Courtesy of
TriSure Corporation

CYBERRISKS&LIABILITIES_

Understanding and Preventing Data Breaches

What do the New York State Electric & Gas Co., Global Payments, Inc., the California Department of Child Support Services, Emory Healthcare, Inc. and Apple have in common? All these companies have been victims of a data breach in 2012, totaling millions of stolen records that include personal information such as Social Security numbers, credit card numbers and bank account numbers.

If your company handles critical assets such as customers' personal data, intellectual property or proprietary corporate data, you are at risk of a data breach. It doesn't matter if you are a Fortune 500 company or a small "ma and pa" shop, cyber thieves are always looking for their next score. It is often assumed that smaller businesses are can escape attention from cyber crooks, but according to Verizon Communication's *2012 Data Breach Investigations Report*, 72 percent of data breaches were at companies with 100 or fewer employees. No company of any size is completely safe from a data breach.

Data Breach Basics
A data breach is an incident where private data is accessed and/or stolen by an unauthorized individual. Data can be stolen by a third party, such as a hacker, or by an internal actor (perhaps a disgruntled or recently fired employee).

According to the Ponemon Institute's *Cost of a Data Breach Survey*, the average per record cost of a data breach was $194 in 2011, and the average organizational cost of a data breach was $5.5 million.

Data Breach Prevention Techniques
To reduce the chance for a data breach, it is wise to develop an IT Risk Management Plan at your organization. Risk management solutions should leverage industry standards and best practices to assess hazards from unauthorized access, use, disclosure, disruption, modification or destruction of your organization's information systems. Consider the following when implementing risk management strategies at your organization:

- Create a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a description of all systems used at the organization based on their function, the data stored and processed and importance to the organization.
- Review the cyber risk plan on an annual basis and update it whenever there are significant changes to your information systems, the facilities where systems are stored or other conditions that may affect the impact of risk to the organization.

Not all companies have the resources to create and implement a fully customized plan. However, there are many simple, cost-effective steps any business can take to help prevent a data breach.

- Never give sensitive information like social security numbers or credit card numbers out over the phone unless you can verify the identity of the person on the other line.
- Shred all credit reports and other sensitive data before disposal.
- Educate employees about phishing and pharming scams. Remind them not to click on anything that looks suspicious or seems too good to be true.
- If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- Always monitor credit reports and other financial data

TRISURE

for the company. If you see things that don't belong, investigate.
- Do not allow employees to write down passwords in the office.
- Always encrypt sensitive data.

What to Do if You Have a Data Breach
It is common to have an "it will never happen to us" philosophy when it comes to data breaches. Unfortunately, that thinking can lead to lax security measures and carelessness when it comes to protecting sensitive information. If your company suffers a data breach:

- **Act quickly.** Report the breach immediately to local law enforcement. Notify important suppliers, vendors and partners.
- **Alert your customers.** If there is a data breach involving customers' personal information, activate your plan to alert them. The information compromised could be incredibly harmful to your customers, so alert them as soon as possible.
- **Investigate.** If you do not have the resources to do an internal investigation, consult a third party. The quicker the breach can be dealt with, the fewer negative effects your company will endure.
- **Take measures to lessen the chance of a future breach.** Fortunately, a data breach can be a good learning tool for your company. Analyze why the breach happened and take steps to make sure it doesn't happen again.

The Federal Trade Commission (FTC) has many resources available to assist you and your company in recovering from a data breach. Those resources can be found on the FTC's website: http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html

Insurance is Important
Chances are, your company doesn't have a "rainy day fund" capable of paying for data breach remediation. Fortunately, there are insurance options available to make recovery easier.

Cyber liability insurance policies can cover the cost of notifying customers and replace lost income as a result of a data breach. In addition, policies can cover legal defense fees a business may be required to pay as a result of the breach.

It's important to remember that it is cheaper to prevent a data breach by securing data than it is to lose that data from a breach. A data breach insurance policy can give you peace of mind and allow you to allocate resources to help keep data secure.

We're Here to Help
A data breach can be very costly and even has the ability to shut a business down. Contact TriSure Corporation today for resources to help support your cyber security efforts. We have the know-how to ensure you have the right coverage in place to protect your business from a data breach.