Data Breach Response Guide

Powered by Experian® Innovation.
Last updated: September 2012

Table of Contents

Introduction 3

Data Breach Preparedness 4

Data Breach Incident Response 15

Data Breach Notification 17

Healthcare Data Breach 21

Legal Considerations 23

Preparedness Plan Audit 26

Resources and FAQs 28

Legal Notice

The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.
Introduction

There is no time like the present to establish an incident response plan. Thoughtful preparation before a breach can have a significant and empowering effect on a company and the sequence of events that will follow. Understanding of roles, notification letters, responsibilities and intended actions can minimize the impact of a breach, including liability and subsequent harm. These are difficult lessons to learn in the midst of a breach. It is ITRC’s experience that when you are unprepared for a situation and under pressure, the probability of error increases drastically.

Since 2005, data breaches have continued to remain in the spotlight. Many headlines over the years have focused on the record number of breach incidents, record number of personal records exposed or record high costs to organizations. The unfortunate aspect of these headlines is that they represent, for the most part, only those breaches that have been reported by some agency, media outlet or survey group that managed to garner access to the information.

We know that data breaches happen – many industry experts say it is not an if but a when situation. Therefore, it is critically important to assess your company’s potential vulnerabilities and develop protocols to address any areas of weakness. These protocols, as part of a Data Breach Response Plan, should clearly define the corporate roles and responsibilities of all those involved in the decision making process. Subsequently, these measures should be clearly communicated throughout the organization so that everyone understands the scope of the issue.

Breach Notification

While breach notification laws have been on the books in a growing number of states since 2002, these laws vary from state to state regarding mandatory reporting and notification. This situation has allowed for under-reporting and even non-reporting of many breaches nationwide. Current state notification laws have such a wide variety of loopholes that it is nearly impossible to determine the true extent of the number of incidents occurring annually. Data breaches involving paper documents: No mandatory reporting. Those with less than 500 victims or records: No problem. Whether or not reporting is mandated during a data breach at your company, you risk losing credibility with the public for not notifying.

For the most part, it really doesn’t matter if you are a small business or a large corporation, or if you handle only 5,000 personal records or tens of millions. There are currently several efforts underway to establish a national standard for the “who, what, when, where and how” of data breach notification. It should be the responsibility of all entities who handle personal information to protect that data and disclose security breaches to those who may be adversely affected.

Types of Breaches

There are many categories involved in the modern day “breach reports” that are made available by numerous entities. For instance, you have “type of entity,” such as: banking/financial, business/corporate, educational, government/military and medical/healthcare. A second tier of attributes may include the “how” aspect of a breach: insider theft, data on the move, hacking, accidental Web/Internet exposure or even subcontractor (third party) data loss. A quick look at the data breaches identified by the ITRC Breach Report over the past year points to a significant number of incidents where no “attributes” were identified, making it impossible to quantify any specific details relating to those breaches.

So how do breaches go public? If you’ve been hacked recently, it will likely make the news when the hackers go public and claim responsibility for the attack. Or, remember that old university website that posted grades along with Social Security numbers? Someone is bound to find the cached file that was left behind.

Other scenarios include a disgruntled employee who left with electronic files on a flash drive and later got arrested for identity theft, with the source of the data loss leading back to your company. A vendor transporting back-up files could lose them along the way or leave un-shredded documents in an abandoned warehouse. Once someone finds these files or documents, he/she will likely report it to the local media. By the time a breach does hit the media, your company has already potentially lost consumer confidence and brand equity.

Consider the Consumer Perspective

It is fundamentally important that the concept of corporate image and reputation be fully understood by everyone within the organization. A high level of understanding in these areas will enable everyone involved to better communicate with concerned consumers.

“Most companies experience opportunity costs associated with a breach incident, which results from diminished trust or confidence by present and future customers. Accordingly, our research shows that the negative publicity associated with a data breach incident can often damage companies’ reputations and may lead to abnormal turnover, or churn, rates and a diminished rate for new customer acquisitions.” (2010 Annual Study: U.S. Cost of a Data Breach, Ponemon Study, p 12)

It should be noted that corporate training and awareness programs should be in place before a breach occurs and not taken as a post-breach remedy. Knowledgeable, trained employees can help in maintaining a customer’s trust and respect during the critical time surrounding a breach incident. Customer loyalty is often retained by the timely dissemination of accurate information along with transparency of actions.

