Data Security: Insurance and Risk Management Issues

By: Joshua Gold

Joshua Gold

When guests check in to their favorite hotels, they entrust more than just their jewelry, passports and luggage. They also entrust their data. Whether customers are working wirelessly, using the business center or asking the concierge or front desk to receive and transmit data for them electronically, an amazing amount of customer data is flowing through and off of the premises. Some of it is sensitive, private, and valuable.

The risk of data theft has never been greater. The cunning encompassed by hackers, viruses, spyware, malware, etc. grows exponentially each year. Data security is always in catch-up mode. Nevertheless, the risk of data theft can be minimized through prudent risk management.

Risk Management: Safeguarding Data

Risk managers should work in tandem with their IT departments and in-house attorneys to protect data that is created by the business or entrusted to it by outside entities and individuals. One starting point is developing a data security protocol establishing clear directives regarding the handling of and access to information within the organization. Virtually any hospitality firm will have its own business and employee information electronically captured. So too will it have customers' e-data, including credit card information and other information gathered upon check-in and through rewards programs.

It is important to inventory this information and determine its sensitivity. Categories hat call or heightened protection include: health information, identifying information certain types of non-public financial information, trade secrets and customer lists.

It is not enough simply toward such information against external threats of unauthorized access. It is also important to make intelligent decisions about internal access to protected classes of information. It can be risky (and unnecessary) to grant company-wide access to sensitive customer information. Limiting access to such information based upon necessity and security clearance reduces the risk of unauthorized or improper use.

Another important consideration is access to data from off-site locations. The very technology that allows increased mobility to transact business also poses an increased peril of security breaches. A smart data security protocol will address access to and handling of documents away from the premises. Additionally, the protocol should address the security of laptops used at home, on business trips and at any other remote location.

Insuring Data Security with New Insurance Products

Insurance coverage is available for losses arising from computer fraud or theft under both existing and new stand-alone insurance products. Some of this coverage is quite valuable -- but "customer-friendly."

Policy terms should be closely scrutinized. For example, a common feature of recent network security policies is a clause that purports to condition coverage on the absence of errors or omissions in the data security measures employed by the policyholder. Insurance companies may exploit such clauses by arguing that the policyholder was somehow derelict in failing to safeguard data from hackers. Some policies may further attempt to limit coverage for a data breach that occurs when a computer is not actively connected to a network. Accordingly, Policyholders should strive to select policy forms that are devoid of as many such exclusions as possible.

Data security measures coupled with risk transfer in the form of insurance coverage can serve as a financial buffer when the data genie escapes the bottle.

Joshua Gold is a shareholder in the New York office of the law firm of Anderson Kill & Olick, P.C. Mr. Gold regularly represents policyholders, including gaming and hospitality businesses, in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property insurance coverage issues. Mr. Gold can be reached at jgold@andersonkill.com or (212) 278-1886.