Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity Insurance

Every business, regardless of its size, structure, industry and security measures, will, at some point, be the victim of a data security breach. Coverage for all costs incurred in connection with an actual or suspected data security breach, however, is not automatic. Although policy language will undoubtedly be updated over time to better address such issues, insureds and insurers should take certain steps in the interim to protect their interests, the author writes.

Think Fast: The Potential for Tension Between Insureds and Data Security Insurers

BY PAUL JANOWICZ

Like ''death'' and ''taxes,'' there are two inescapable certainties in the world of data security. First, a breach is inevitable. That is, every business, regardless of its size, structure, industry and security measures, will, at some point, be the victim of a data security breach (for the purpose of this article, the term ''data security breach'' means any unauthorized event, or suspected event, that violates a business's security and privacy policies and/or applicable laws). *See, e.g.*, Larry Kunin, *Data Security: It's Not a Matter of If, but When . . .* , MORRIS, MANNING & MARTIN LLP (Dec. 4, 2015); Kevin Cunningham, *The Data Breach Question: No Longer an ''If'' but ''When''*, SAILPOINT (Oct. 13, 2015). Second, a data security breach can be astronomically expensive. Last year, the average total cost of a data security breach was $4 million and the average cost per record was $158. PONEMON INSTITUTE, 2016 COST OF DATA BREACH STUDY 2–3 (June 2016). Those totals include, for example, the costs to investigate data security breaches, repair affected systems, notify affected consumers, manage public relations and defend lawsuits.

Paul Janowicz is an associate at Tucker Ellis LLP in Cleveland and is a member of the firm's Privacy & Data Security Group.

When you consider the inevitability of a breach and the high costs involved, it is no wonder why so many insurance providers have introduced specialty ''Data Security'' policies over the past few years (depending on the insurer, the coverage may also be referred to as ''Cyber Security,'' ''Cyber Risk,'' ''Data Breach and Network Protection,'' ''Security and Privacy Protection'' or one of many other names). The demand could not be higher and, until recently, the supply of such risk-specific insurance coverage was limited.

While the data security coverage are undoubtedly a welcomed form of risk relief, the newly-introduced policies contain coverage grey areas and a notable lack of uniform language. Consequently, insureds should avoid viewing their new policies as automatically covering all expenses connected with any data security breach. On the other side of the equation, insurers must take extra caution to ensure they fulfill their obligations to work

 ISSN 1538-3423

with their insureds in ''good faith'' when evaluating whether coverage exists under the plain and unambiguous terms of their policies.

Data Security Policies—A Brief Overview

Generally speaking, many of the data security form policies presently on the market follow similar formulas. They include several insuring provisions, each designed to address a specific data security risk and the losses associated with that risk, and further outline the coverage available through the use of specific exclusions and definitions set out in the policy. In any data security policy, you will likely see coverage provisions for:

- ''Privacy breaches'' (i.e. the unauthorized access of private information). Insuring provisions for ''privacy breaches'' typically provide coverage for ''breach costs'' incurred in connection with a known, and not merely a suspected ''privacy breach.'' Covered ''breach costs'' generally include, among other things, (1) the investigation into the cause of the breach, (2) breach notifications, as required by state and federal law, (3) credit monitoring services for affected individuals, (4) the cost to set up a call center to field questions regarding the breach and (5) defense costs, if necessary. ''Breach costs,'' however, are usually covered only to the extent they are ''reasonable and necessary'' under the circumstances.

- ''Network interruptions'' (i.e. a situation where a business's computer or network is temporarily shut down). Insuring provisions for ''network interruptions'' typically provide coverage for (1) lost income, (2) expenses to restore the system and, potentially, (3) certain operating expenses.

- ''Cyber extortion'' (i.e. an attack or threat of attack combined with a demand for money to stop or avert the attack). Insuring provisions for ''cyber extortion'' typically provide coverage for (1) costs to investigate the threat and (2) money paid to end the threat. The insuring provisions typically require the insurer's approval for any payment.

While the insuring provisions, definitions and exclusions in available data security policies cover an extensive amount of ground, whether coverage exists is not always clear-cut. Moreover, the number of decisions an insured must make to respond to a data security breach (each requiring its own coverage analysis) and the limited amount of time the insured has to make those decisions can create a unique challenges for insurers when they are asked to make their coverage decisions quickly.

While the insuring provisions, definitions and exclusions in available data security policies cover an extensive amount of ground, whether coverage exists is not always clear-cut.

The Potential for Disputes—A Few Examples

It is easy to envision situations where an insured and insurer may disagree on the coverage available for a data security breach, with each having legal and factual support for their respective positions. The following examples highlight only a few of those potential scenarios (without commenting on the likelihood that an insurer would make a certain coverage determination).

Situation One—Proactive Credit Monitoring Offers

An insured's employee loses an unencrypted flash drive that contains electronic records for tens of thousands of customers, including credit card numbers and other sensitive information. As a result of the incident, and in accordance with applicable notification laws, the insured prepares a written notice of the incident to send to customers whose information was on the drive. In its notice, which must be sent out mere weeks following the incident, the insured also intends to offer two years of credit monitoring services (at a cost of roughly $150–250 per person, per year) as a way to maintain goodwill and, potentially, limit the likelihood of lawsuits, including class actions. *See Identify Theft Protection Reviews & Prices*, NEXTADVISOR, (last visited July 11, 2016). The insured requests coverage for the costs associated with preparing and sending the notices as well as the credit monitoring under its ''privacy breach'' insuring provision.