For more information about the Identity Theft Resource Center, visit: www.idtheftcenter.org.
Data Breach Preparedness

Why Create a Data Breach Preparedness Plan?

The cost of a data breach can average $214 per compromised record\(^1\). Multiply that by the hundreds or thousands – even millions – of records that are typically compromised in one breach and you begin to realize just how costly a data breach is. That's why it's so important to be prepared.

A data breach can take a toll on a company of any size. Having a breach preparedness plan in place can help you act quickly if one occurs. Acting quickly can help to prevent further data loss, significant fines and costly customer backlash.

Incident Preparedness

In the midst of a data breach is no time to decide how you're going to handle one or who's going to take care of what. So develop your response plan and build your response team before you need them.

Your team will coordinate efforts between your company's various departments and fulfill two primary functions:

1. The immediate function is to develop the data breach response plan and prep the entire organization on proper protocol during a breach.
2. Then, if a breach does occur, the team will implement the response plan, engage the proper resources and track the efforts.

Assemble Your Response Team

Incident Lead

Start by selecting your incident lead – think someone from an internal or external legal department or a Chief Privacy Officer. Your incident lead should be able to:

- Manage and coordinate your company's overall response efforts and team.
- Act as an intermediary between C-level executives and other team members to report progress and problems.
- Identify key tasks, manage timelines and document all response efforts from beginning to end.
- Outline the budget and resources needed to handle a breach.
- Summarize the steps needed to assess the scope of a breach.
- Ensure contact lists remain updated and team members remain ready to respond.
- Analyze response efforts post-breach to better prepare the company and team for the next incident.

Your incident lead, as well as every response team member, needs a backup.

---

\(^1\) U.S. Cost of Data Breach Study, Ponemon Institute (2010)
Here is a quick look at the other members you will want on your team and what their responsibilities might entail:

**Executive Leaders**

Include the company's key decision makers as advisors to your data breach response team to help ensure you have the needed leadership, backing and resources to properly develop and test your plan.

**IT & Security**

Your IT and security teams will likely lead the way in catching and stopping a data breach but not necessarily in investigating it. You’ll want someone from IT and/or security on your response team to:

* Train personnel in data breach response, including securing the premises, safely taking infected machines offline and preserving evidence.

* Work with a forensics firm to identify the compromised data and delete hacker tools without compromising evidence.

**Legal & Privacy**

Rely on internal and/or external legal, privacy and compliance experts to shape your data breach response and help minimize the risk of litigation and fines. Your legal representatives will need to:

* Determine whether it’s necessary to notify affected individuals, the media, law enforcement, government agencies and other third parties, such as card holder issuers.

* Establish relationships with any necessary external counsel now – not once a breach occurs.

* Review and stay up to date on both state and federal laws governing data breaches in your industry.

**PR**

Depending on the size of the data breach and your industry, you may need to report the breach to the media and/or notify affected individuals. Your response team member from PR or communications will need to:

* Identify the best notification and crisis management tactics before a breach ever occurs.

* Handle any information leaks regarding a breach.

* Track and analyze media coverage and quickly respond to any negative press during a breach.

**Customer Care & HR**

Data breaches may affect both your customers and your employees so appoint representatives from both customer service and HR to your response team to provide needed support. Your representatives should:

* Create simulation training for your customer service representatives that demonstrates how their roles would change during a data breach.

* Outline a plan for setting up a data breach hotline for customers and/or employees if a breach occurs. Determine in advance if you’ll use internal or external resources.

**Law Enforcement**

Depending on the severity of a data breach, you may need to involve law enforcement. Take time to collect all of the appropriate contact information now so you can act quickly if a breach does occur.

* Identify which state and federal authorities, including the FBI and Secret Service, to contact in the event of a data breach involving criminal activity.

* During a breach, be sure everyone on the data breach response team is aware of any law enforcement directives so the investigation isn’t interrupted.

