New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 249—NO. 98
WEDNESDAY, MAY 22, 2013

CORPORATE INSURANCE LAW

Expert Analysis

Insuring Against Cyber Risks: Coverage, Exclusions, Considerations

By **Howard B. Epstein**

And **Theodore A. Keyes**

In *War Games*, the 1983 science-fiction film, Matthew Broderick stars as an unmotivated high school student who, with the help of Ally Sheedy and some other friends, unwittingly hacks into a U.S. military computer that has automated command of the United States' nuclear missile silos. Believing that he has accessed a set of advanced computer games, Broderick's character selects Global Thermonuclear War and begins playing what he believes is a simulation of the start of a nuclear war between the United States and the Soviet Union. At the risk of spoiling the ending for those who have not seen the movie, it turns out that Broderick's character may have started the real thing and he and Ally Sheedy's character spend the rest of the movie racing around to prevent the mutually assured destruction that a nuclear war would bring.

In the 30 years since *War Games* was first released, computer networks have become far more advanced. Likewise, those who are intent on hacking into computer systems have become incredibly more sophisticated. While not every network security breach poses a risk of global nuclear war, the risk of security breaches has become a serious concern for any commercial enterprise that maintains private records in digital form.

As news stories reporting the latest theft of credit card data, Social Security numbers and ATM codes have become more prevalent, the issue of cyber security has only become more important to management and investors. Computer systems security has evolved into a significant issue with such broad implications that, in 2011, the Securities and Exchange Commission issued guidance concerning disclosure obligations relating to cyber risks and cyber security incidents.[1] More recently, in 2013, the SEC and Commodity Futures Trading Commission (CFTC) jointly issued Identity Theft Red Flag rules which impose requirements on financial institutions and creditors to address reasonably foreseeable identify theft risks.[2]

As a result of the rise of cyber incidents and the increased focus on computer security, more insurance carriers have begun offering insurance to cover cyber risk liability. Not surprisingly, more companies are purchasing these policies, particularly those companies in the financial services, technology and health care industries.[3] While cyber risk insurance is still evolving, in this column, we take a look at some of the specific features of cyber risk liability policies based on a review of the policies available in the marketplace.

Covered Risks

Many companies maintain standard crime policies, and these policies may provide coverage for direct losses from funds stolen via computer theft, forgery or electronic fraud. These crime policies do not usually provide coverage for other cyber risks arising from stolen data, unauthorized disclosure or damages incurred due to a virus or denial of services attack. Likewise, standard general liability policies are unlikely to cover cyber risks and may, in some cases, expressly exclude those risks.

Cyber liability policies typically cover third-party claims, and some offer coverage for first-party claims as well. Third-party claims refer to those claims made against the insured alleging that the insured is liable to a third party for damages. These claims can range from suits by customers seeking damages due to disclosure of their personal data to suits by shareholders for an alleged breach of duty concerning a failure to detect or prevent a data leak. First-party claims refer to claims made by the insured to recover from the insurer damages suffered by the insured. For example, the insured may seek to recover costs for restoration of lost data following a hacking incident.

As a result of the rise of cyber incidents and the increased focus on computer security, more insurance carriers have begun offering insurance to cover cyber risk liability.

In the context of third-party claims, cyber liability policies can cover a wide range of risks. For example, policies may include coverage for third-party claims involving the following issues: (i) unauthorized disclosure, through theft, data breach or otherwise, of personal data including Social Security numbers, credit card information, banking codes or medical information; (ii) destruction of computer records or data; (iii) failure to prevent transmission of a virus or other malicious code; and (iv) failure to prevent the spread of a denial of service attack. Third-party claims can also arise out of the insured's breach of its own privacy policy or

HOWARD B. EPSTEIN *is a partner at Schulte Roth & Zabel, and* THEODORE A. KEYES *is special counsel at the firm.*

the violation of applicable privacy laws or regulations and related notice requirements.

In the context of first-party claims, cyber risk policies may cover the cost of significant expenses incurred by the insured to respond to data breaches. For example, covered first-party claims may include: (i) the costs to retain computer forensic services to determine the cause or source of the data security breach; (ii) the costs to notify impacted consumers pursuant to applicable regulations; and (iii) the costs of providing credit monitoring services. Policies may also cover business interruption damages caused by a virus or denial of services attack.

Services and Defense Costs

Many insurance carriers offer crisis management services under their directors' and officers' (D&O) liability insurance policies. In addition to providing coverage in response to claims, these D&O policies cover the costs incurred to retain the professionals necessary to help the insured navigate a crisis. For example, covered services typically include the costs of retaining a public relations firm in the event of a government investigation that might generate negative publicity or an incident that may impact the solvency of the insured. Similarly, some cyber risk policies offer coverage for the services necessary to respond to a network security breach.

