top issues

The promise and pitfalls of cyber insurance

January 2016

pwc

The promise and pitfalls of cyber insurance

Cyber insurance is a potentially huge but still largely untapped opportunity for insurers and reinsurers. We estimate that annual gross written premiums will increase from around $2.5 billion today[1] to $7.5 billion by the end of the decade.[2] Accordingly, 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.

However, wariness of cyber risk is widespread. Many insurers don't want to cover it at all. Others have set limits below the levels their clients seek, and also have imposed restrictive exclusions and conditions – such as state-of-the-art data encryption or 100% updated security patch clauses – which 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 claims, many companies question if their cyber insurance policies provide real value.

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 start to question the value of their policies and concerns widen about the level and concentration of cyber risk exposures?

1 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)

2 PwC estimate

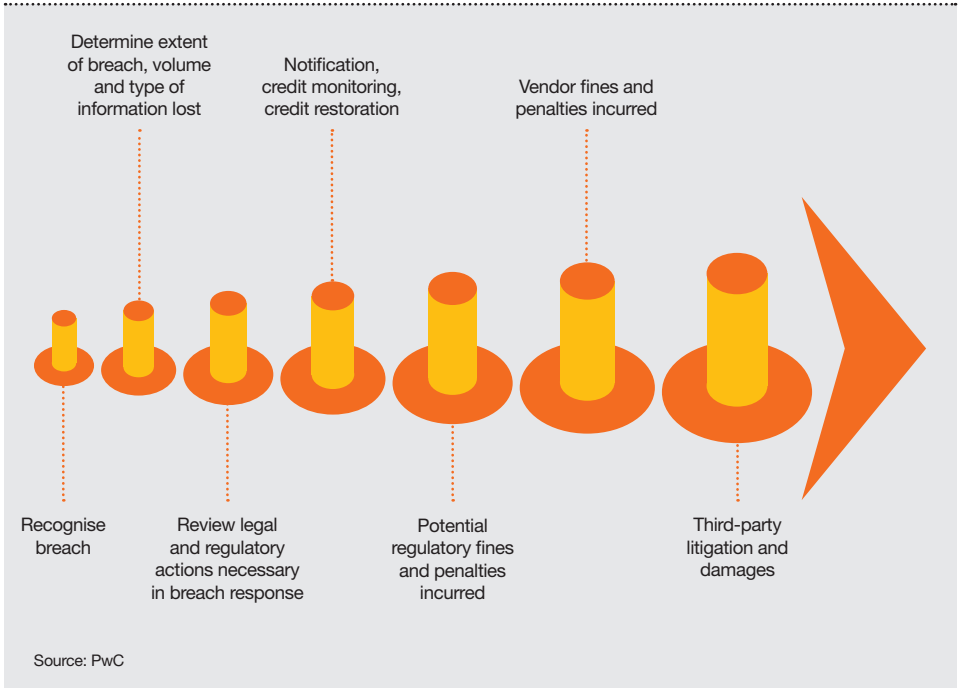
The risk pricing challenge

The biggest challenge for insurers is that cyber isn't like other risks. There is limited publicly available data on the scale and financial impact of attacks and threats are very rapidly changing and proliferating. Moreover, the fact that cyber security breaches can remain undetected for several months – even years – creates the possibility of accumulated and compounded future losses.

While underwriters can estimate the cost of systems remediation with reasonable certainty, there isn't enough historical data to gauge further losses resulting from brand impairment or compensation to customers, suppliers, and other stakeholders. And, although the scale of potential losses is on par with natural catastrophes, cyber incidents are much more frequent. Moreover, many insurers face considerable cyber exposures within their technology, errors & omissions, general liability, and other existing business lines. 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 rapid sequence of high loss events.

So, how can cyber insurance be a more sustainable venture that offers real protection for clients, while safeguarding insurers and reinsurers against damaging losses?

Figure 1: A cyber breach has a long and unpredictable tail



Source: PwC

Real protection at the right price

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. **Clarify risk appetite –** Despite the absence of robust actuarial data, it may be possible to develop a reasonably clear picture of total maximum loss and match it against risk appetite and tolerances. Key inputs include worst-case scenario analysis. For example, if your portfolio includes several US power companies, then what losses could result from a major attack on the US grid? What proportion of claims would your business be liable for? What steps could you take now to mitigate losses by reducing risk concentrations in your portfolio to working with clients to improve safeguards and crisis planning?

   Asking these questions can help insurers judge which industries to focus on, when to curtail underwriting, and where there may be room for further coverage. Moreover, even if an insurer offers no standalone cyber coverage, it should gauge the exposures that exist within its wider property, business interruption, general liability and errors & omissions coverage.

Even if an insurer offers no standalone cyber coverage, it should gauge the exposures that exist within its wider property, business interruption, general liability and errors & omissions coverage.