**Data Breach Resolution Provider**

Contract with a data breach resolution vendor in advance of a breach to secure the best rates. Your vendor should be able to:

* Assign you a dedicated account manager to handle escalations, tracking and reporting.

* Handle all aspects of notification, including drafting, printing and mailing letters and address verification.

* Offer proven identity protection, comprehensive fraud resolution and secure call center services for affected individuals.

Clearly defined steps, timelines and checklists help keep everyone focused during the stress of a data breach.
Preparedness Training

In addition to a company-wide focus on data security and breach preparedness, department-specific training should trickle down from the data breach response team. Each member of the team has a unique responsibility to apply prevention and preparedness best practices to his/her own department.

- Work with employees to ingrain data security efforts into their daily work habits.
- Develop data security and mobile device policies, update them regularly and communicate them to business associates.
- Invest in the proper cyber security software, encryption devices and firewall protection. Update these security measures regularly.
- Limit the type of both hard and electronic data someone can access based on job requirements.
- Establish a method of reporting for employees who notice that others aren’t following the proper security measures.
- Conduct employee security training/re-training at least once a year.

While your data breach response team coordinates your preparedness and response efforts, everyone in your company plays a role in data security. Therefore everyone should be involved in data breach preparedness.

Prepare for the Worst So You Can Respond at Your Best

Be sure everyone on your data breach response teams understands their specific responsibilities—both in preparing for and responding to a breach. The forms in this section will give you a starting point for organizing the contacts for your team. Be sure to update and distribute the contact list every quarter so everyone is always prepared to act.

Data Breach Preparedness Continued

Data Breach Response Team Contact List

<table>
<thead>
<tr>
<th>Incident Lead</th>
<th></th>
<th></th>
<th>Company:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Lead Primary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td>Title:</td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td>Mobile Phone:</td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td>Email:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Lead Secondary</th>
<th></th>
<th></th>
<th>Company:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td>Title:</td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td>Mobile Phone:</td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td>Email:</td>
</tr>
</tbody>
</table>
## Data Breach Preparedness Continued

### C-Level Executives

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Title</th>
<th>Work Mobile Phone</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
<th>Internal</th>
<th>External</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Privacy Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief Compliance Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Data Breach Preparedness

## Response Team Members

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Title</th>
<th>Work Mobile Phone</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
<th>Company</th>
<th>Internal/External</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Title</th>
<th>Work Mobile Phone</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
<th>Company</th>
<th>Internal/External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Title</th>
<th>Work Mobile Phone</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
<th>Company</th>
<th>Internal/External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response Team Members</td>
<td>Company:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Phone:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Data Breach Preparedness Continued

### Response Team Members

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Title</th>
<th>Work Mobile Phone</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
<th>Company</th>
<th>Internal/External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Care Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Care Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR Primary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HR Secondary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:**
- **Company:** [Company Name]
- **Internal/External:** [Select the appropriate option]

---

*Data Breach Response Guide*
## External Data Breach Resources Contact List

### Resolution Partners

<table>
<thead>
<tr>
<th>Company:</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Legal Counsel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Public Relations/Crisis Management Firm

<table>
<thead>
<tr>
<th>Company:</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Forensics Firm

<table>
<thead>
<tr>
<th>Company:</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notification Vendor

<table>
<thead>
<tr>
<th>Company:</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Customer Service Vendor

<table>
<thead>
<tr>
<th>Company:</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Law Enforcement and Government Agencies

<table>
<thead>
<tr>
<th>Agency</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police Department</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secret Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FBI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State Attorney General</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Data Breach Preparedness Continued

<table>
<thead>
<tr>
<th>Third Parties</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Partners</strong></td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>Contact</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Vendors</strong></td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>Contact</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Third Parties

<table>
<thead>
<tr>
<th>Regulators</th>
<th>Company</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
</table>

### Card Processors

<table>
<thead>
<tr>
<th>Company</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
</table>

### Media

<table>
<thead>
<tr>
<th>Company</th>
<th>Contact</th>
<th>Mobile Phone</th>
<th>Office Phone</th>
<th>Email</th>
</tr>
</thead>
</table>
Data Breach Incident Response

“Discovery” of a breach refers to the first day any employee, officer or agent of the company knew about the breach or reasonably should have known about it.²

Acting quickly yet strategically following a data breach can help you regain your security, preserve evidence and protect your brand. Always collect, document and record as much information about the data breach and your response efforts, including conversations with law enforcement and legal counsel, as you can.

