New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 17
MONDAY, JULY 27, 2015

Corporate Insurance Law

Expert Analysis

Cyber-Risk Insurance Update: Claims Increase and Policies Evolve

By **Howard B. Epstein**

And **Theodore A. Keyes**

What do the U.S. Office of Personnel Management, Target, Anthem, Sony, P.F. Chang's and the State Department have in common? It's an easy question, if you have been paying attention. In recent months, each has been the subject of a cybersecurity attack or data breach.

We first covered the topic of cyber-risk insurance in a column published here two years ago.[1] At the time, we wrote that news stories reporting the latest theft of credit card data, Social Security numbers and ATM codes had become more prevalent. Since then, however, the rate of data breaches and related disclosures has only increased and the organizations identified above, unfortunately, represent merely a few high-profile examples culled from an ever-growing list. In fact, if recent news reports are correct, we may soon be adding the Houston Astros to the list.

Cyber-risk concerns initially appeared to be primarily confined to retailers, banks, credit card companies and other businesses that maintain large volumes of personally identifiable information (PII). Today, the risks are even more widespread. Companies that maintain PII or other sensitive records on a network or that conduct business online have addressed (or should address) these risks through privacy policies, employee training, incident response plans, contractual protections with vendors, and network security technology. Given the ever-increasing sophistication of hackers, however, it is unlikely that such policies, procedures, and contractual provisions will be sufficient to entirely eliminate the risk of a data breach. Consequently, companies should also consider whether cyber-risk insurance should be part of their risk management approach.

> Over the last few years, cyber-risk insurance products have evolved so that coverage is now available for cyber-risk exposures related to third-party claims as well as for first-party loss.

Over the last few years, cyber-risk insurance products have evolved so that coverage is now available for cyber-risk exposures related to third-party claims as well as for first-party loss. In addition, some policies provide insureds with access to experienced service providers who can help the insured respond to a data breach crisis and can also assist the insured with regard to preventative risk management and loss-control activities.

Government Guidance

Although the United States has no comprehensive privacy and security legislation, various federal and state laws require implementation of cybersecurity measures and several government agencies, including the Federal Trade Commission (FTC), Federal Communications Commission (FCC), the Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC), as well as the attorney generals of several states, have increasingly engaged in related enforcement activity.

In February 2013, President Barack Obama issued an executive order which cited the need for improved cybersecurity to address repeated intrusions and threats to infrastructure in the United States.[2] The executive order directed the National Institute of Standards and Technology (NIST) to develop a framework to reduce cyber risks. About a year later, in February 2014, the NIST Cybersecurity Framework was published.[3]

The heart of the Cybersecurity Framework is the Framework Core, which emphasizes activities to identify, protect, detect, respond and recover from a cyber attack. The Framework Core and similar principles have formed the basis of cybersecurity guidance issued by other government agencies or associations, including the SEC and the International Organization for Standardization (ISO).

For example, in April 2014, in connection with the announcement that it would be conducting an examination of

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

registered broker-dealers and investment advisers with regard to cybersecurity issues, the SEC's Office of Compliance Inspections and Examinations issued a sample cybersecurity document request and a risk alert that addressed the following cybersecurity principles and issues: (i) cybersecurity governance; (ii) identification and assessment of cybersecurity risks; (iii) protection of networks and information; (iv) risks associated with remote customer access and fund transfer requests; (v) risk associated with vendors and third parties with access to the firm's networks or data; (vi) detection of unauthorized activity; (vii) experience with cybersecurity threats; and (viii) cyber-risk insurance.[4]

The SEC followed up with a guidance update, issued in May 2015, which set forth three steps for investment advisers and funds to consider in addressing cyber risks: (i) assessment of threats; (ii) design of a strategy to prevent, detect and respond to cybersecurity threats; and (iii) implementation of the strategy through policies, procedures, training and education.[5]

Liability and Crime Policies

In the event that risk management policies and procedures are unsuccessful in preventing a data breach, the existence of an insurance policy may mitigate some losses and expenses associated with the breach. While standard crime policies or fidelity bonds may provide coverage for direct losses from funds stolen via computer theft, forgery or electronic fraud, these policies typically do not provide coverage for claims and losses due to stolen data or PII, unauthorized disclosure, or a denial of services attack.

