PREVENTING & CONTAINING A DATA BREACH

THE PROBLEM:

Risk is rampant. If you have electronic data, you are at risk of a breach. You must be prepared to contain the legal and monetary fallout.

THE SOLUTION:

There is no silver bullet, but there are three steps you can and should take:

Did you know?

In 2014, there were over 2,000 data breaches in the U.S., costing companies an annual average of **$5.9 million** .[1*]

Prime targets were the healthcare and financial services industries.

FOLEY HOAG LLP

The Law Firm to Help You:

Foley Hoag knows that an ounce of prevention is worth a pound of cure. We can help you create a policy, stay on top of changes in the law, and manage a crisis.

For more information contact:

Colin Zick
617 832 1275
czick@foleyhoag.com

Martha Coakley
617 832 1115
mcoakley@foleyhoag.com

Check out the Security, Privacy and the Law blog:
www.securityprivacyandthelaw.com

1. Maintain an up-to-date data breach policy.

The best defense is a good offense. Much of the cost of containing a data breach results from lack of preparation. Creating a policy will focus your actions and contain your costs. Your policy should contain the following:

A plan for how employee and customer personal information will be maintained and safeguarded.

A plan for how customer, state agencies and law enforcement will be contacted in the event of a data breach.

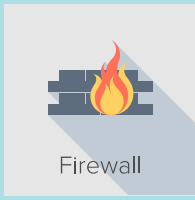
A plan for business continuity in the event of a data breach.

Your policy should also reflect applicable laws. In the United States, your business activities will be governed by both federal and state laws. To respond appropriately to breaches, you must know what laws apply and what each requires from you in response. If you don't, a breach can become a costly and time-consuming headache.

Decide on insurance. Cyber insurance is widely available to mitigate the costs of a breach. You should select a cyber insurance product that is right for your business.

2. Audit your data breach policy and your network annually.

Your company's needs and resources change. Your experience of what works for your company and what doesn't can change your perspective over time. Don't let your policy and best practices gather dust.



3. Keep up-to-date on changes in data breach notification laws and regulations on personal confidential information.

Laws and best practices change quickly. Just as technology evolves rapidly, laws move in parallel directions. You must stay informed and be prepared to adjust your policies and practices accordingly.

*Source: Ponemon Institute/IBM 2014 Cost of Data Breach Study: U.S.
[1] Verizon, 2014 Data Breach Investigation Report, http://www.verizonenterprise.com/DBIR