FTI CONSULTING

HOW MUCH IS ENOUGH?

Pricing insurance in the age of cyber-risk

The demand for cyber insurance is increasing with written premiums expected to grow to over $2 billion by 2020. However, as the impact of cyber-attacks continues to escalate, actuaries and underwriters are facing increased pressures to model adequate protection which covers the full scope of the business value chain.

How can the insurance industry effectively measure and price cyber-risk insurance policies?

Here we explore the key challenges insurers are now facing when pricing cyber-risk policies and look at some different pricing options.

The great mismatch

Cyber-attacks give rise to a range of new issues which make risk measurement almost impossible for actuaries and underwriters. For example, a cyber-attack could cause a blackout affecting homes, businesses, healthcare facilities, schools and government agencies. This category of risk is not well covered by the insurance industry, which historically has simply needed to provide coverage where the damage and value to physical assets are measurable.

Therein lies the dilemma: a cyber risk is priced as a man-made risk, yet has many of the features of natural disasters with high impact and large-scale damages. This will become even more important as sovereign combatants and terrorists increasingly target their attacks on the industrial control systems of critical infrastructure, such as water authorities, energy and power generation and distribution systems, where detection can be very difficult and damage consequences existential. When a high-risk event occurs, such as a natural disaster, insurers will typically cover only a small portion of the required capital to pay for the losses, perhaps covering only a limited number of components. This is due to the difficulties and ambiguities of establishing the direct cause, determining what and who is affected and accurately measuring the damage.

As a result, insurance coverage issues arising from cyber-attack claims are typically unresolved, or in negotiation, dispute or litigation for many years.

The complexity and interconnectedness of large data sets cause the risk to be difficult to identify and underwrite, so that there is often a mismatch of value and coverage.

Pricing mechanisms

With cyber-attacks representing a new risk category, a major challenge is posed to reinsurers who wish to give guidance on pricing and potential coverage to their clients. Most reinsurers have therefore sought to establish pricing mechanisms based on scenario, planning and forecasting, enabling them to cover large portions of potential losses.

Where there is lack of data for pricing certain risks such as cyber-risks, insurers tend to use scenarios and split the risks into components. They then look for similar risks which can be measured. For example, if a virus attacks a portion of an IT system and the system is subsequently patched, the virus or parts of the virus may still remain in the system. If all, or part of this virus subsequently reemerge sand attacks the system again, it is not clear whether this is a new event or part of the old one. This is a serious and new issue which can have significant coverage implications,

Simply put, there is a large gap between the demand for cyber-risk coverage and the current ability of insurers to underwrite the necessary insurance programmes. Partly, this is since insurers have limited data with which to understand and qualify a risk profile, but they also have little experience on which to base their underwriting efforts. Asa result the majority of the techniques in the underwriting process are used on a primary basis and very few insurers write excess-only business for cyber-risks. This explains the gap between the damages and the paid claims.

The techniques for underwriting cyber-risk coverage fall under Errors & Omissions (E&O) insurance, which is also known as professional liability or professional indemnity insurance.

Most insurers sell a stand-alone policy or a policy with an endorsement written for E&O, Directors and Officers, Crime or General Liability Insurance.

Since cyber-attacks result in multiple costs, including customer and third-party liabilities and lost revenues, notification costs, forensic investigations, legal fees and repair and reinstatement costs for data and physical property, these different risk components must be observed and priced separately. The technical environment, the security of data and the other security measures need to be part of the overall risk profile when calculating the expected costs of damage.

Example of a cyber-risk claim

Every company retains or stores sensitive personally identifiable information and could be financially ruined if that data is compromised and exposes customers to the possibility of identity theft and credit problems.

For example, a hacker could break into the company's network, steal all its customer data and threaten to post it publicly or sell it to the highest bidder.

A computer malfunction or employee error results in the accidental distribution of sensitive customer data contained in the employee's laptop or USB flash drive, perhaps in the form of a mass e-mail, print-outs, or on a website.

The insurance market recognises that it needs to find a solution to the challenge posed by cyber-risk. Yet with this emerging sector relying largely on highly hypothetical scenarios, the key question remains: Can cyber-risk be measured with sufficient reliability to enable companies to effectively and reliably insure it? The answer to this is still not clear.

Petra Wildemann
Actuarial Practice Leader, EMEA
+41 (76)322 5716
+44 (0)20 3727 1759
petra.wildemann@fticonsulting.com

Scott Corzine
Risk Management Practice
Co-leader, US
+1 336-768-8218
scott.corzine@fticonsulting.com

Jo Franklin
Marketing Manager
+44 20 3727 1762
jo.franklin@fticonsulting.com