News and Publications

Breach Notification: Time for a Wake Up Call

By Mark G. McCreary - September 2, 2011

The scope of information that requires public disclosure in the event of a data breach is growing exponentially. For example, an email address that is verified as associated with a particular business is infinitely more valuable to phishing scammers than an email address and a guess. CIOs now have the unenviable task of discussing a broad range of data losses with legal, marketing and risk assessment professionals.

In case you haven't heard, the days of having no obligation to notify consumers of a data breach or loss that involves only email addresses may have ended. This should be a major wakeup call for every CIO.

Historically, a business and its CIO were only required to be concerned about personally identifiable information. In other words, if a business did not collect banking information, Social Security numbers, medical information or similar data, then the duty to report a breach or loss only arose in the event that the business had contractually promised its customers that it would do so.

State data breach notification laws focus almost entirely on personally identifiable information. While some states use the amorphous term “personal information,” without further definition, those statutes that do define “personal information” generally require combinations of the following in order to be covered by the breach notification statute:

- A first name or initial and last name

- Financial data
- Social Security number
- Health or genetic data

Stated another way, if your business has a list of customer names that is lost or stolen, the breach notification statutes generally do not kick in.

There is a huge gray area between losing a name and Social Security number, on the one hand, and a name only, on the other hand. For example, let's consider the loss of an email address and password for a web service. Zibingle.com is a fictitious web service where users interact by sharing messages and posting information about their social lives.

If the servers used by Zibingle.com are hacked, and the hackers make off with an unencrypted list of email addresses and passwords, there is relatively little legal obligation on the part of Zibingle.com to notify its users of the data loss. Granted, the Federal Trade Commission may get involved, and there is almost certainly a class action law firm that would commence an action, but Zibingle.com would generally be under no legal obligation to notify users of the data loss.

Despite the lack of legal obligation, the first businesses facing the situation that Zibingle.com faces realized the inherent harm arising from the loss of data that is not “personal information.” The most obvious reason to notify users is because unauthorized users could access the Zibingle.com account and impersonate the true user. Character assassination in the world of Web 2.0 is not the most pressing concern, however.

Most people not only use simple passwords, but we tend to use the same password for multiple web sites and web services. Robert, our fictional user of Zibingle.com, uses his email address as his handle: bobtheslob@majoremailprovider.com. Robert also uses the exact same password for his Zibingle.com account, his email account, his banking account and his Facebook account. Hackers with the above information now own Robert’s life, finances and spare time for the next six to 12 months while Robert tries to recover from identity theft.

Reporting the loss of email addresses and passwords may be a decided issue for business. However, those in charge of safeguarding consumer information may have noticed something a little odd about the Epsilon data theft this spring. When news of the Epsilon data breach broke, and notifications started arriving, the pendulum toward breach notification obligation made a further shift — a seismic leap, frankly.

There was no personally identifiable information involved in the Epsilon breach. There were no passwords lost and only mixed reports of any names being lost. Legally speaking, there may have been no legal obligation by Epsilon to report the loss of millions of email addresses. Only Rhode Island includes a telephone number in the definition of “personal information,” and no state includes email addresses. Practically speaking, the type of information lost by Epsilon is lost all the time by businesses with no more than a whisper, headshake or shrug.

The reasoning behind the disclosure by Epsilon -- a multichannel marketing firm -- and its customers (Epsilon’s customers were the businesses who actually owned the customer data, such as Target, JPMorgan Chase, Capital One and Walgreens) of the data theft are easy to surmise: News of the theft would have leaked out anyway. It is likely the owners of the data felt a duty to their respective customers to notify them of an increased threat of phishing attacks. An email address that is verified to be associated with a particular business is infinitely more valuable to phishing scammers than an email address and a guess.

We all receive daily emails, purportedly from a major banking institution, notifying us that we need to log into our account to confirm our information or a transaction. In the past, it was easy to ignore most of these emails because we know that we do not have a bank account at that particular institution. However, when we receive an email from the with which we actually do business, we are more likely to trust the email. We click where the email tells us to click and we are taken to a Web site that looks exactly like the bank’s Web site. We do not notice the URL at the top of the browser, and we dutifully enter our username and password. The owner of the Web site records that information, sends us to the actual bank Web site where we enter our username and password, with success this time, and we think nothing of what just happened. We complete the phishing circle of life, and we are none the wiser.

The disclosure of an email-only data theft may have changed the rules of the game forever. A number of substantial companies may have inadvertently taken legislating out of the hands of the federal and state governments. New industry pressure will be applied going forward for the loss of fairly innocuous data. This change in practice has the potential to affect every CIO who collects “contact” information from consumers, maybe even from employees in an otherwise purely commercial context.

CIOs now have the unenviable task of discussing a broad range of data losses with legal, marketing and risk assessment professionals. The loss of an unsecured smartphone, even one remotely wiped 48 hours later, may have not previously raised any eyebrows if it contained no “personal information." Now, it is arguable that a new assessment must be undertaken to see what information was on the smartphone that could lead to an association between the applicable individual and a third party. This same assessment applies to lost laptops, thumb drives and paper files. Likewise, a known network intrusion may not have raised too many concerns if the “personal information” was encrypted, but going forward there will need to be an analysis of what types of information may have been accessed.

About the author

Mark G. McCreary, a partner in the law firm of Fox Rothschild LLP, focuses on compliance with privacy-related laws, rules and regulations, as well as responses in the event of a data breach. He can be reached at 215.299.2010 or mmccreary@foxrothschild.com.