The Cost of a Breach

One breach can ruin your business, but there are ways to prevent, detect, respond to and remediate the worst cases.

Gerard M. Stegmaier
Wilson Sonsini Goodrich & Rosati

A RECENT ESTIMATE by the Ponemon Institute pegs the average cost of a large security breach at $6.3 million. Such a breach could cripple or even bankrupt a small business. Preventing security breaches and managing them when they occur have become a critical piece of every company's information governance program.

Prevention, detection, response and remediation are the critical phases in planning for a security breach. Because virtually every state has passed legislation modeled after California's security breach notification law SB 1386 — which requires custodians of personal data to notify affected parties in the event of a breach — more companies have begun to focus on these issues.

Let's start with prevention. The most common type of breach is internal. Employees may volunteer information to outside individuals when they should not, or access to company information may not be cut off when an employee is terminated. Companies can take steps to improve security by creating specific written policies that are regularly audited. Such policies often require businesses to:

- Regularly change passwords and discourage employees from choosing obvious passwords or leaving their passwords in plain sight of their computers.
- Appoint someone who has the authority to make necessary improvements and conduct unannounced tests that penetrate the company's systems and identify vulnerabilities.
- Terminate network access, including remote access, for recently discharged employees.
- Develop information use and access procedures to manage the company's data.
- Create a written incident response plan that helps the company respond systematically to security breaches.

Detection and response may be the most difficult aspects of dealing with threats to an organization's data. While intrusion detection technologies have improved, even when companies have adequate internal security protocols and procedures, IT managers may be reluctant to admit that their systems have been compromised. They may also be inclined to investigate on their own, potentially delaying an effective response and increasing the company's liability.

> "Companies can take steps to improve security by creating **specific written policies that are regularly audited**."

When a company suspects its systems have been compromised, it should immediately seek legal counsel. Another important decision is whether or when to call law enforcement agencies.

This decision requires weighing the cost and benefit of relying on internal or private resources before (or in lieu of) contacting law enforcement. The use of law enforcement inevitably entails a certain loss of control, presents coordination and interference issues, and may lead to negative publicity or disruption of the company's business.

Gathering the facts remains among the most important activities in responding to an incident. Having appropriate systems in place can be invaluable in determining if a breach has occurred and identifying its scope. Preserving evidence may require specific and unusual measures that may be unfamiliar to many employees, especially the IT pros who might initially respond.

Remediation may overlap other steps in timing, but it is often the most important as a test of the company's preparedness. Having clear internal lines of authority and establishing relations, in advance, with key outside actors may be valuable. Knowing appropriate local law enforcement personnel may be helpful. Understanding the company's insurance coverage can also be invaluable, as many insurers now offer coverage for the costs of incident response and breach notification.

Finally, when data is central to a company's success, elevating security to the corporate governance level may be wise. Because of potential liability, top officers may find themselves confronted by costly litigation as a result of the security measures they took — or failed to take. Given the potential consequences, companies must be prepared to manage these issues. [BT]

Gerard M. Stegmaier is an attorney in the Washington, D.C., office of a national law firm and an adjunct professor at George Mason University School of Law where he specializes in privacy and information governance.