CYBERRISKS&LIABILITIES_

Responding to a Data Breach

No company, big or small, is immune to a data breach. Many small employers falsely believe they can elude the attention of a hacker, yet studies have shown the opposite is true. According to Verizon Communication's *2012 Data Breach Investigations Report*, 72 percent of the 855 data breaches analyzed were at companies with 100 or fewer employees.

Data breach response policies are essential for organizations of any size. A response policy should outline how your company will respond in the event of a data breach, and lay out an action plan that will be used to investigate potential breaches to mitigate damage should a breach occur.

Defining a Data Breach
A data breach is an incident where Personal Identifying Information (PII) is accessed and/or stolen by an unauthorized individual. Examples of PII include:

- Social Security numbers
- Credit card information (credit card numbers – whole or part; credit card expiration dates; cardholder names; cardholder addresses)
- Tax identification information numbers (Social Security numbers; business identification numbers; employer identification numbers)
    - Biometric records (fingerprints; DNA; or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information (paychecks; paystubs)
- Medical information for any employee or customer (doctor names and claims; insurance claims; prescriptions; any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; names; customer numbers)

Data breaches can be costly. 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; the average organizational cost of a data breach was $5.5 million.

Internal Responsibilities upon Learning of a Breach
A breach or a suspected breach of PII must be immediately investigated. Since all PII is of a highly confidential nature, only personnel necessary for the data breach investigation should be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PII were possibly compromised? (Detailed as possible: name; name and social security; name, account and password; etc.)
- How many customers may be affected?

Once basic information about the breach has been established, management should make a record of events and people involved, as well as any discoveries made over the course of the investigation to determine whether or not a breach has occurred.

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PII lost (customer contact information alone may present much less of a threat than financial information)
- Amount of PII lost and number of individuals affected
- Likelihood PII is usable or may cause harm

TRISURE

- Likelihood the PII was intentionally targeted (increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting PII (e.g. encrypted PII on a stolen laptop, which is technically stolen PII, will be much more difficult for a criminal to access.)
- Ability of your company to mitigate the risk of harm

Government Regulation
There aren't many federal regulations regarding cybersecurity, and the few that exist largely cover specific industries. The 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley (GLB) Act and the 2002 Homeland Security Act, which includes the Federal Information Security Management Act (FISMA) mandate that health care organizations, financial institutions and federal agencies, respectively, protect their computer systems and information. The language is generally vague, so individual states have attempted to create more targeted laws regarding cybersecurity.

California led the way in 2003 by mandating that any company that suffers a data breach must notify its customers of the details of the breach. Today, 46 states and the District of Columbia have data breach notification laws in place. Only Alabama, Kentucky, New Mexico and South Dakota have yet to enact such a law.

While notification laws vary from state to state, all include four basic provisions:

1. All notification laws put a number on how long companies have to notify customers of a data breach and by what medium the notice will be given (written, email, press release, etc.).
2. Laws set forth a penalty system (that differs from state-to-state) for failure to notify customers in a timely manner.
3. Depending on the specifics of the breach, customers can sue the company for its part in the data breach.
4. All notification laws have exceptions in a range of situations.

Your Notification Responsibilities
Responsibility to notify is based both on the number of individuals affected and the nature of the PII that was accessed. Any information found in the initial risk assessment should be turned over to the legal counsel of your company who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification should be made in a timely manner, but make sure the facts of the breach are well established before proceeding.

In the case that notification must be made:

- Only those that are legally required to be notified should be informed of the breach. Notifying a broad base when it is not required could cause raise unnecessary concern in those who have not been affected.
- A physical copy should always be mailed to the affected parties no matter what other notification methods are used (e.g. phone or email).
- A help line should be established as a resource for those who have additional questions about how the breach will affect them.

The notification letter should include:

- A brief description of the incident, the nature of the breach and the approximate date it occurred.
- A description of the type(s) of PII that were involved in the breach (the general types of PII, not an individual's specific information).
- Explanation of what your company is doing to investigate the breach, mitigate its negative effects and prevent future incidences.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a representative from your company who can answer additional questions.

We Can Help You Recover from a Data Breach
At TriSure Corporation, we understand the negative effects a data breach can have at your company. Contact us today so we can show you how to recover from a breach and get your company back on its feet.