CYBER SECURITY SERIES:

CYBER INSURANCE PRICING

CAPCO

QUANTIFYING THE UNKNOWN IN A MULTIBILLION DOLLAR MARKET

Cyber insurance is potentially a huge growth opportunity, but to exploit it profitably firms must identify and quantify cyber risks.

The attitude to cyber insurance is changing. This is partly being driven by the increasing awareness of major security breaches. Cyber insurance is now seen as a core element of mainstream business risk management, with uptake increasing by a staggering 50% in one year*. The shift in perception is driving the market growth, with projections for the global market to triple and reach $7.5 billion by the end of the decade**.

These levels of growth present insurers with massive opportunities. However, cyber insurers are waking up to a tough reality. Accurately quantifying the underlying cyber risk and the impacts of security breaches is exceptionally complex. Insurers must develop better methods of cyber risk modelling to improve accuracy and consistency. The pay-off is that this will enable them to realise the market potential.

PRICING CHALLENGES

To price a premium, insurers must accurately quantify the risks to which their clients are exposed. Beyond this, comparisons with conventional risk pricing are scarce. Cyber risk arises in a complex ecosystem of interlinked vulnerabilities, security threats, and potential associated impacts. It is also inherently specific to individual clients, with characteristics including:

- The attractiveness of a business as a cyber target
- Potential financial and reputational damage a cyber attack could inflict
- The organisation's 'security posture'; i.e. how robustly they are equipped to detect and repel cyber threats, based on their information security infrastructure and practices
- The orgnisation's ability to effectively respond to a breach.

These variables have proven difficult to ascertain. Conventional premium generation employs modelling techniques that incorporate data from past events. However, a major challenge confronting the cyber security domain is the scarcity of historical data relating to cyber threats, actual breaches, and resulting impacts. Only recently it became mandatory for breached entities to disclose details of their cyber security breaches. Previously, companies were reluctant to (voluntarily) disclose breaches due to potential reputational damage. And although third-party threat intelligence sources do exist, insurers have been slow to use their expertise.

In addition to analysis of past events, accurate cyber insurance pricing must also account for future events. This is particularly difficult, due to a number of factors, including:

- Constantly changing business environment
- Rapid evolution of information technology
- Evolving and difficult to predict threat landscape
- Fast-paced and complex regulation.

The combined effect of these challenges is that the scope and degrees of liability of cyber insurance policies are difficult to predict.

Compounding the issue, cybersecurity risk is shared between businesses and other enterprises they interact with. Known as risk correlation, it means that a breach of any one component within an interconnected system could potentially compromise the entire network. Historically, risk correlation has been a major factor that makes realistic premium calculation very difficult. But getting it wrong can bring serious implications, both for the individual insurer's business and the market as a whole.

INSURERS' REACTIONS

In this complex and rapidly developing cyber threat environment, insurers have mitigated their exposure to liabilities by offering bespoke policies at high premiums. This has fragmented the cyber insurance market and hindered realisation of its full potential. Today's offerings bear hallmarks of highly 'niche' products, including non-standardised policies that dramatically vary by geography and industry.

High barriers to entry have left smaller businesses unprotected. But serious vulnerability extends beyond the uninsured, to the insurance companies themselves. Any institution tackling cyber threat challenges, while lacking the necessary expertise, risks direct exposure to multiple and unaccounted risk correlations. The worst-case scenario is a single, major catastrophe - a 'contagion event' that affects large numbers of consumers. It is possible that such an event could have consequences similar to the financial crisis of 2008.

QUANTIFYING UNKNOWNS WITH A HOLISTIC APPROACH

The combination of obstacles discussed so far have blocked development of truly comprehensive methods for cyber risk modelling. As a result, premium pricing remains inaccurate. This has inhibited greater uptake of cyber insurance as an effective element of risk management.

A dynamic landscape necessitates a dynamic response. This must include real-time security posture monitoring and dynamic risk quantification. To enact positive change, there are clear areas that actuaries and underwriters must address, such as:

- Compensation for weak historical data through innovation
- Incorporation of expert-derived security and industry-specific intelligence
- Implementation of cutting-edge technologies, including machine learning.

As cyber threats continue to expand in the near future, commercial opportunities in the cyber security domain continue to grow. Provision of appropriate, accessible, and affordable cyber security protection products and premiums is critical to this growing market. But it will not happen until the right innovation is widely implemented. Nor can the industry make this positive shift alone. Legislation has a key role to play, promoting policy standardisation and helping prepare for the big move from niche to sustainable mass-market offerings.

REFERENCES:

*Cybersecurity insurance grew 50% in the UK between 2015 and 2016
(source: https://www.infosecurity-magazine.com/news/cyber-insurance-adoption-soared-50/)

**https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges/at_download/fullReport

AUTHORS:

Evdokia Kardoulaki, Associate Consultant

Kian Adam Rahnejat, Consultant

Kristian McCaul, Associate Consultant

Danushka Jayasinghe, Consultant

Jibran Ahmed, Managing Principal

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on **Twitter, Facebook, YouTube,LinkedIn** and **Xing.**

WORLDWIDE OFFICES

Bangalore	Frankfurt	Pune
Bangkok	Geneva	São Paulo
Bratislava	Hong Kong	Singapore
Brussels	Houston	Stockholm
Charlotte	Kuala Lumpur	Toronto
Chicago	London	Vienna
Dallas	New York	Warsaw
Dusseldorf	Orlando	Washington, DC
Edinburgh	Paris	Zurich

CAPCO.COM

CAPCO