

Data breach at Epsilon underscores key cyber risk

By Judy Greenwald

11 April 2011

Business Insurance

Companies received another wake-up call about the dangers of data breaches when hackers obtained the names and email addresses of customers of dozens of businesses, but observers say the companies involved are handling the situation well.

It still is unknown how the March 30 breach involving data maintained by Dallas-based Epsilon Data Management L.L.C. was accomplished; how much damage will result; and what parties, if any, will be held liable.

Epsilon said only 2% of its database had been invaded, but dozens of major companies across a variety of industries responded by emailing their customers to notify them of the breach. The companies include Citigroup Inc., Capital One Financial Corp., JPMorgan Chase & Co., 1-800-Flowers.com Inc., Best Buy Co. Inc., L.L. Bean Inc. and Target Corp.

Observers say the most likely danger from the breach is “phishing” attacks, where hackers send emails to company customers in an effort to obtain financial and other personal data.

A “phishing” email “really does appear to be coming from your bank or from a hotel chain that you do business with,” said Alan E. Brill, Secaucus, N.J.-based managing director for Kroll Ontrack Inc., a unit of Kroll Inc.

Data from San Diego-based Identity Theft Resource Center, which tracks this information, indicates the scope of the problem. In 2010, there were 662 data breaches that exposed 16.2 million records. The center defines a breach as an event where individuals' names plus personal information such as a Social Security number is potentially put at risk, which would not include the Epsilon incident.

Steps to take

Experts say there is no guarantee that online data can be kept secure, but there are steps firms can take to mitigate such risks, including purchasing cyber insurance and making sure firms that store their data have up-to-date security in place.

“Data breaches generally represent enormous problems for companies,” said Alan N. Situn, a shareholder with law firm Greenberg Traurig L.L.P. in New York. “Not only can they be very expensive, but equally important to many companies (is) the reputational damage that they perceive from these types of breaches” if information they provide to a third party is somehow breached.

For the most part, the companies that are affected are in a damage- or crisis-management mode, said Robert J. Scott, managing partner with law firm Scott & Scott L.L.P. in Dallas. “They’re emailing their customers; they’re apologizing for the inconvenience, trying to clarify and limit the scope of the magnitude of the problem; and they’re hopeful the leakage of the email doesn’t result” in other problems.

Observers noted that the firms were notifying customers of the data breach even though they were not legally required to do so by state laws, except in North Dakota, unless more damaging personal information, such as Social Security or credit card numbers, had been revealed.

Given that only email addresses were obtained, “It’s a relatively painless wake-up call for a lot of companies as to the risk associated with outsourcing aspects of your data or your system,” said Robert Parisi, New York-based senior vp with brokerage Marsh Inc.

Epsilon customers whose data was breached have been “doing everything they should be doing in terms of being up front and honest with the consumers,” Mr. Scott said.

Observers say it is premature to conclude Epsilon bears any fault for the breach, or whether there is more its clients could have done. "No one is in a position to know that, and to reach a conclusion at this point," said Joseph J. Lazzarotti, a partner with law firm Jackson Lewis L.L.P. in White Plains, N.Y. Observers say criminal hackers are notoriously nimble in keeping one step ahead of firms' security measures.

Phishing, if not now, then later, is a major concern. Hackers tend to hold on to such information "usually about a year, and then use it in the hope that folks have become a little bit more relaxed and not as vigilant," said Mauricio F. Paez, a partner with law firm Jones Day in New York.

If the breach results in litigation, the question will arise of "how does that fit into the overall risk management program of the company" that hired the outside marketing company, said Kroll Ontrack's Mr. Brill, who suggested that affected firms review their risk management programs now.

Mr. Parisi said Epsilon clients with robust cyber liability policies will find coverage under the vicarious liability provisions. It also is possible Epsilon has a professional liability policy that may respond if its corporate clients make a claim against the company, he said.

Epsilon said in a statement that it is conducting an ongoing investigation.

Leaders of the House Committee on Energy and Commerce's Subcommittee on Commerce, Manufacturing and Trade, sent the president and CEO of Epsilon's parent company a letter asking questions about the breach.

Experts say there are lessons to be learned from the situation.

"There is a tendency to look at these sorts of marketing arrangements as presenting a lower level of risk," said Michael R. Overly, a partner with law firm Foley & Lardner L.L.P. in Los Angeles. But companies should look at agreements with these firms "just as carefully as they would any agreements where they're putting sensitive information at risk."

Firms should revisit their data breach response plans and ensure their vendor's management protocols and procedures are up to date, said Jennifer Smith, Washington-based vp and technology, media and telecom practice leader at Lockton Cos. L.L.C.

Companies that contract with marketing firms should find out how they store data, if it is encrypted, and if they have had an independent security review, said Mr. Brill.

The contract also should provide for immediate notification of client companies if there is a breach so they can take damage-control measures, Mr. Overly said, observing that Epsilon acted "very responsibly" in this case.

Insurance available

Dozens of markets offer cyber insurance coverage, experts say.

"There are no standard policies. They are highly manuscripted and vary from underwriter to underwriter," Ms. Smith said.

"Theoretically, there's capacity for up to \$300 million" of coverage, with "more than enough capacity for anyone who wants to buy it" in a competitive market, Mr. Parisi said.

Experts recommend firms should be sure to cover themselves, and make sure their vendors have cyber liability insurance as well.

"Make sure that they have coverage, that it isn't illusory," said Peter S. Vogel, a partner with law firm Gardere Wynne Sewell L.L.P. in Dallas.

Mr. Paez said he always advises clients to be “very specific about who’s ultimately liable for the cost and damages incurred by the company and its customers arising from this type of data security breach.”