Cyber risks are increasingly frequent and severe, loss contagion is hard to contain, and risks are difficult to detect, evaluate, and price.

2. **Gain broader perspectives –** Bringing in people from technology companies and intelligence agencies can lead to more effective threat and client vulnerability assessments. The resulting risk evaluation, screening, and pricing process could be a partnership between existing actuaries and underwriters who focus on compensation and other third-party liabilities, and technology experts who concentrate on data and systems. This is similar to the partnership between CRO and CIO teams that many companies are developing to combat cyber threats.

3. **Create tailored, risk-specific conditions –** Many insurers currently 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 a client's business. It also could draw on threat assessments by government agencies and other credible sources to facilitate evaluation of threats to particular industries or enterprises. Another possible component is exercises that mimic attacks to test both weaknesses and plans for response. As a result, coverage could specify the implementation of appropriate prevention and detection technologies and procedures.

   This approach can benefit both parties. Insurers will have a better understanding and control of risks, lower exposures, and more accurate pricing. Policyholders will be able to secure more effective and economical protection. Moreover, the assessments can help insurers forge a closer, advisory relationship with clients.

4. **Share data more effectively –** More effective data sharing is the key to greater pricing accuracy. For reputational reasons, many companies are wary of admitting breaches, and 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 and the UK's Cyber Security Information Sharing Partnership). In addition, data pooling on operational risk, through ORIC, provides a precedent for more industry-wide sharing.

5. **Develop real-time policy updates –** 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. **Consider hybrid risk transfer –** Although the cyber reinsurance market is relatively undeveloped, a better understanding of evolving threats and maximum loss scenarios could encourage more reinsurers to enter the market. Risk transfer structures likely would include traditional excess of loss reinsurance in the lower layers, and the development of capital market structures 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 could apply reinsurers' and/or technology companies' expertise to develop appropriate evaluation techniques.

7. **Improve risk facilitation –** Considering the complexity and uncertainty 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 brokers – will need to bring together all parties and lead the development of effective solutions, including the cyber insurance standards that many governments are keen to introduce.

Evaluating and addressing cyber risk is an enterprise-wide matter – not just one for IT and compliance.

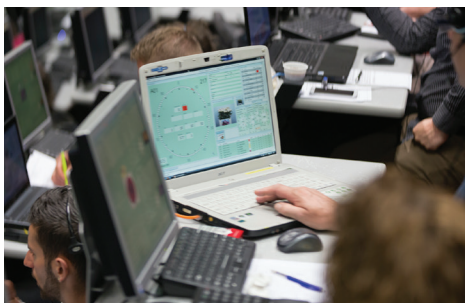
8. **Enhance credibility with in-house safeguards –** If an insurer can't protect itself, then why should policyholders trust it to protect them? If the sensitive policyholder information that an insurer holds is compromised, then it likely would lead to a loss of customer trust that would be extremely difficult to restore. 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.

Key questions for insurers as they assess their own and others' security

From the board on down, insurers need to ask:

- Who are our adversaries, what are their targets, and what would be the impact of an attack?
- We can't defend everything, so what are the most important assets we need to protect?
- How effective are our processes, assignment of responsibilities, and systems safeguards?
- Are we integrating threat intelligence and assessments into proactive cyber defense programs?
- Are we adequately assessing vulnerabilities against the tactics and tools perpetrators use?

Implications



- Even if an insurer chooses not to underwrite cyber risks explicitly, exposure may already be part of existing policies. Therefore, all insurers should identify the specific triggers for claims, and the level of potential exposure in policies that they may not have written with cyber threats in mind.
- Cyber coverage that is viable for both insurers and insureds will require more rigorous and relevant risk evaluation informed by more reliable data and more effective scenario analysis. Partnerships with technology companies, cyber specialist firms, and government are potential ways to augment and refine this information.
- Rather than simply relying on blanket policy restrictions to control exposures, insurers should consider making 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. This more informed approach can enable insurers to reduce uncertain exposures and facilitate more efficient use of capital while offering more transparent and economical coverage.
- Risk transfer built around a hybrid of traditional reinsurance and capital market structures offer promise to insurers looking to protect balance sheets.
- To enhance their own credibility, insurers need to ensure the effectiveness of their own cyber security. Because insurers maintain considerable amounts of sensitive data, any major breach could severely impact their market credibility both in the cyber risk market and elsewhere.

Contacts

Joe Nocera
FS Cybersecurity Principal
+1 312 298 2745
joseph.nocera@pwc.com

Chris Morris
FS Cybersecurity Principal
+1 617 530 7938
christopher.morris@us.pwc.com

Shawn Connors
FS IT Infrastructure Principal
+1 646 471 7278
shawn.joseph.connors@us.pwc.com

www.pwc.com/us/insurance