Inside the Mind of a Cyber Underwriter

May 2015 • Lockton® Companies

Significant data breaches, such as Community Health System, Target, Home Depot, Staples Inc, Bebe Stores, Anthem, Premera, and White Lodging (their second), during the past 18 months, have impacted the cyber/data breach insurance market.

The combination of these 'earthquakes', insurance regulatory scrutiny, and the underwriters' desire to maintain profitability have led to fewer insurers providing cyber/data breach cover. Rates are going up, as underwriters are better able to understand their exposures and the ripple effects of claims.

The part of the cyber insurance policy that is paying the most on claims, privacy data breach response costs, has a short loss life cycle. The underwriters realise their losses very quickly, often within 12 months rather than 3-5 years. As a result, underwriters' rates move quickly, unlike the traditional ebb and flow of professional liability, and their risk selection has become increasingly discerning.

MAX PERKINS
Senior Vice President
Global Technology &
Privacy Practice
+44 (0) 207 933 2694
Max.Perkins@uk.lockton.com

> "Rates are going up, as underwriters are better able to understand their exposures and the ripple effects of claims."

LOCKTON®

The underwriters' long-term goal is to be sustainable

The long-term goal of an underwriter is to offer insurance solutions that yield a margin, in order to maintain a stable presence in their marketplace. Underwriters constantly monitor claims trends, including severity and frequency of cyber breaches across industry sectors. Examples of severity breaches in the cyber and data breach insurance market include Target and Anthem. The industry with the highest frequency of breaches is healthcare, where HIPAA violations occur on a daily basis.

Underwriters also cross-reference specific claims against the policy wording that triggered an unforeseen loss. Underwriting teams write business plans that include the cost of paying claims. However, they, like any business, find it hard to plan for unintended costs. DSW Shoe Warehouse received data breach coverage under their commercial crime policy, due to bespoke wording which was unintentionally broad enough to cover a cyber/data breach.

Both expected severity and frequency trends, and forecasted claims payments are used by underwriters to prepare models for their business plans. Higher than predicted, severity or frequency of claims will results in adjustments to an underwriter's rates, retentions, or risk selection. Unforeseen loss leads to a change in risk appetite or policy wordings.

How do the underwriters deal with loss trends?

Since December 2013, the increase in hacking on a criminal, hacktivist and state sponsored basis has made it hard for underwriters to predict their losses. The difficulty in modelling insurance coverage for persistent outside threats, is that they constantly evolve. These loss patterns are unpredictable, and difficult for underwriters to model in order to provide profitable returns and sustainable insurance products.

Underwriters believe you can improve your network security controls but hackers will continue to work tirelessly to beat them. Your rates and retentions will go up. The insurers informed risk selection is making it harder for you to buy cyber/data breach insurance cover.

> "Underwriters believe you can improve your network security controls but the hackers will continue to work tirelessly to beat them."

What is next for underwriters?

Aggregation! Underwriters are growing concerned about their exposure to one breach which affects many of their insureds simultaneously. Anthem's breach was the first that affected the market in this way, and is being used as an example for underwriting management teams and regulators to inquire about systemic exposures involving multiple insureds. This is an on-going conversation, and we will work to keep you informed.

The cyber breach insurance market is maturing

We are in the midst of a challenging market for new and existing buyers in the retail, hospitality, and healthcare industries. Risk selection is more discerning and the underwriting process is more sophisticated.

The cyber insurance market has gone from approximately 70 insurers providing cover, with over 25 offering a primary lead. We anticipate that we will soon have fewer than 15 true primary insurers, and that each primary or excess will find their sweet-spot for risk selection. Only the largest insurers will have books that can withstand the unpredictable losses in order to maintain broad risk appetites. Like other mature markets, the profits from their books will lead to the rise and fall of rates and retentions going forward. To better understand their exposure, underwriters are now using supplemental application forms, combined with follow-up conference calls.

Supplemental applications look at data encryption tools, network segmentation, and point of sale systems, if there is exposure to credit card details. Please keep in mind that presenting best in class data privacy controls will help you obtain better quotations from underwriters. Presenting the antiquated controls and a lack of privacy culture within your organization will lead to unfavourable terms, if any are offered at all.

How can Lockton's Global Technology and Privacy Practice team help?

The Global Technology and Privacy Practice is the largest cyber broking in the London market. We are dedicated to providing the best service and most comprehensive solutions to meet your business needs. Working with us gives you access to the insurance markets in London, Bermuda and continental Europe.

We leverage global knowledge that comes from placing $20 billion of premiums for clients across multiple industries and jurisdictions.

The team is made up of a diverse group of individuals, including people with deep broking, legal and underwriting backgrounds.

We continue to invest in the team, to help you with your business needs.

About the Author

Max joined to Lockton's Global Technology and Privacy Practice in early 2015 to develop solutions in partnership with you, to help you manage your cyber and network security, and emerging cyber risks.

Prior to joining Lockton, Max was an underwriter at the Beazley Group, where he led the development of data breach and tech errors and omissions products for Beazley's Lloyd's syndicate, underwrote risk management accounts and was the team leader for Beazley's London market US information security and breach response products. Max also underwrote miscellaneous professional liability and cyber liability in both the middle market and risk management segments at AIG and ACE.

Max is from North Carolina and a graduate of Duke University.

Max Perkins, Senior Vice President
+44 (0) 207 933 2694
Max.Perkins@uk.lockton.com

Our Mission

To be the worldwide value and service leader in insurance brokerage, employee benefits, and risk management

Our Goal

To be the best place to do business and to work

Rest of Team

Carl Moore, Partner
Email: carl.moore@uk.lockton.com
Tel: +44 (0)20 7933 2198

James Gordon, BA (Hons) Cert CII, Vice President
Email: james.gordon@uk.lockton.com
Tel: +44 (0)20 7933 2711

Vlad Polyakov, LLB (Hons), Assistant Vice President
Email: vlad.polyakov@uk.lockton.com
Tel: +44 (0)20 7933 2048

Mark Walters, Assistant Vice President London
Email: mark.walters@uk.lockton.com
Tel: +44 (0)20 7933 2023

Lucy Scott, LLB (Hons), Associate
Email: lucy.scott@uk.lockton.com
Tel: +44 (0)20 7933 2382

Reece Kent, Cert CII, Associate
Email: reece.kent@uk.lockton.com
Tel: +44 (0)20 7933 2209

Corinne Hammond, Bsc (Hons), Associate
Email: corinne.hammond@uk.lockton.com
Tel: +44 (0)20 7933 2039

Cliff White, Dip CII and CITIP, Senior Vice President
Email: cliff.white@uk.lockton.com
Tel: +44 (0)20 7933 2704