What to Look for in Cyber Insurance

Cyber risks are everywhere. A national retailer reported that *40 million* debit and credit cards were affected in a 2013 breach. More recently, the federal government admitted that it experienced a huge breach affecting over *20 million* individuals that involved highly sensitive information, including information from security clearance applications.

Although the foregoing statistics are jaw-dropping, it is probably tempting for small and medium-sized businesses to think they are not attractive targets. This is wishful thinking. In a May 2015 report, the Ponemon Institute reported that the average cost of data breaches affecting compromised records ranging from 5,000 to slightly less than 100,000 – hardly "mega breaches" – involved an average total cost of $6.53 million. Recent reports of vulnerabilities at manufacturing companies, utilities and even in automobiles show that almost any business is at risk.

Companies seeking to manage their cyber risks should of course be vigilant in managing their systems, implementing appropriate security policies and procedures, and engaging security experts. But if a company experiences a breach, can it expect its business insurance to respond? The answer is a firm "maybe." From the policyholder perspective, there is good news and bad news.

The good news is that some insureds have found coverage for cyber losses under their standard commercial general liability (CGL) policies. Some have successfully argued that CGL coverages – including coverages for "damages because of … 'property damage' …" and damages because of "Personal and Advertising Injury" – cover cyber-related losses.

The bad news is that the results are far from uniform. Further, insurers are rapidly moving to modify their CGL policies to exclude cyber-related claims. The Insurance Services Office (ISO) – an organization that prepares form policy language – has issued a series of highly restrictive endorsements insurers may choose to add to their CGL policies. Many insurers are also vigorously contesting cyber-related claims under CGL policies.

The insurance industry is clearly trying to force insureds to purchase cyber coverage separately, whether as an add-on to existing policies or in stand-alone policies. The good news is that over 30 insurers, including industry leaders, are offering various forms of cyber coverage, which is presently reported to be widely available for small and medium-sized companies at attractive premiums. The bad news is that there is no uniformity among cyber policies. The scope of coverage varies and the policy wording for seemingly equivalent coverage differs among carriers, making it difficult for insureds to compare offerings.

Nevertheless, cyber coverage is available for both first-party losses (losses experienced directly by the insured, such as business interruption) and third-party liabilities (claims by third parties, such as for damages resulting from the exposure of personally identifiable information (PII)). As a far from exhaustive list, the following types of coverage are currently available (although not necessarily in the same policy):

- Defense and settlement costs for claims resulting from the insured's failure to secure or allowing unauthorized access to PII or other data.
- Defense and settlement costs for claims associated with transmitting viruses or malicious code.
- Liabilities associated with a customer's inability to access or utilize the insured's hosting or similar services.
- Remediation costs following a breach, including for investigation, public relations, customer notification and credit monitoring.
- Business interruption experienced by an insured attributable to loss or denial of service.
- Costs to restore data, software or hardware.

Some cyber or related policies also include coverage for copyright infringement or other alleged intellectual property violations. Some insurers also offer risk management services to assist policyholders in avoiding losses and responding to breaches.

Although cyber coverage can be attractive, there are many potential pitfalls, some of which include:

- Most cyber coverage is written on a claims-made basis, meaning it generally covers only claims made during the policy period, or, if available, extended reporting period. Further, the broker should endeavor to obtain a reasonable "retroactive date" so that liabilities resulting from acts or omissions occurring before the policy period will cover a claim made during the policy period.
- Cyber policies, like all policies, have exclusions. Some contain an exclusion for claims resulting from the insured's failure to maintain security standards. Coverage lawyers are closely watching how this exclusion will be applied by carriers, as it potentially may completely undermine coverage. Other exclusions may also be problematic.
- Some coverages have "sub-limits," or lower policy limits, for particular types of coverage.
- Insurers may deny claims or even seek to rescind coverage based on errors in the application, so insureds and their brokers should use care in the application process.
- Because there have been very few cases decided regarding cyber policies, it is difficult

to know how the courts will react to coverage denials. This lack of precedent, coupled with the differing policy language, results in uncertainty regarding the actual scope of coverage.

A business contemplating insurance coverage for cyber-related liabilities should thus consider:

- Thoroughly reviewing potential cyber exposures with the assistance of an experienced insurance broker or agent, or other professionals. The application process may be helpful in making this assessment.
- Assessing with its advisers how possible coverage offerings fit with the perceived exposures. This will not be a perfect process, because it is difficult to predict how insurance will respond to particular claims, but the effort should be made.
- Coordinating potential cyber coverage with other business insurance. Some insurers offer “package” policies that may be attractive to some insureds.
- Asking carriers for modifications to policy language when appropriate.

One final important tip: *Never* simply accept an insurance company’s initial determination that a claim is not covered, whether under a traditional or cyber policy. Seek independent advice. Denials can often be reversed, either in negotiations with the carrier, or, if necessary, in court.

Partner, Thompson Hine LLP’s Atlanta office. John Watkins practices in the firm’s business litigation and corporate practice groups, including a focus on insurance coverage. He is also an Adjunct Professor at the University of Georgia School of Law teaching Insurance Law. This article was first published in the *Fulton County Daily Report*, September 14, 2015.