An ALM Website

CORPORATE COUNSEL

May 21, 2012

From the Experts: 10 Steps for Responding to a Corporate Data Security Breach

By David Fagan and Stephen Satterfield

Data security breaches can have significant reputational, business, and legal costs for companies. Depending on the nature and severity of the incident, a data security breach can result in the loss of key business assets, cause public embarrassment, diminish customer goodwill, result in costly response and remedial requirements (including legal obligations), create contractual liability risks, attract regulatory scrutiny at the federal and state levels, and result in litigation.

While companies can reduce the likelihood of a breach by maintaining robust data security practices and procedures, the reality is that there is no such thing as perfect security. In other words, when it comes to data breaches, the question for most businesses will be not "if," but "when." Thus, to manage risk around data breaches, businesses must also have in place procedures to guide a quick and effective response.

Although every incident is unique, these procedures generally should include the following steps:

1. Develop Your Plan Before the Incident

Develop a written incident response plan before an incident occurs, and

David Fagan

Stephen Satterfield

then create a hypothetical scenario to test the plan. Such a plan ultimately will not be a precise script for when an incident occurs, but it will help ensure preparedness—and that the right team and procedures have been identified in advance of the incident. This is important not only to help expedite a response, but also to address regulatory risks. If a breach becomes subject to regulatory scrutiny, the company will need to demonstrate that it had a reasonable plan in place to address incidents and made a good faith effort to follow that plan.

2. Assemble an Incident Response Team (IRT)

A core team of representatives from key departments should coordinate the company's response to a breach. This often will involve IT/CIO, management, business leads, and communications personnel, but it is vital that it also involve the legal department from the outset. The response should be guided by counsel to help preserve legal privileges and guard against later discovery risks.

3. Begin the Investigation Immediately

Once a potential breach is discovered, an investigation should begin immediately to determine the scope of the incident and the types of data affected.

4. Continue to Consult with Counsel

It is imperative that the investigation and response be conducted in consultation with and at the direction of counsel (whether in-house or outside counsel). In addition to preserving the privilege of confidential communications, consulting with counsel is important to the myriad legal issues—from notice obligations to coordinating with law enforcement to managing litigation risks—that can arise when investigating and responding to a data security breach.

5. Evaluate Whether to Involve Law Enforcement

When criminal activity is suspected as the cause of the breach, the company should consider contacting law enforcement. Such consultations with law enforcement may be important in determining the timing for notifying affected individuals; for example, there can be a safe harbor under certain state laws in the U.S. if notice is delayed at the request of law enforcement. Notification to law enforcement also can help create a record that the company is doing everything it can to pursue the criminals and to mitigate the incident. (For most computer hacks or other criminal breaches not involving financial fraud, the appropriate contact will be the FBI; for financial fraud, the U.S. Secret Service may be the appropriate first contact.)

6. Evaluate Whether to Engage External Consultants

For significant incidents, it may be necessary to engage a forensic consultant and/or a public relations firm. These engagements should be undertaken and supervised by counsel in order to preserve the privilege of communications between the company and its consultants.

7. Determine Notice/Remedial Obligations (Both Domestically and Internationally)

Depending on the nature of the incident and the company, the company may be legally required to notify affected individuals and regulators at the federal and state levels, or to take other remedial measures. For incidents that affect individuals outside the United States, it also may be necessary and appropriate to consult with local counsel regarding any notice or other legal obligations in the particular countries implicated by the incident.

8. Develop Internal and External Communications Strategies

For those incidents that require notice, either to internal stakeholders or to others outside the company, a company should have a well-developed communications strategy to guide its notifications and responses to questions.

9. Review Your Coverage Policies

As part of its response to an incident, a business should review its insurance policies to determine the extent to which they may cover the data security incident at issue, and to consider whether it should add coverage options to help guard against losses from cyber risks or data security breaches in the future.

10. Assess the Effectiveness of Each Response

Your IRT should review the procedures that were carried out in response to the breach and provide an after-action report that assesses the extent to which the procedures adequately prepared the company to address the incident and how the procedures should be revised or improved based on the lessons learned from the incident and response.

David Fagan is a partner at Covington & Burling LLP. His practice covers national security law, international trade and investment, and global privacy and data security. He can be reached at dfagan@cov.com.

Stephen Satterfield is an associate at Covington & Burling LLP. He counsels clients on the legal issues surrounding online marketing, social media, and other emerging digital technologies. He can be reached at ssatterfield@cov.com.