Regulatory/Law

By John Mullen

Risk Management 101

The value of customer data is recognized by all businesses. Each piece of data brings power but also risks. You can use it, sell it, update it, ignore it, even—and here's the catch—lose it.

If your business possesses personal, identifiable information such as Social Security numbers or dates of birth, customer account information such as account numbers and expiration dates, or medical records, then you have a legal duty to maintain the privacy of that information.

Businesses have a legal duty to maintain the privacy of customers' and employees' personal information.

Each week, millions of cyber attacks attempt to steal customer or employee data. The risk is greatly increased by portable devices such as Blackberry phones and laptops, which can easily be lost or stolen. Many companies allow too many employees or vendors access to sensitive information without properly protecting it. The result is data breaches, increasing exponentially. This phenomenon has caught the attention of plaintiffs' lawyers.

Lawsuits are likely to increase in the event of data loss. Plaintiffs include government entities; banks/retailers who suffered fraudulent charges or costs to replace credit cards; shareholders whose company stock value drops as a result of bad publicity; and individuals whose information is compromised. Most expensive is class action litigation. So far, plaintiffs have had a difficult time showing that sufficient damages exist to sustain a legally cognizable cause of action when data is lost or stolen. This trend is turning.

Where once plaintiffs might have simply asserted damages in the form of credit monitoring for a few years, now they will assert damages consisting of:

- average lost time per person of having to monitor credit risk (forever);
- cost of credit monitoring (forever);
- cost of private identity theft insurance (forever); and
- other creative damages

When taken individually these items may not amount to more than, let's say, $100 per year, but multiplied by a 100,000 records, that equals $10 million. That's just for one year; it's a numbers game.

While you might expect such lawsuits to be covered by insurance, many policies cover little to none of the risk involved when you experience a cyber loss. Data is not tangible under the typical commercial general liability policy and its loss is therefore not covered. For a variety of coverage reasons, other policies will probably not respond or only on a limited basis.

What can you do?

In short, pay more attention. Make data security a priority. Implement document management policies. Regularly evaluate who has access to what records, how they access them, whether they need that access, and whether access is secure. Engage third parties to complete objective, benchmark evaluations of your security risks. And buy insurance. There are products out there that cover most, if not all, of the expenses related to these matters.

Lastly, prepare by identifying the steps you will need to take should such an event happen. Do you have a public relations firm lined up? Legal counsel with specific cyber risk knowledge? Computer forensic company identified? Have you identified someone to be the focal point?

This merely touches the surface of cyber risks for companies that hold customer, or even employee, information—and there are few that don't. BR

Companies need to pay attention and make data security a priority.

John Mullen, a Best's Review *contributor, is a commercial litigation attorney and member of the law firm of Cozen O'Connor, and focuses on e-discovery, cyber risk/privacy, and construction law. He can be reached at* jmullen@cozen.com.