

Plan ahead to tackle data breaches

Response strategy should be in place before problems arise

Posted On: Sep. 18, 2011 6:00 AM CST



Judy Greenwald (mailto:jgreenwald@BusinessInsurance.com)

ADVERTISEMENT



Establishing a data breach response plan before a problem occurs will help firms navigate the delicate issue of when they should inform those affected by a breach.

Businesses “should have an incident response/breach response plan in place where all the players are clearly defined, and where they could act quickly and efficiently to contain the harm...and to gather all the facts quickly and offer appropriate remediation services, whether it's credit monitoring or identify theft,” said Jon A. Neiditz, a partner with law firm Nelson Mullins Riley & Scarborough L.L.P. in Atlanta.

“It's very helpful for companies to have an incident response plan, because the timing requirements of

doing this as soon as reasonably practical are pretty tight,” said Aaron P. Simpson, a partner with Hunton & Williams L.L.P. in New York. Getting the right people “who can remediate appropriately and in a timely manner is very important,” he said.

“The faster a company can act in response to a breach, the better it will be able to assess what needs to be done” and the more responsive it will be “to the needs of law enforcement, the desire of its customers to be able to protect themselves and the other factors that are involved in any data breach,” according to John Doernberg, a vp at William Gallagher Associates Insurance Brokers Inc. in Boston.

Mr. Neiditz said it is important to “contain the potential harm” as quickly as possible and form a “coherent and reliable narrative” in notifying those affected.

However, “if you are only part of the way through gathering the facts and you notify, you can get yourself in a lot of trouble,” Mr. Neiditz said.

Alex Ricardo, New York-based director of breach response services at Beazley P.L.C., said firms might need to do a forensic investigation depending on the nature of the data breach.

With certain breaches in particular—such as a lost laptop, lost portable device or malware—the ability to do a forensic investigation “is certainly valuable” to confirm not only that a data breach occurred but also to define those affected, which could reduce the risk of notifying too many or too few people, he said.

Scott N. Godes, of counsel at law firm Dickstein Shapiro L.L.P. in Washington, said the first thing to do when there is a data breach is “look at your insurance policies, and figure out whom you can notify and from whom you can request coverage right away.” To the extent an insurer agrees to cover the breach, “they can start providing you with resources right away,” he said.

Mr. Godes also suggested that policyholders “seek coverage under any possible policy that can provide coverage.”

However, he also had a warning.

“We've learned there's no guarantee...because no matter how you act, there's always the risk of class actions and other claims from plaintiffs,” Mr. Godes said.
