Liability for Data Storage and Security

By Brian A. Nettleingham

In recent months, the news has been filled with reports of data breaches, prompting growing concern among businesses regarding the liability cost of such breaches. To reduce this risk, companies must accurately assess their level of risk, implement appropriate security measures, and create quick response plans.

Liability for data breaches can arise in various ways, but the key concern for most professional service and retail companies relates to the theft of non-public personal information ("NPI"). Examples of NPI include:

- Social security numbers
- Driver's license numbers
- Birth dates
- Credit card information
- Health data

If such data is stolen or copied from a company's systems, the costs can be devastating, even absent any lawsuits brought by the affected consumers.

For example, the cost of simply notifying affected individuals can be significant. Most states have passed laws imposing specific notification requirements in the event of a data breach. Although a uniform federal law has been discussed, no national standard currently exists. Therefore, if a company's data includes information regarding individuals residing in multiple states, then the law of each state must be followed. Failure to do so can result in greater potential liability and fines.

Therefore, once a company learns of a potential data breach, it is critical to identify – as quickly as possible – the scope of the breach, so that the applicable notification laws (some of which have relatively short timelines for issuing notices) can be identified. In addition, early identification of the scope of any breach will help determine the number of individuals that need to be notified. Narrowing the list of potentially affected clients and customers not only reduces the cost of the

notification process; it also reduces the potential impact on the company's reputation and goodwill.

Companies should adopt policies and procedures that demonstrate an appropriate level of care for stored NPI. For example, employees should be trained to regularly change their passwords, not store passwords in unencrypted files (or tape them on a piece of paper near their computer), and to store NPI data only on secure systems.

Data breaches are not always the result of a sophisticated hacker in another country; they can be relatively low-tech. For example, a laptop or drive containing NPI can be stolen or lost, or a data thief might simply walk into an office and take a picture of passwords taped to the underside of a keyboard. Therefore, physical security measures must complement sound technology solutions. Because such breaches can result from vendors or subcontractors, written agreements should require that vendors protect any NPI and maintain insurance for any breach caused by the vendor.

Maddin Hauser helps its clients proactively manage potential liability for data breaches. We can help assess potential risk, assist with creating security policies and procedures, review and negotiate vendor contracts, and develop response plans. In the event of a breach, we can assist with coordinating forensic investigators and compliance with applicable notification laws. These steps, in conjunction with appropriate technology solutions and insurance coverage, can help your company mitigate the otherwise crippling cost of a data breach.