The First 24 Hours Checklist

Panicking won’t get you anywhere once you’ve discovered a data breach. Accept that it’s happened and immediately contact your legal counsel for guidance on initiating these 10 critical steps:

- **Record the date and time** when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.

- **Alert and activate everyone** on the response team, including external resources, to begin executing your preparedness plan.

- **Secure the premises** around the area where the data breach occurred to help preserve evidence.

- **Stop additional data loss.** Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.

- **Document everything** known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.

- **Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.

- **Review protocols** regarding disseminating information about the breach for everyone involved in this early stage.

- **Assess priorities and risks** based on what you know about the breach.

- **Bring in your forensics firm** to begin an in-depth investigation.

- **Notify law enforcement**, if needed, after consulting with legal counsel and upper management.

Once you have begun or completed the 10 initial steps, stop briefly to take inventory of your progress. Ensure your preparedness plan is on track and continue with these next steps:

**Fix the Issue that Caused the Breach**
- Rely on your forensics team to delete hacker tools.
- Determine if you have other security gaps or risks and address them.
- Put clean machines online in place of affected ones.
- Ensure the same type of breach cannot happen again.
- Document when and how the breach was contained.

**Identify Conflicting Initiatives**
- Make the response team and executives aware of any upcoming business initiatives that may interfere or clash with response efforts.
- Decide whether to postpone these efforts and for how long in order to focus on the breach.

**Alert Your Data Breach Resolution Vendor**
- Contact your pre-selected vendor to choose business services for your company and protection products for individuals affected in the breach.
- Determine how many activation codes you will need for the protection products based on the number of affected individuals.
- Draft and sign a data breach resolution agreement if you do not have a pre-breach agreement in place.
- Engage your vendor to handle notifications (learn more in the next section: Breach Notification) and set up a call center so affected individuals have access to customer service representatives trained on the breach.
- Work closely with your account manager to review incident reporting and metrics.

**Keep Your Response Efforts on Track**

Resolving a data breach requires a coordinated effort between your response team members, executives, external resources, law enforcement, forensic firm and data breach resolution vendor. Staying organized and documenting every step and decision should be a top priority. Act quickly to minimize the damage but don’t lose sight of your priorities or of the needs of affected individuals.

---

**Any data breach could lead to litigation. Work closely with your legal and compliance experts to analyze risks and ways to mitigate them, such as proper documentation and notification.**

**Identify Legal Obligations**
- Revisit state and federal regulations governing your industry and the type of data lost.
- Determine all entities that need to be notified, i.e. customers, employees, the media, government agencies, regulation boards, etc.
- Ensure all notifications occur within any mandated timeframes.

**Report to Upper Management**
- Compile daily breach reports for upper management.
- The first report should include all of the facts about the breach as well as the steps and resources needed to resolve it.
- Create a high-level overview of priorities and progress, as well as problems and risks.

**Don’t just document what steps you take. Document why you took them.**

**Continue Working with Forensics**
- Determine if any countermeasures, such as encryption, were enabled when the compromise occurred.
- Analyze backup, preserved or reconstructed data sources.
- Ascertain the number of suspected people affected and type of information compromised.
- Begin to align compromised data with customer names and addresses for notification.

**Never send sensitive information, such as SSNs, unnecessarily to vendors supporting the breach.**
Sixty days. That’s generally the amount of time businesses have to notify affected individuals of a data breach, assuming notification is required by law. The countdown starts the moment a breach is discovered. Depending on varying circumstances, you may have even less time.

Notification Challenges to Consider

Your legal counsel can help you determine if any of these or other challenges may impact your notification process:

• Certain state laws and federal regulations shrink the timeline to 30 or 45 days, meaning there’s no time to waste in verifying addresses; writing, printing and mailing notification letters; and setting up a call center and other services for affected individuals.

