CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

Cyber Insurance Trends Amid Rising Data Privacy Regulations

Escalating Cyber Threat Landscape Challenges Cyber Insurance Market

While the cyber and data privacy insurance market continues to mature, the escalating cyber threat landscape, coupled with ever-expanding domestic and foreign data privacy and cyber event disclosure regulations, pose challenges for companies seeking to obtain enough insurance to mitigate the financial risks of cyber attacks. A slew of new state and federal cybersecurity regulations has been enacted to further protect shareholders and consumers in the past 16 months. These new regulations are driving up the costs and reputational risk of each new cyber attack. This article explores cyber insurance market trends in the current regulatory landscape to help companies ensure they are adequately covered for cyber incident regulatory risks.

The Current Regulatory Landscape

In 2023, the SEC demonstrated its commitment to hold companies accountable for failures to make cybersecurity-related disclosures. In March 2023, the SEC brought an enforcement action against Blackbaud relating to its alleged failure to make adequate disclosures regarding a ransomware attack that allegedly impacted company customers.

Following those enforcement actions, the new U.S. Securities and Exchange cybersecurity rules took effect on Dec. 15, 2023. These rules target publicly traded companies and require open disclosure of material cybersecurity incidents within four business days of discovery. The new rules also require public companies to disclose their cybersecurity risk management practices, governance structures, and incident response procedures in their annual 10-K reports.

Practical Implications of the New Rules

These rules came into effect after an extensive commenting period, whereby companies raised concerns about the practical complications associated with the short disclosure period as well as concerns about publicly disclosing details about a company’s cyber-security practices. While the full impacts of these regulations are yet to be seen, the new reporting requirements for public companies have already led to disclosures by several well-known companies, through SEC 8-K filings relating to cyber incidents. Although the rule only requires disclosure of material cybersecurity incidents, in some instances these companies have made disclosures out of an abundance of caution.

Notable Disclosures Under the New SEC Rules

For example, on Jan. 19, 2024, Hewlett Packard filed an 8-K revealing a cyber incident taking place on Jan. 12, 2024, where a suspected nation-state actor had gained unauthorized access to HPE’s cloud-based email environment. The company specifically noted that the company had not yet reached a determination on

materiality of the breach, stating, “as of the date of this filing, the incident has not had a material impact on the Company’s operations, and the Company has not determined the incident is reasonably likely to materially impact the Company’s financial condition or results of operations.” The company later confirmed that it made the disclosure in a proactive attempt to be in compliance with the new SEC regulations.

Future Focus on Cybersecurity

Cybersecurity is likely to remain an area of focus for the SEC in 2024, with rulemaking regarding cybersecurity risk management for brokers and dealers.

State-Level Data Privacy Regulations

At the state level, regulations governing data privacy continue to take center stage. While California initially led the pack when it came to data privacy regulation with the enactment of the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) in 2018, recently other states have joined the fold through the enactment of comprehensive privacy laws that apply across industries and govern how private information is both collected and stored. These regulations typically require companies to inform consumers if they are collecting and/or selling data, and provide the consumer an opportunity to “opt-out” of such practices. To date, 15 states have enacted comprehensive data privacy laws with more states likely to follow in 2025.

International Cybersecurity Regulations

Abroad, in the United Kingdom, the Network and Information Security Directive (NIS2) is set to take effect in October 2024. This regulation is a continuation of the previous European Union cybersecurity directive that aims to achieve higher standard levels of cybersecurity across the European Union. Among other things, the NIS2 expands cybersecurity requirements, expands the scope of covered organizations, and enforces more stringent sanctions for violations across Europe. The NIS2 requires an initial report of a cybersecurity incident to be made to a competent authority within 24 hours, and a more detailed notification report communicated within 72 hours. Likewise, the EU Cyber Resilience Act, which is expected to take effect in the third quarter of 2024, is set to impose certain mandatory cybersecurity requirements for manufacturers and retailers.

Trends in the Cyber Insurance Market

These regulatory trends further illustrate the importance of cyber liability insurance. While the insurance market softened a bit coming out of 2023, with multiple industry participants reporting slightly decreased premiums and significant growth in the cyber insurance market, coverage for regulatory risk has generally become more restrictive due to increased concerns surrounding costs for regulatory compliance, investigations, settlements, and penalties. In a 2024 KYND survey of over 100 insurers and brokers, 11% of respondents identified regulatory changes as a top driver for cyber insurance sales in 2024, and we may see coverage premiums start to reflect increased risks as we move further into 2024.

Mitigating Cyber and Privacy Risks

There are still many things policyholders can do to obtain optimal coverage for cybersecurity regulatory risks. First, companies can better protect themselves from regulatory challenges in the first instance by prioritizing how to prevent and mitigate cyber and privacy risks and costs. According to IBM’s Cost of Data Breach Report 2023, the average cost of a data breach in 2023 was $4.45 million. Companies can proactively

protect themselves by conducting routine employee training, regular security audits and assessments, and by developing a strong incident response plan. Along the same lines, companies should keep apprised of evolving regulatory requirements to make sure they remain in compliance.

Reviewing and Enhancing Cyber Insurance Policies

Second, companies should carefully review their current cyber policies to identify gaps and ensure that they have coverage for their increased exposures resulting from regulatory rules. There is little standardization across the cyber insurance industry, and the language used in a particular policy will define the scope of coverage as well as exclusions and limitations. Companies should then seek adequate additional coverage as necessary. For example, affirmative coverage for wrongful collection may be particularly important given the ever-expanding regulatory landscape governing the collection of consumer data. This could include coverage for damages resulting from the wrongful collection of personal or confidential information (regardless of whether a cyber-security event contributed to such alleged wrongful collection).

Coverage for Executives and Regulatory Compliance

Additionally, given the SEC's new requirements concerning the disclosure of risk management practices and governance structures, coverage specific to a company's executives may be necessary. Some policies may affirmatively cover claims alleging executives failed to fulfill their cybersecurity roles. While some cyber policies often cover assessments of fines and penalties in investigations and adversarial proceedings involving the Federal Communication Commission and Federal Trade Commission, they may exclude coverage for securities claims. Seeking affirmative coverage for SEC compliance may be beneficial. We may see new policy endorsements introduced aimed towards these risks, including affirmative endorsements covering the costs associated with the updated U.S. Securities and Exchange Commission cyber-incident reporting compliance obligations, including legal fees for compliance and disclosure requirements such as the filing of an 8-K.

Proactive Measures for Incident Response

Finally, given the tight time frame for disclosing material cyber-incidents under the new SEC rules, companies need to be able to respond to cyber-events expeditiously. At the same time, some cyber insurance policies require an insured to obtain approval prior to retaining any incident response vendor or counsel. Companies should consider seeking advanced approval for incident response vendors and data privacy counsel to help minimize delays.

Email: info@cannabisriskmanager.com | Phone: +415-226-4060