General liability policies, which typically provide coverage only for damages arising from an occurrence that results in bodily injury or property damage, are also unlikely to extend coverage to data breach loss. Some insureds have sought coverage for data breach losses under the personal and advertising liability coverage section of their general liability policies. These claims have not met with widespread success, as courts have found that such claims are outside the scope of coverage where there has not been publication of personal information.

For example, in *Zurich American v. Sony*, the New York State Supreme Court, New York County, ruled against Sony in connection with the Sony PlayStation data breach, finding that the activities of third-party hackers did not constitute "publication" and did not trigger personal and advertising injury coverage under the terms of Sony's general liability policy.[6] Sony appealed, but the insurance dispute was settled prior to an appellate ruling.

In a similar case, *Recall Total Information Management v. Federal Insurance*, the Connecticut Supreme Court recently ruled against the insured, affirming the Appellate Court of Connecticut's decision and holding that the loss of computer tapes containing PII of IBM employees did not trigger the general liability policies issued by Federal Insurance Company and Scottsdale Insurance Company because there was no "publication" of the information stored on the tapes.[7]

Third-party cyber-risk coverage available in the marketplace provides coverage for loss incurred by the insured, including defense costs, due to claims related to the theft, loss, or failure to protect PII or confidential business information.

Of course, these decisions have not stopped insureds from trying. A dispute between Travelers Indemnity and P.F. Chang's concerning coverage for three class action suits arising out of a data breach is pending in the U.S. District Court of the State of Connecticut.[8] Among other defenses, Travelers, like the other carriers, has argued that the general liability policies have not been triggered due to the absence of "publication."

Cyber Risk Insurance Policies

While general liability and crime policies are unlikely to provide coverage for data-breach losses, specialty cyber-risk policies present insureds with a legitimate opportunity to mitigate the loss associated with a data breach. New insurers continue to enter into this marketplace, each using its own terminology in policy forms, making it sometimes difficult to compare one policy with another. However, the better policies provide potentially valuable coverage for both first-party and third-party losses.

Third-Party Claims. In the context of data breach events, third-party claims have become a significant concern. News of a data breach event is often followed soon after by a class action lawsuit seeking damages allegedly incurred by customers. P.F. Chang's, eBay, Barnes & Noble, Target, LinkedIn, Google, Kmart, Home Depot, Anthem, Wyndham and many other companies have faced such lawsuits. These class action lawsuits often face significant obstacles, in particular with regard to standing and damages, but in certain cases these obstacles may prove less daunting.

Customer class action lawsuits are not the only risk of third-party claims. Businesses that share information or access to networks or data may bring claims against a company whose failed security efforts resulted in disclosure of confidential information or damage to their own computer systems.

Third-party cyber-risk coverage available in the marketplace provides coverage for loss incurred by the insured, including defense costs, due to claims related to the theft, loss, or failure to protect PII or confidential business information. Such coverage may include claims alleging that the insured failed to comply with its own privacy policy or to implement security practices required by law.

Coverage is also available for third-party claims based on the insured's alleged failure to prevent a cybersecurity breach that results in unauthorized access to a network, a denial of service attack, or infection of a computer system by a virus or other malicious code. Some policies also provide coverage for the defense and resolution of regulatory proceedings concerning cybersecurity and privacy law issues, including certain fines and penalties. In addition, many policies include coverage for third-party claims for libel, slander, defamation, copyright infringement and invasion of privacy rights, or other claims based on material published on a website or social media space.