• Some states mandate specific content for you to include in your notification letters. This can include toll-free numbers and addresses for the three major credit bureaus, the FTC and a state’s attorney general.

• Notification may be delayed if law enforcement believes it would interfere with an ongoing investigation.

• Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside, not where the business is located.

• If some affected individuals live in a state that mandates notification and others live in a state that doesn’t, you should notify everyone so you’re not singled out for inequality.

• Keep in mind that some recipients will think the notification letter itself is a scam.

Mishandling notifications can lead to severe consequences, including fines and other unbudgeted expenses. It could also tarnish your brand reputation and customer loyalty, leading to potential revenue loss. In a recent survey, 76 percent of companies who had experienced a breach of customer data believed the incident had a moderate or significant impact on the organization’s reputation.³

Successful Notification

It is your responsibility to determine the deadlines for notification according to state law. The notification deadline is a heavy weight on top of the already burdensome and stressful ordeal of a data breach. One way to help eliminate some of that stress is determining how you’ll handle notifications before a breach occurs. Lining up a data breach resolution provider in advance can help shave off both time and stress from your response efforts. In many cases, you can even save money by signing a contract with a provider in advance of a breach.

What to Look For in a Data Breach Resolution Provider

Above all, your data breach resolution provider should make security a top priority throughout the notification process. Unlike standard direct mail production, data breach notification requires critical service and quality assurance elements to ensure compliance. Look for one vendor that can seamlessly handle notifications from beginning to end and make a positive impact on your brand.

Legal Notice: The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

³ Reputation Impact of a Data Breach, Ponemon Institute (2011)
Account Management

Amid the stress of a data breach, you’ll appreciate having an experienced account manager that streamlines and simplifies the notification process for you. Your account manager should know the ins and outs of your breach, your priorities and your deadlines. That can only happen if you have an assigned, dedicated account manager. Otherwise you’ll waste valuable time working with a different account manager every time you call.

Be sure to double check and test phone numbers and URLs in all communications.

Critical Notification Services

A full-service data breach resolution vendor should offer a range of options, as well as strict security standards, to fit your business needs and the scope of your breach:

Comprehensive letter management

- Templates for you to customize to your company and breach
- Management of multiple letter versions based on state regulations, affected individuals (employee vs. consumer audience), etc.
- Four-color or black-and-white letters
- Professional printing with your company logo and electronic signature

Address validation & delivery

- Return mail management to securely handle and discard returned notification letters
- Certified address cleansing confirmed against USPS standards

Quality assurance for printing and fulfillment

- Dedicated quality assurance personnel
- Robust integration controls to ensure 100% produced and mailed
- Tier-1 data security protocols with a secure/ restricted access production area
- Ongoing training and certification of personnel
- 24/7 camera monitoring with secure archiving

Reporting for compliance

- Daily inventory reporting
  - Initial mailings
  - Address changes
  - Undeliverable and returned letters
- Electronic letter copies for proof of notification
- USPS postal delivery report

As dictated by state law, a notification letter may need to include:

- Clear language, not industry jargon, that the average person could understand.
- Toll-free phone number for individuals wanting additional information.
- Details about the type of data lost and how it was lost, unless prohibited by law.
- Next steps to help affected individuals regain their security, such as signing up for a complimentary identity protection product.

Notification letters may contain sensitive data and require secure handling through every stage of drafting, printing and mailing.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.
Important Security and Protection Notification.
Please read this entire letter.

Dear [Insert customer name]:

I am contacting you regarding a data security incident that has occurred at [Insert Company Name]. This incident involved your [describe the type of personal information (of your client) that may be potentially exposed due to the breach incident (i.e., Social Security number, etc.)]. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

[Insert Company Name] takes this incident seriously and is committed to assuring the security of your data. To help protect your identity, we are offering a complimentary one-year membership of Experian’s ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: [date]
2. VISIT the ProtectMyID Web Site: www.protectmyid.com/enroll or call 1-XXX-XXX-XXXX to enroll
3. PROVIDE Your Activation Code: [code]

