Bloomberg BNA

Privacy & Security Law Report®

VOL. 14, NO. 24 1077-1079 JUNE 15, 2015

Cybersecurity

Views on Cybersecurity Insurance Coverage From Maria Quintero of Hinshaw & Culbertson

Hacking attacks and other data breaches have made cybersecurity insurance a hot topic, with companies looking for a backstop to their data security efforts.

Bloomberg BNA Managing Editor for Privacy & Data Security News Donald G. Aplin posed a series of questions about cybersecurity insurance to Maria Quintero, a partner at Hinshaw & Culbertson LLP, in San Francisco.

BLOOMBERG BNA: Are companies lagging in recognizing the value of their data assets and the possible need to insure them?

Quintero: Many companies recognize the value of data assets but nevertheless underestimate the risks of data breaches and the costs to remedy these events. There are a number of reasons for the lack of appreciation of the risks involved.

Senior managers and officers often aren't engaged in cybersecurity decisions but instead regard data security as an information technology issue. Until senior management becomes invested, companies may not recognize data management and security as an enterprise risk management issue as opposed to just an IT problem. As with any enterprise risk, insurance should be an integral component of the company's risk assessment.

Companies are overly optimistic about the time to identify intrusions and address any damage the attack caused. Many respondents to a recent survey estimated that attacks could be identified in hours. As breaches at Target Corp. and Verizon Communications Inc. have shown, identifying a cyberattack can take months or even years, and fixing the problem could take just as long.

Perceptions might be changing in light of the well-publicized data breaches involving banks and major retailers. But massive breaches involving tens of millions or hundreds of millions of records skew perceptions of risk as well.

Because most companies don't maintain records on a Target or Sony Corp. scale, these smaller companies might consider themselves to be unlikely targets of a

 ISSN 1538-3423

cyberattack. This reflects a misunderstanding of the types of risks most companies actually face. The risks are both internal and external. Although the threat of an external cyberattack is real, the majority of data breaches result from other sources, such as employee negligence, a lost or stolen device or vendor mistakes. These are common risks that all companies face regardless of size.

And even a small breach or error could be more expensive than most people think. In one breach, an online vendor discovered that the personal data of approximately 3,500 customers had been compromised. Despite the relatively small scale of the breach, the company reportedly lost $200,000 through breach notification costs, forensic costs and lost sales.

BLOOMBERG BNA: In the developing cybersecurity insurance marketplace, what factors may be preventing companies from obtaining coverage?

Quintero: One of the major factors in the past that prevented companies from obtaining coverage was access to the coverage. Not so any more. There are over 50 major insurance providers that offer cyber-liability insurance coverage. This is a huge jump from just a few years ago. Companies now have access to a broad array of products, but many companies still don't understand the need to purchase it.

For those companies that do recognize the need for cybersecurity insurance, two major factors preventing them from obtaining it are the absence of or inadequacy of a risk prevention or management program and premium cost.

Many companies, especially those that aren't in the retail, financial or medical industry, haven't developed programs to minimize the threat of loss or even have procedures in place to respond to a loss. Insurance companies want to see that a company is actively trying to prevent loss, and the majority of insurance companies will not cover a business without at least a risk prevention program at some level in place.

The lack of standardized cybersecurity best practices to minimize the threat of loss has contributed to a failure to establish or implement a cybersecurity risk management program. In 2014, however, the National Institute of Standards and Technology developed the Framework for Improving Critical Infrastructure Cybersecurity, consisting of voluntary standards, guidelines and practices to manage and reduce cybersecurity risk (13 PVLR 281, 2/17/14).

Although the framework was initially addressed for companies essential to the nation's infrastructure, it is now being promoted to help companies both large and small achieve effective cybersecurity risk management. A company's participation in the framework will help make it a more attractive risk to a cyber-liability carrier, and may earn the company a preferred premium rate.

BLOOMBERG BNA: From the perspective of a data breach, are there cybersecurity insurance options specifically designed to help defray the notification and remediation costs of a breach?

Quintero: Federal and state laws generally require companies to provide consumer notice if they determine that misuse of consumer information has occurred or is reasonably possible. A typical cyber-liability policy will cover these data breach notification costs, which can be substantial.

As required by law, data breach notices recommend that affected consumers take steps to monitor their credit. The notifying company might not have an obligation to pay for these credit monitoring services. However, to mitigate reputational harm from a data breach, many companies offer credit monitoring free of charge. Cybersecurity insurance can help cover this cost.

Due to notification and reporting requirements, knowledge of a data breach quickly becomes public. This often results in litigation. A cyber-liability policy would cover defense costs and damages arising from these lawsuits, including harm from identity theft or some other wrongdoing.

A data breach can also cause direct harm to the policyholder itself. The company could incur costs repairing or restoring data, as well as forensic costs to determine the source of the attack, assess the scope of damage and repair any damaged or infected software. Depending upon policy language, a cybersecurity policy could help defray these costs as well.

Cybersecurity policies tend to offer targeted coverages for discrete harms. And unlike commercial general liability policies, which tend to use standard forms, each insurer uses its own terms and classifications for describing the risks being covered. Because cybersecurity coverages are compartmentalized and each insurer uses unique forms, firms should scrutinize the risks they face and ensure that their cyber policies actually cover those potential losses.

BLOOMBERG BNA: Are there privacy and/or data security procedures or policies that companies should ensure are in place before contacting insurers?

Quintero: No specific procedures or policies apply to all companies. The recommended data security will vary depending upon nature of the business and its data.

Of course, the better the company's data management, the lower its premiums are likely to be. Depending upon the policyholder's sophistication with respect to data management, insurers also might be willing to waive certain policy conditions—such as a requirement that the data breach begin during the policy period.

As a few basic precautions, all data stored on portable devices such as thumb drives and laptops should be encrypted. Companies should limit access to sensitive information, use strong password protocols, install firewalls and of course regularly install security patches.

  PVLR ISSN 1538-3423

Retailers should consider upgrading their point-of-sale terminals so that they are chip-enabled. At the very least, companies should encrypt payment card data, ideally from the point of capture until the completion of transaction authorization.

BLOOMBERG BNA: Are we at the tipping point for making the case to obtain cybersecurity insurance coverage within the corporate risk analysis that underlies most data security and privacy compliance issues?

Quintero: If the trend of an increased availability and accessibility to cyber-insuranceproducts continues, companies without cyber insurance will be the exception. Companies providing health, financial, communications and retail services, among others, already understand the necessity of cybersecurity insurance coverage and have integrated that risk management as well as premium cost into their business structure.

With more comprehensive cybersecurity guidelines and standards in place, there should be no obstacle to integrating cybersecurity risk management with a company's broader risk management processes. This integration will better allow for the identification of risk, communication regarding that risk and the development of cost-effective risk management programs.

Given the efficiency that can be achieved, as well as the protection of the business as a whole, we are certainly at the tipping point, if not beyond it, for making the case to obtain cybersecurity insurance.

Ms. Quintero thanks her colleague Travis Wall, a partner at Hinshaw & Culbertson in San Francisco, for his assistance in preparing her answers.