JKJ JOHNSON KENDALL JOHNSON

CYBER INSURANCE
MARKET WHIPLASH 2021

It's no secret that the broader commercial insurance industry is well into a true "hard market" – a term used to describe an increase in rates and decrease in capacity, or unwillingness of carriers to write larger limits of insurance.

However, the first half of 2020, despite the dawning of a global pandemic, saw relatively flat Cyber Insurance renewals in the small-to-medium size business (SMB) space. But the effects of laxed security controls (amidst competing priorities of a pandemic) and remote working has taken a toll through an increase in cyber events. The second half of 2020 we started to feel what would become a true "hardening" of the Cyber Insurance market: rates are increasing in double digits, capacity/limits reduced, and policy structures starting to change.

It now seems that almost overnight, we have a ***whiplash of new underwriting scrutiny facing SMBs*** leaving them no choice but to pay significantly more for the same product, or for reductions and modifications in coverage, or often both. The markets have begun to tack on a laundry list of cybersecurity requirements as well before coverage may be granted or reduced.

Exacerbated by the significant uptick in ransomware incidents in 2020, the Office of Foreign Assets Control (OFAC) was compelled to issue a "Ransomware Advisory" on October 1, 2020 (found here https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001). The goal of the advisory was to heighten awareness that there are potential repercussions of paying a ransom. It affirms that from the perspective of law enforcement, ransomware *should not be paid if possible*, and in fact, in certain circumstances is *illegal* to pay certain blocked list of criminals.

And then, there is the SolarWinds breach that became public in December, which will reverberate through the cyber industry for years to come. This breach in particular exposed the vulnerability and impact of an extraordinary (and potentially catastrophic) cyber supply chain incident. Insurance carriers are now asking about whether their insureds utilize SolarWinds Orion network security technology, and potentially adding exclusions on policies for incidents related to the breach going forward.

Cyber Insurance as a product is remarkably younger than the other lines of commercial insurance. As cyber insurance exits its infantile stage of development, we are seeing the maturity in the insurance underwriting to better identify what aspects of a cybersecurity program will truly dictate the respective risk of any one organization. This maturation is met with improvements in the pre- and post-breach services offered by the carriers that accompany the purchase of a policy.

JKJ JOHNSON KENDALL JOHNSON

What can you expect will be ***required*** at your next Cyber Insurance renewal?

Soon the days of completing a minimalistic questionnaire on your organization to obtain Cyber Insurance will be gone. Insurance carriers are adding supplemental applications designed to identify your security controls, or lack thereof. It is now becoming commonplace for the insurance carrier to require multi-factor authentication (MFA) deployed across all emails and remote system access, segregated system backups, employee awareness and/or phishing training, the establishment of a dedicated cyber incident response policy, deployment of endpoint detection systems, and increased controls on remote access (locking down Remote Desktop Protocol). Certain carriers will also require next generation antivirus software, a patch management program (including the latest patches for known, exploited vulnerabilities), and multiple layers of authentication on financial transactions.

Mark Greisiger, President of NetDiligence® - a Cyber Risk Assessment and Data Breach Services company – shared: *"Next generation safeguards such as EDR (endpoint protection with AI) and secure third-party cloud backup are becoming a baseline standard of care for cyber underwriters trying to especially mitigate ransomware losses. It is important to note that even with these effective protective measures, losses can still occur as threat actor adversaries are smart and persistent. Also, upstream dependencies, such as third-party SPs (service providers) that host or process sensitive data, remain in place and they can be the weak link."*

Related to supply chains, organizations should consider their dependent business operations; for example: cloud hosted or other as-a-service providers, or up and downstream supply chain partners. If a dependent business partner is to suffer a cyber incident that results in extended downtime, how does that impact your organization? If the answer is that the impact could be significant, this information should be shared with your insurance broker and carrier to ensure you properly align this risk in your insurance policy.

TAKEAWAY: *These security requirements may entail a significant investment of both time and energy to deploy. It is critical for organizations to be aware of these requisites coming down the pike, and to start planning and preparing accordingly.*

What ***changes*** will we see in Cyber Insurance coverage for 2021?

