Market Conditions: Not Soft

We use the word soft to describe the cyber world: soft copy vs. hard copy; software vs. hardware. While the same word could be used to describe most of the insurance marketplace today, it does not apply to cyber insurance. A hardening cyber insurance market persists, particularly for health care and retail risks.

Premiums are higher, capacity is restricted and underwriting scrutiny is heightened. The driving force is, of course, losses: in the past 18 months, major claims have hit not just primary underwriters but excess underwriters through layered towers of $100M to $150M in limits.

We do not expect the marketplace to flatten out any time soon. Further, cyber threats are escalating, with concern that U.S. infrastructure and businesses could be under attack from cyber criminals with varying agendas. Growing technology risks associated with the expansion of the mobile workforce, broad adoption of ‘bring your own device’ (BYOD) policies, and innovations, such as wearable technologies and the internet of things (IoT), will only expand threats to data privacy and security. Cyber-attacks and data breaches are likely to be the rule rather than the exception for businesses of all types going forward. Not surprisingly, the number of businesses considering purchasing cyber coverage for the first time is increasing.

Governmental responses, including the uncertain fate of U.S. Safe Harbor agreements with Europe, evolving U.S. state laws and federal oversight through audits and examinations conducted by the SEC, FTC, FCC and HHS/OCR, are likely to add further hardening pressure for buyers of cyber insurance.

The Underwriting Process: Not Faster

The underwriting process for new and renewal business, for both primary and excess coverage, is taking longer due to the scrutiny that carriers are applying to security controls, processes and procedures. Certain underwriters require a conference call to address these issues before they will look at an application. In some cases, detailed risk assessments may be required prior to quoting.
Renewal Pricing: Not Lower

Good risks – organizations with no claims and proper risk management protocols in place – can expect renewal pricing to increase 10% – 20%. For questionable risks – organizations that have experienced claims and have yet to adopt proper risk management protocols – increases of 200% or more can be expected, particularly in the health care and retail sectors.

Areas of Underwriting Scrutiny

Underwriters are looking to see that proper risk management protocols are deployed:

- **Governance and risk assessment** requiring current, tailored processes with senior management (including CISO and CPO positions) and board involvement
- **Access rights and controls** inside and outside the enterprise, including credentialing, access tracking and BOYD policies
- **Encryption** of PII, PHI and the transmission lines in the credit processing systems (if PII cannot be encrypted, underwriters are looking for compensating controls around the protection and monitoring of data, including file integrity monitoring and malware detection)
- **Data loss prevention**, including patch management, system configuration and outbound communications, with special emphasis on PII
- **Vendor management** that includes due diligence at the time of selection and downstream compliance controls over third-party providers
- **Training** of employees and vendors
- **Incident response plans** and data protection priorities

Capacity: Not Shrinking Entirely

Insurance industry analysts are forecasting a growth rate of 150% for cyber/privacy liability insurance in the next five years. So, while insurers are being cautious with their cyber capacity, increased demand is expected to lure carriers into what is still a marketplace in its infancy. In addition to new markets, we expect innovative solutions (such as ACE’s New Global Cyber Facility).

Benchmarking: Not Easy

Limited penetration of cyber insurance makes benchmarking a challenge. Stand-alone cyber policies, created in 1999, only started to take off in 2007 and to date, only 35% of businesses purchase cover – and that estimate may be overstated.

To complicate matters further, true peers are difficult to identify, as each company’s cyber security controls and risk mitigation efforts have a huge impact on premiums, retention levels and limits purchased. Moreover, data on the first-party sub-limits is not captured, and that is the dynamic coverage element that is triggered for data breach responses. Without critical mass and less than 10 years of historical data, public benchmarking is not a meaningful tool in the “cyber market of things.”

Even if typical benchmarking data by industry sector and revenues were available, it might not be an especially useful gauge of cyber and privacy risks. An effective cyber insurance program should be tailored to an organization’s specific exposures to loss, risk tolerance level and its regulatory and legal compliance requirements.

More concretely, the current statistics tell us of businesses with over $5B in revenue, 29.9% are buyers; with $1B–$5B in revenues, 21.8% are buyers; with $300M–$1B in revenues, 20.5% are buyers; and with $100M–$300M, 17.6% are buyers. Only 10% of businesses with $25M to $100M in revenue are buyers.

The U.S. has the highest cost of cyber-crime, and companies in all industries and all sizes are targets. The average cost to a business in the U.S. after a data breach is $6,530,000.

The Costs

<table>
<thead>
<tr>
<th>Average cost (in millions USD) of cyber-crime as of June 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States: 12.69</td>
</tr>
<tr>
<td>Germany: 8.13</td>
</tr>
<tr>
<td>Japan: 6.91</td>
</tr>
<tr>
<td>France: 6.38</td>
</tr>
<tr>
<td>United Kingdom: 5.93</td>
</tr>
<tr>
<td>Australia: 3.99</td>
</tr>
<tr>
<td>Russia: 3.33</td>
</tr>
</tbody>
</table>
Average organizational cost to a business in the U.S. after a data breach from 2006 to 2015

Share of companies with cyber insurance worldwide by revenue as of November 2014 – Millions U.S. Dollars

Share of companies considering purchasing cyber liability insurance in the next year worldwide from 2011 to November 2014

The observations, comments and suggestions we have made in this publication are advisory and are not intended nor should they be taken as legal advice. Please contact your own legal adviser for an analysis of your specific facts and circumstances.

Contact
Anthony V. Dagostino
Executive Vice President
Cyber Practice Leader
D: +1 212 915 8785
T: +1 347 205 5312
anthony.dagostino@willistowerswatson.com

Copyright © 2016 Willis Towers Watson. All rights reserved.
WTW-NA-2016-15081
willistowerswatson.com