First-Party Coverage. For some companies, first-party coverage may be more important than third-party coverage. First-party coverages available in the marketplace provide coverage to respond to data breach incidents. These costs can include the costs of computer experts as well as legal and crisis management professionals. For example, coverage may include the following activities in response to a data breach: (i) legal analysis of applicable laws regarding reporting and notification; (ii) computer forensics to analyze scope, extent, and cause of data breach; (iii) notification services; (iv) call center services; (v) credit or identity monitoring and protection services; and (vi) public relations and crisis management.

In addition to providing coverage for certain first-party expenses, cyber-risk policies may also give the insured access to an available roster of professionals skilled in legal, crisis management, computer, and notification issues and services. In fact, some insurers have developed a list of preferred service providers based on experience addressing data breach claims. In some cases, these or similar service providers can also be made available to the insureds to review computer systems and privacy policies in an effort to strengthen security and avoid breach.

First-party coverages may also include coverage for costs incurred to recover data and costs incurred to respond to cyber-extortion threats. In addition, coverage may include lost business income incurred during the period of time that a business is shut down due to cyber attack. This coverage may also include extra expenses incurred to minimize the lost income. Typically, this business interruption coverage is provided above a retention that is defined as a certain number of hours of interruption.

Exclusions. The cyber-risk policies that are currently available do contain a lengthy list of exclusions. These should be carefully reviewed before binding, but in many cases these exclusions are intended to limit coverage to the specialty area of cyber risk and to avoid overlapping with general liability, D&O or other insurance policies. For example, one standard exclusion bars coverage for bodily injury and property damage, which is typically covered by general liability policies. Other exclusions bar coverage for claims arising from pollution, employment practices claims, or from ERISA (Employee Retirement Income Security Act) violations.

Some of the exclusions are similar to the standard exclusions contained in D&O insurance policies. For example, cyber-risk policies will contain an exclusion for claims arising from fraud or intentional conduct and for claims filed by one insured against another insured. As claims experience increases, we can expect insurers to refine the exclusions as well as other terms and conditions of the policies.

Looking Forward

Across the spectrum, as businesses of all shapes and sizes continue to become more reliant on data stored on networks and clouds and on Internet-based commerce, cybersecurity is only going to become more important. Network security, employee training and privacy policies and procedures are a critical part of cybersecurity planning. For some businesses, cyber-risk insurance can provide an additional risk mitigation tool. In some cases, just going through the application and underwriting process can help a business identify cybersecurity issues that need to be addressed.

The available insurance products can provide valuable coverage for first-party and third-party cyber loss and can also give the insured access to expert service professionals who can provide pre-claim cybersecurity assistance as well as post-claim response services. In most cases, cyber-risk insurance is available as a separate insurance policy. However, we are beginning to see some insurers offer cyber-risk coverage sections in their D&O insurance policy forms. These coverage sections may not offer as broad coverage as a stand-alone cyber policy, but nevertheless may prove to be a viable alternative for some businesses.

1. "Insuring Against Cyber Risks: Coverage, Exclusions, Considerations," NYLJ, Volume 249-No. 98 (May 22, 2013).
2. Exec. Order No. 13636, Federal Register, Volume 78, No. 33, 11739 -11744 (Feb. 19, 2013).
3. http://www.nist.gov/cyberframework/
4. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Risk Alert: OCIE Cybersecurity Initiative (April 15, 2014).
5. Securities and Exchange Commission, Division of Investment Management, IM Guidance Update (April 2015), No. 2015-02, "Cybersecurity Guidance."
6. *Zurich American Insurance v. Sony*, 2014 WL 3253541 (N.Y. County Feb. 24, 2014).
7. *Recall Total Information Management, Inc. v. Federal Insurance Co.*, 2015 WL 2371957 (Conn. May 26, 2015).
8. *Travelers Indemnity Company of Connecticut v. P.F. Chang's China Bistro*, No. 3:14-cv-01458-VLB (D. Conn.).

Schulte Roth&Zabel

Schulte Roth & Zabel LLP
919 Third Avenue, New York, NY 10022
212.756.2000 tel | 212.593.5955 fax | www.srz.com
New York | Washington DC | London