Insurance markets are working hard to adapt their solutions to the evolving risk as quickly as they can. For those with state-admitted insurance products, this timeframe is extended is it requires regulatory filings and approvals. But for the excess & surplus lines products, the changes are happening almost overnight.

These are a few changes we are experiencing already this year:

- ***Significant Rate Increases (10-45%)*** - even if you've never reported a cyber incident, you can expect to pay more for the same product at your next renewal.
- ***Reduction in Limits*** - especially for Cyber Crime-related coverages, carriers are restricting their willingness to put up limits of $5M or greater without several security measures in place. Carriers are continuing to limit their willingness to cover social engineering fraud (a continually growing exposure).
- ***Coinsurance on Extortion*** – beyond the deductible, businesses are going to be required to share in the payment of any extortion demand, as much as 50/50 of any payment. This is designed to incentivize you to prevent finding yourself in a position where the best option is to pay!
- ***Breach-Specific Exclusions*** – for example, certain carriers are adding exclusions for future claims associated with the SolarWinds Orion hack.
- ***Strict Subjectivities*** **–** as outlined above, carriers are requiring certain cybersecurity measures are in place before offering coverage or higher limits.

TAKEAWAY: *Reviewing coverage options and staying attune to the marketplace is critical this year, more than ever. Not all cyber policies will be created equal, and an experienced, knowledgeable broker is needed to navigate the stormy waters ahead.*

The Silver Lining:

When your neck stops aching from the whiplash from Cyber Insurance underwriting, we can see that the restrictions and requirements being passed down are ultimately to **all** of our benefit – as we should begin to see improvements in the protection of our personal and private information and company networks. Cyber is being forced to the top of the corporate priority list, demanding more time, energy, and money be invested to improve cybersecurity posturing and risk management programming.

Organizations should bring Cyber security to the top of the pile to tackle in 2021 and start preparing for their insurance renewals now.

JKJ JOHNSON KENDALL JOHNSON

ALEXANDRA BRETSCHNEIDER, CCIC

Cyber Practice Leader | Johnson, Kendall &Johnson

Alexandra joined Johnson Kendall & Johnson (JKJ) in 2015, bringing with her diverse IT consultative relationship management experience. At JKJ, Alexandra focuses on serving clients in the nonprofit, human services, senior living, manufacturing and distribution, and technology industries. She manages the complete portfolio of her clients' commercial insurance and risk management programs.

Given her background in IT consulting, she specializes in Cyber Insurance and managing the emerging cyber and technology risks for JKJ's clients – named JKJ's Cyber Practice Leader in 2020. ***JKJ is proud to have been recently awarded Cyber Risk Retail Broking Team of the Year by Advisen in 2021, beating out the largest brokerages internationally.*** She recently obtained the Cyber COPE Insurance Certification (CCIC) designation through Carnegie Mellon – Heinz College of Information Systems and Public Policy. The objective of the CCIC designation is to better evaluate and prepare clients to manage Cyber Risk, Security, and Resilience. Alexandra can often be found speaking at various cyber seminars and associations, recently joining as a founder in the U.S. chapter of WINCyght - an international association bringing together women in the Cyber industry. Additionally, Alexandra runs the JKJ summer internship program and college recruitment process.

Alexandra graduated summa cum laude with a dual Bachelor's degree in Management Information Systems & Finance from Saint Joseph's University in Philadelphia, PA. She went on to be a Senior Consultant at Ernst & Young in Philadelphia in the Advisory Services practice, during which time she passed the Certified Internal Systems Auditor (CISA) exam. Alexandra later became the Director of Client Services at a boutique telecommunications consulting firm, managing the organization's largest consulting engagements and internal support teams. She is currently pursuing her Chartered Property and Casualty Underwriter (CPCU) designation and actively serves on the Boards of Eagleville Hospital, and Saint Joseph's University – Pedro Arrupe Center for Ethics.

Email: abretschneider@jkj.com
Phone: (215) 579-6491
Cell: (267) 274-635

JKJ JOHNSON KENDALL JOHNSON