dangerous exposures. But we believe that a combination of smart analytics, agility of response and risk transfer innovation would enable you to capitalise on the opportunities without jeopardising the safety of your business.

Contacts

This report covers part of the overall picture and there are many more areas to share and discuss. If you would like to explore the trends further to help you assess how these could affect your business, please speak to your usual PwC contact or one of the authors listed here:

Stephen O'Hearn
Global Leader, Insurance
Partner, PwC (Switzerland)
+41 (0)44 628 0188
stephen.ohearn@ch.pwc.com

David Grace
Global Leader, Financial Crime (FS)
Partner, PwC (UK)
+44 (0) 20 7212 4881
david.w.grace@uk.pwc.com

Sarah Butler
Insurance Leader, Strategy&
Partner, PwC (Australia)
+86 138 1735 5416
sarah.butler@strategyand.pwc.com

Stewart Room
Global Head of Cyber Security and Data Protection
Partner, PwC Legal (UK)
+44 (0) 20 7213 4306
stewart.room@pwclegal.co.uk

Vincent Loy
Financial Crime & Cyber Leader (FS)
Partner, PwC (Singapore)
+ 65 6 236 7498
vincent.j.loy@sg.pwc.com

Alex Finn
European Leader, Insurance
Partner, PwC (UK)
+44 (0) 20 7212 4791
alex.w.finn@uk.pwc.com

Simon Copley
Asia-Pacific Leader, Insurance
Partner, PwC (HK)
+852 2289 2988
simon.copley@hk.pwc.com

Greg Galeaz
US Leader, Insurance
Partner, PwC (US)
+1 (774) 573 0220
gregory.r.galeaz@us.pwc.com

Australia

Christopher Daniell
Partner, PwC (Australia)
+61 (2) 8266 1682
christopher.daniell@au.pwc.com

Canada

Keegan Iles
Insurance Consulting Leader
Director PwC (Canada)
+1 416 815 5052
keegan.a.iles@ca.pwc.com

China

Ramesh Moosa
Forensic Technology Solutions Leader China/Hong Kong
Partner, PwC (China)
+86 (21) 2323 8688
ramesh.moosa@cn.pwc.com

France

Philippe Trouchaud
France Consulting Technology Leader
Partner, PwC (France)
+33 (0)1 56 57 82 48
philippe.trouchaud@fr.pwc.com

Germany

Kurt Mitzner
Partner, PwC (Germany)
+49 (211) 981 1496
kurt.mitzner@de.pwc.com

Hong Kong

Kenneth Wong
Cybersecurity Leader Stephen Catlin China/Hong Kong
Partner, PwC (HK)
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

India

Anuraag Sunder
Director, PwC (India)
+91 124 616 9757
anuraag.sunder@in.pwc.com

Japan

Naoki Yamamoto
Cybersecurity and Privacy Leader
PwC (Japan)
+81 80 2105 3073
naoki.n.yamamoto@jp.pwc.com

Yasuhiro Kishi
Partner, PwC (Japan)
+81 90 6514 4913
yasuhiro.kishi@jp.pwc.com

UK

Alex Petsopoulos
UK FS Cyber Security Leader
Partner, PwC (UK)
+44 (0)20 7804 6775
alex.petsopoulos@uk.pwc.com

Paul Delbridge
Partner, PwC (UK)
+44 (0) 20 7212 3085
paul.p.delbridge@uk.pwc.com

David Bettesworth
Partner, PwC (UK)
+44 (0) 20 7212 2989
david.bettesworth@uk.pwc.com

Kris McConkey
Partner, Cyber Security
PwC (UK)
+44 (0) 20 7804 2471
kris.mcconkey@uk.pwc.com

Daljitt Barn
Director, Cyber Security
PwC (UK)
+44 (0) 20 7804 8488
daljitt.barn@uk.pwc.com

Charlie McMurdie
Senior Cyber Crime Advisor
PwC (UK)
+44 (0) 20 7804 8895
charlie.mcmurdie@uk.pwc.com

Richard Horne
Partner, PwC (UK)
+44 (0) 20 7213 3227
richard.horne@uk.pwc.com

Michael Cook
Director, PwC (UK)
+44 (0) 20 7213 2015
michael.g.cook@uk.pwc.com

Dom del Re
Director, PwC (UK)
+44 (0) 20 7213 5720
domenico.del.re@uk.pwc.com

James Rashleigh
Director, PwC (UK)
+44 (0) 20 7212 2060
james.m.rashleigh@uk.pwc.com

US

Joseph Nocera
US FS Cybersecurity Leader
Partner, PwC (US)
+1 (312) 298 2745
joseph.nocera@us.pwc.com

Richard Mayock
Global Broking Leader
Partner, PwC (US)
+1 (646) 471 5090
richard.mayock@us.pwc.com

James Shira
Principle & Network Chief Information Security Officer
Partner, PwC (US)
+1 (213) 433 7284
james.shira@us.pwc.com

Eric Matrejek
Global Advisory Computer Forensics & eDiscovery Leader
Partner, PwC (US)
+1 (312) 298 5637
eric.matrejek@us.pwc.com

Jamie Yoder
US Advisory Leader, Insurance
Partner, PwC (US)
+1 (773) 255 2138
jamie.yoder@us.pwc.com

Anand Rao
PwC Innovation Leader, Analytics
Principal, PwC (US)
+1 (617) 530 4691
anand.s.rao@us.pwc.com

For more information on the Global Insurance Marketing programme, contact Claire Clark on +44 20 7212 4314 or at claire.l.clark@uk.pwc.com.

www.pwc.com/insurance