The insurer agrees to provide coverage for the notices questions whether coverage exists for the credit monitoring services, as it is unclear whether such costs are ''reasonable and necessary'' since there are no known reports of identity theft following the loss of the flash drive. The insurer also wants to know if it would be more reasonable to withhold the offer unless and until the customers make a demand or initiate litigation.

Situation Two—Payments Without Consent

The quick decisions insureds must make to respond to a data security breach will require insurers to work diligently to ensure they fulfill their duty to act in good faith.

A cyber extortionist gains access to an insured's computer system, including confidential documents stored

  PVLR ISSN 1538-3423

on the system. The extortionist contacts the insured's chief executive officer and threatens to post the confidential documents on the internet in one hour unless the insured wires $5,000 to a specified account. The CEO believes the release of the documents could irreparably harm the company, immediately pays the $5,000, and subsequently notifies and seeks reimbursement from its insurer.

The insurer questions whether coverage exists because, under the terms of the policy, only amounts paid to end cyber extortion threats with the insurer's consent are covered. Given the extortionist's short time limit, the insured understands why the CEO paid the $5,000. At the same time, the policy provisions are clear and unambiguous.

Situation Three—Coverage for a Potential Breach

The insured uses a third-party administrator to manage its employee retirement accounts and learns that the third-party administrator was hacked two months ago, resulting in the exposure of some, but not all of the third-party administrator's electronic records. Given the millions of records in its possession and the complexity of the breach, the third-party administrator believes it may take several more months to determine precisely which records were exposed. Out of caution, and recognizing it *may* have an obligation to provide notice of the breach under state and federal laws, the insured intends to immediately send out a notice of the incident to its employees, inform them of the situation, and explain why the notice is being provided two months after the breach. The insured subsequently seeks coverage for the notice and related expenses under its ''privacy breach'' provision.

The insurer questions whether coverage exists for the notice because, given the known facts, it is unclear whether the insured actually has a legal obligation to provide the notices. The insurer also notes that the third-party administrator agreed to distribute necessary notices of any breaches in its contract with the insured.

The Insurer's Duty of Good Faith

The quick decisions insureds must make to respond to a data security breach will require insurers to work diligently to ensure they fulfill their duty to act in ''good faith.'' The duty of good faith is one that exists in every insurance contract. The duty requires insurers to only make coverage decisions after a fair ''consideration of the insured's interests and based upon adequate information . . . [;]'' insurers must perform their duties honestly, intelligently and objectively. 14 COUCH ON INSURANCE § 198:6 (3d ed. 2016). While insurers may have months to complete an investigation and coverage analysis in other contexts, insureds have little time to respond to data security breaches and could very well demand coverage determinations before taking action and incurring expenses. Insurers must be prepared to act quickly as well.

Given the data security risks businesses now face, data security insurance is quickly becoming a necessity.

If insurers are caught unprepared, they could face an increased likelihood of bad faith claims, including the accompanying potential for punitive damages or other enhanced damages. Id. at § 204:40. ''If the insurer's conduct is wholly contrary to those notions implied by good faith, then it may be considered bad faith conduct.'' *Id.* ''Certain jurisdictions have held that an insurer which unreasonably and in bad faith withholds policy benefits is liable in tort for the breach of its duties, and the insured would be able to recover tort damages. The tort may be based on interference with property rights, unreasonable or malicious conduct, or the tort may be based in a violation of the duty of good faith implied in law.'' Id. at § 204:15. To avoid such claims, insurers must be prepared to show their coverage analysis was correct or, at the very least, that whether coverage existed was ''fairly debatable.'' *Id.* at § 204:28.

Conclusion

Given the data security risks businesses now face, data security insurance is quickly becoming a necessity. Coverage for all costs incurred in connection with an actual or suspected data security breach, however, is not automatic. Indeed, certain types of claims are not covered under the plain language of the policy while others fall into grey areas. While policy language will undoubtedly be updated over time to better address such issues, insureds and insurers should take certain steps in the interim to protect their interests.

1. **Review Policy Language.** Like any other contract, the coverage available under a data security insurance policy is governed by its express terms. Insureds should review their policies to determine what risks are covered, when they need their insurer's approval prior to paying costs and what exclusions may bar coverage. Insurers should similarly review and update policy language on a regular basis to clarify any potential ambiguities and address newly discovered risks and issues and work with agents and brokers to ensure insurers understand the scope of the coverage they are buying.
2. **Be Prepared**. All insureds should have a data security breach response plan in place and, if possible, provide a copy of the plan to their insurers. Similarly, insurers should review their coverage evaluation procedures to ensure they can successfully provide the type of immediate, well-thought-out responses to data security breach coverage questions their insureds may demand, recognizing the limited window of time their insureds have to act following a breach.
3. **Maintain Open Lines of Communication.** Insureds should provide immediate notice of any

suspected data security breach to their insurers and provide continuous updates regarding the steps they intend to take to address the breach. Similarly, insurers should provide their insureds with ongoing updates regarding their coverage analysis and, to the extent possible, ensure the insured understands and does not dispute the coverage decisions.

   ISSN 1538-3423