Insuring and Securing Your Data

by Joshua Gold

The risk of data theft has never been greater. Businesses, organizations and government agencies (as well as their employees) have access to huge quantities of information—some of which is not for public consumption.

Making matters more complicated for risk managers involved in safeguarding data is that improvements in bandwidth, hard drive size and wireless capabilities have permitted firms to transact business with amazing mobility. With this mobility, however, comes added risk. The volume and speed with which data can be hacked is dizzying. As such, risk managers will increasingly be called upon to ensure that these risks are addressed and minimized as best as possible.

Protecting computer data with both existing and new stand-alone insurance products is no mean feat. The insurance market for such coverage is in a continuous state of flux, and very few of the product offerings can be characterized as "customer-friendly." Purchasing coverage for catastrophic loss events at affordable premiums remains challenging.

One major pitfall of policies that are supposed to cover data involves clauses that purport to condition coverage on the absence of "errors" or "omissions" in the data security measures employed by the policyholder. Such insurance policy clauses can be exploited and disputed by insurance companies seeking to evade their coverage obligations by arguing that the policyholder was somehow derelict in safeguarding computer data from hackers, among others. Furthermore, some policies may attempt to limit insurance coverage in situations where the data breach occurs when a computer is not actively connected to a network. This can leave a serious gap in coverage. Accordingly, policyholders should work with their brokers to pick insurance policy forms that are devoid of as many coverage exclusions as possible. Not all insurance policies are created equal.

Risk managers should be working in tandem with their IT departments and in-house attorneys to protect data that is both created by the business or is entrusted to it by outside entities and individuals. One of the starting points is developing a data security protocol that establishes clear directives regarding the handling of and access to information within the organization. An important step in the process is to inventory the information possessed and determine its sensitivity. Certain categories of information call out for heightened protection, including: health information, personally identifying information of customers and employees, certain types of nonpublic financial information, trade secrets, customer lists and business processes that yield competitive advantages.

Once such information is identified for heightened protection, it is not enough to simply guard against external threats of unauthorized access. It is also important to make intelligent decisions about internal access to protected classes of information. For example, it can be risky (and unnecessary) to grant companywide access to sensitive customer information. Instead, under most circumstances, limiting the access internally to such information based upon necessity and security clearance reduces risks of unauthorized or improper disclosure of sensitive information.

Another important risk management consideration is access to and use of data from off-site locations. There should be policies specifying the types of documents that can be kept at home, as well as the permissible time period for keeping documents off-site. Additionally, the protocol should address the security of laptops used at home, on business trips and at any other remote location. Given the size of their hard drives, the theft of a laptop computer from a hotel room, office or elsewhere possesses a significant risk of unauthorized use and access to potentially sensitive information.

Developing a smart data security protocol will not eliminate the risk posed by unauthorized access to private or sensitive data but it should at least reduce it. And when the data genie does escape the bottle, risk transfer in the form of insurance coverage can hopefully soften the financial blow. ■

RISK MANAGEMENT

Reprinted with permission from *Risk Management Magazine*, November 2008 issue, page 60.