InsideCounsel

Technology: Understanding the ins-and-outs of cyber insurance

Insuring against technology risks is a young, but fast-growing field

BY DANIEL NELSON
September 28, 2012 • Reprints

The ongoing technological revolution is undeniable. What was science fiction a few years ago is now an everyday reality deployed across the business world to increase efficiency and uncover new opportunity. But, the same technologies that attract business with the promise of cost efficiencies, better margins and enhanced marketing techniques have created vast new spaces for both inadvertent mistake and criminal conduct.

While prevention is often the best cure, the daily headlines demonstrate that even the most technologically advanced companies fall prey to a myriad of technology accidents or crimes. The pervasive presence of technology, such as email, cloud-stored data and electronically transmitted payments, combined with the complexity of the systems providing these services and the rapid pace of those systems' change, unite to create an environment where accidental or intentional harm will occur despite robust caution and defense. According to the Verizon 2012 Data Breach Investigations Report, there were more than 850 reported data loss events in 2011, affecting more than 170 million records. Moreover, many experts agree that the reported losses are only a small fraction of the actual number of data loss events; for every headline-making data breach, there are thousands of smaller data breaches that go unreported.

Thus, insuring against technology risks is a young, but fast-growing field. Industry surveys indicate that, despite the economic downturn, premium dollars collected for "cyber insurance" products are growing, year-over-year, at a double-digit rate. Moreover, this growth rate likely underestimates the

growth in new policies issued, as insurers are often reducing premiums to boost the number of insureds and to enter new markets such as the smaller business segment.

The growth in cyber insurance owes much to the limits of traditional business risk policies. In response to some of the earliest court decisions construing the coverage of traditional business risk insurance for data loss events, many carriers revised their standard policies to exclude “data” from the definition of the insured’s covered property. These policy modifications, combined with the explosion of new technologies, has left a wide coverage gap between the risks many businesses face and the coverage of traditional insurance. This coverage gap, in turn, attracted those insurers willing to understand the unique risks of the cyber world and tailor coverages and associated premiums to fill the gap.

While descriptions vary, cyber insurance can fairly be described as covering several different risk categories.

- **Data breach coverage** offers protection against the expenses associated with responding to and mitigating a loss of third-party data (often consumers’ or employees’ private data), and may include coverage for expenses such as notification, credit monitoring, forensic investigation and legal advice.
- **Regulatory action coverage** may assist with costs incurred in responding to and defending against regulatory claims; some policies may pay for part of any civil penalties assessed.
- **Outage coverage** can reimburse for business interruption losses relating to system or website downtime.
- **Data loss coverage** assists with the cost of replacing the insured’s lost data.
- **Liability coverages** may also be available, including **content** coverage, for claims relating to information posted on a company’s website (including, potentially, copyright materials), and **virus** coverage for claims that the insured’s systems transmitted a virus.

Other coverages may also be available for particular risks.

Because the cyber insurance market is still young, and both new entrants and established market players continue to analyze loss experience and market opportunities, the policy offerings in the cyber insurance market vary more widely, and offer more potential for customization, than is often found in more traditional business risk lines. While this flexibility offers more opportunity for insureds to target their premium dollar, the added complexity also often requires the assistance of a specialist in the cyber insurance field to assist in identifying pertinent risks and tailoring coverages.

Regardless of if you're working with a specialized broker, certain key questions should be posed regarding any contemplated cyber insurance policy. What types of risks are covered? Does the policy cover only remediation, or does it include provisions for penalties or civil liabilities? What events trigger coverage? What types of data are covered? How are remediation costs defined? Does the carrier offer any value-added services, such as discounted remediation services like credit monitoring?

In addition to answering these key questions, careful study of all portions of the policy is critical. As underwriters become more sophisticated as to the specific risks, the possibility increases that insured-specific exclusions may be inserted that limit or deny coverage for those security risks that are the insured's weakest links.