Covered response services may include the costs for attorneys, computer security experts and forensic experts. Coverage may include the costs for these professionals to determine the cause or source of the security breach, determine what disclosures are legally required in connection with the breach, assist in preventing against future attacks and provide required notifications to impacted consumers. Coverage may also include the costs of credit monitoring or identity monitoring programs set up in response to the incident. In many cases, the costs of expenses for public relations and crisis management may also be covered as well as legal services concerning the insured's compliance with applicable regulations.

In the event of a third-party claim, the policies typically provide that the insurer will have the right and duty to defend and defense costs will be paid above the applicable deductible.

Exclusions

Most of the policies currently available in the marketplace do have a lengthy list of exclusions and these should be carefully reviewed before binding coverage. In many cases, the exclusions are similar to the exclusions that are standard in D&O policies.

For example, there is no coverage for claims that arise out of fraud or intentional illegal conduct, at least where a final judgment confirms that the fraud or crime did take place and at least as to those individuals who had knowledge of the events that constitute the fraud or crime. Similarly, typical exclusions bar coverage for claims arising out of antitrust or ERISA (Employee Retirement Income Security Act) violations, patent infringement, express warranties or pollution claims.

Other exclusions that may be more unique to cyber risk policies include exclusions for claims arising out of the unlawful collection of personal information, the distribution of unsolicited emails (i.e. spam) by or on behalf of the insured or claims due to the interruption or outage of Internet access caused by the Internet service provider.

Directors and officers of small businesses must be equally vigilant. In fact, according to a recent report, almost half of the confirmed data breaches that occurred in 2012 took place at companies with less than 1,000 employees.

Considerations for Directors

The guidance and rules issued by the SEC and the CFTC underscore for directors and officers the importance of addressing cyber risk issues. The Identity Theft Red Flag Rules require financial institutions and creditors to develop and implement a written program to address reasonably foreseeable identify theft risks. The rules require the direct involvement of the board of directors, a board committee or a senior management employee. While the details of the program may vary, the program must be designed to detect, prevent and mitigate identity theft.[4]

The SEC guidance makes clear that, in some circumstances, it is appropriate for companies to disclose information about specific cyber security incidents, operations that give rise to cyber security risks, potential costs and consequences and how these risks are being addressed. This discussion, in some cases, may include a description of relevant insurance coverage.

Although the stories that typically make headlines involve security breaches or cyber attacks on large companies, directors and officers of small businesses must be equally vigilant. In fact, according to a recent report, almost half of the confirmed data breaches that occurred in 2012 took place at companies with less than 1,000 employees.[5] For these small companies, insurance may be even more critical, because they may otherwise lack the resources to recover from a data breach.

Small companies may also lack the expertise and the resources to properly protect against cyber attacks. This is another area that insurance may be useful. The underwriters of cyber risk liability insurance have expertise in network security, and it is in their interest to make sure that their insureds have secure systems. Consequently, while going through the underwriting process, small companies may learn valuable lessons about the protections and policies that they can put in place to reduce their risks.[6]

Looking Forward

Computer technology has come a long way since the oversized computer that took up the whole wall of the large war room in *War Games*. In fact, Google only recently announced the release of a test version of Google Glass, a wearable glasses-like computer device that is sure to raise its own privacy and security concerns.

There is a growing recognition in government and in the business world of the need to upgrade computer systems security. As technology products become more advanced and more accessible, we can anticipate that cyber attacks will continue to become more prevalent. Insurance products that address these cyber risks are still evolving. However, for directors and officers seeking to address these risks, these insurance products should be part of the equation.

1. CF Disclosure Guidance: Topic No. 2, U.S. Securities and Exchange Commission, Division of Corporate Finance (Oct. 13, 2011); http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

2. 17 CFR Part 162 and 17 CFR Part 248.

3. Provost, Taylor, "Should You Consider Cyber-Liability Insurance?" (April 24, 2013) http://www3.cfo.com/Print/PrintArticle?pageId=e806ca61-9682-4436-8046-653789ca2bd7

4. Bailey, Dan. "Cyber Risks: New Focus for Directors" (The D&O Diary, Feb. 20, 2013) http://www.dandodiary.com

5. Bortnick, Richard J., "Cyber Security and Data Breaches—Why Directors and Officers Should Be Concerned" (The D&O Diary, Sept. 11, 2012) http://www.dandodiary.com

6. Provost, Taylor, "Should You Consider Cyber-Liability Insurance?" (April 24, 2013) http://www3.cfo.com/Print/PrintArticle?pageId=e806ca61-9682-4436-8046-653789ca2bd7