PUBLICATION

Prepare for the Hack: Five Things to Keep in Mind when Shopping for Cybersecurity Insurance

Authors: Samuel Lanier Felker
October 17, 2016

When your company's confidential information ends up on the dark web, it is obviously too late to start thinking about adequate insurance coverage for the barrage of claims and expenses that are about to hit like a tidal wave. With expensive and high-profile cybersecurity breaches on the rise, we are encouraging our clients to review their insurance coverages now to make sure they are protected, if and when a hack or other cybersecurity incident occurs. It is important to understand there are significant and sizeable gaps present in traditional insurance products (e.g., the standard Commercial General Liability policy), and most insurers are now adding cyber-specific exclusions to general liability policies. Thus, there is now a tremendous and ever-expanding market for specialty cyber policies, and in today's environment, that is likely the solution you will have to seek for your cyber insurance needs.

When considering specialty coverage for cyber incidents, here are five important things to keep in mind:

1. **Coverages offered in cybersecurity policies vary greatly.** As a starting point, carefully evaluate your company's greatest risks and make sure to tailor the policy to cover your company's greatest exposures. Common types of first-party coverage include crisis management and identity theft responses, cyber extortion and malware, data asset recovery and restoration, and business interruption caused by cybersecurity events. It is also essential to understand the event that will trigger coverage, because expenses mount quickly after a breach or other cyber event and it is important to have insurance funds in place to assist with the expedited response that is often needed.
2. **Be sure to consider coverage to protect your business from third-party liability.** In addition to the damage to your own business and its network, you must also consider potential liability to third parties caused by the breach or security incident. Common third-party coverages include network security liability (claims arising from breach in network security or transmission of malware to someone else's network) and privacy liability (claims related to your failure to properly handle and protect personal or confidential information).
3. **The exclusions in cyber policies vary and can greatly affect the handling of your claim.** Common policy exceptions include ones for claims arising from unencrypted portable electronic devices, intentional acts of employees (as distinguished from negligent conduct causing the event), cyber terrorism, Acts of God and security lapses that could have been prevented. Many standard cyber policies also exclude liability that is assumed by the insured, such as through indemnity under a vendor agreement. Ultimately, it is important to recognize every exception and negotiate on the ones that are important to your business.
4. **Carefully consider policy limitations of liability and applicable retentions.** In addition to aggregate policy limits, many policies also have sub-limits that may apply for things like breach notification costs, forensic expenses, credit monitoring costs, business or network interruption and extra expenses. In addition, business or network interruption coverage may have a larger deductible or include a time element component (i.e., business or network must be down for a certain number of hours before business interruption coverage will be triggered). Also, be cognizant of suggested retention amounts, which must be paid by the company before the policy will respond to an event.

5. **Choose an insurer who will partner with you.** The cybersecurity market is extremely competitive and insurers will offer a host of "free" services along with your cyber policy. Many insurers today will "partner" with the insured prior to an event to assist with cybersecurity policies and procedures and training of employees on incident response strategies. Many insurers also provide the services of specialty vendors to assist the client with forensic investigations and remediation in the event of a cyber incident. These services and relationships can provide an added benefit to the insured and help prevent devastating cybersecurity incidents.

As this overview makes clear, the cyber liability insurance market is complex and quickly changing in today's market. For that reason, it is best to ask your attorney to review your coverages with your insurance broker to make sure you receive the protection you desire. In the event you have any questions about your cyber coverage or wish to schedule a review, contact Sam Felker, CIPP/US or one of the members of our Privacy and Information Security Team.