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You’ll receive timely Surveillance AlertsTM from ProtectMyID on any key changes in your credit report, a change of address, or if an Internet Scan detects that your information may have been found in an online forum where compromised credentials are traded or sold. ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

Your complimentary 12-month ProtectMyID membership includes:

- Credit Report: A copy of your Experian credit report
- Surveillance Alerts
  - Daily 3 Bureau Credit Monitoring: Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax, and TransUnion credit reports.
  - Internet Scan: Alerts you if your Social Security Number or Credit and/or Debit Card numbers are found on sites where compromised data is found, traded or sold.
  - Change of Address: Alerts you of any changes in your mailing address.
- Identity Theft Resolution: If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- Lost Wallet Protection: If you ever misplace or have your wallet stolen, an agent will help you cancel your credit, debit and medical insurance cards.
- $1 Million Identity Theft Insurance*: As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Activate your membership today at www.protectmyid.com/enroll or call 1-XXX-XXX-XXXX to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian’s customer care team at XXX-XXX-XXXX.

[Insert a detailed explanation about the circumstances surrounding the breach incident (e.g., this information was contained on a computer that was stolen from our offices.), what investigative steps have been taken, if you are aware of any fraudulent use of the information, explain the steps your company has taken to ensure that this issue won’t happen again, e.g., better secure our computers and facilities and include any and all other relevant facts]

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us at [insert company phone number].

Sincerely,

[Signed by appropriate executive - president, CEO or VP HR]

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.
## Data Breach Notification Continued

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Client identifies affected individuals, determines notification requirements and contacts vendor.</td>
</tr>
<tr>
<td>2</td>
<td>Vendor assigns a dedicated account manager and conducts kickoff meeting.</td>
</tr>
<tr>
<td>3</td>
<td>Client selects products and services and signs a data breach resolution agreement.</td>
</tr>
<tr>
<td>4</td>
<td>Vendor provides samples of notification letters and options for consumer protection products.</td>
</tr>
<tr>
<td>5</td>
<td>Client provides final data files and letter materials.</td>
</tr>
<tr>
<td>6</td>
<td>Vendor aligns affected individuals with addresses and generates product activation codes.</td>
</tr>
<tr>
<td>7</td>
<td>Vendor preps call center using incident-specific FAQs.</td>
</tr>
<tr>
<td>8</td>
<td>Client and vendor jointly approve final letter proof.</td>
</tr>
<tr>
<td>9</td>
<td>Vendor oversees mailing, delivery and re-mailing from secure fulfillment center.</td>
</tr>
<tr>
<td>10</td>
<td>Vendor provides regular reporting and metrics to client to track engagement.</td>
</tr>
</tbody>
</table>

**Legal Notice:** Always check with your legal counsel in order to identify the notification requirements for your specific incident.
Healthcare Data Breach Response and Readiness - A Special Case

Preventing and responding to data breaches within the healthcare sector requires extra vigilance. Not only do many healthcare companies and vendors have to comply with the normal spate of state data breach laws, but, in addition, they must comply with new federal requirements. Healthcare companies also must search for a broader array of private data in their investigations, respond to a growing number of regulators and put new emphasis on taking action to prevent – not just respond to – data breaches.

A More Complex Legal Landscape

The Health Information Technology for Economic and Clinical Health (HITECH) Act passed as part of the economic stimulus package of 2009 required companies to report breaches of “protected health information” (PHI). In doing so, the HITECH Act added a significant level of complexity to data breach response plans for many organizations.

• First, more companies now have to pay attention to health-related information and how it is handled. Traditional healthcare entities like insurance plans and hospitals have long had to comply with healthcare privacy and security rules as “covered entities” under the Healthcare Insurance Portability and Accountability Act (HIPAA). The HITECH Act, however, extended security and data breach notification requirements to “business associates” such as Web portals, data aggregators, consultants and even lawyers who handle health data and offer services to traditional healthcare providers.

• Second, the HITECH Act requires healthcare companies and their vendors to comply with new federal law, while still taking into account the confusing patchwork of state data breach notification laws. In some states, an organization that is already subject to HIPAA/HITECH may be exempt from state notification rules, but this is not true across the nation. Some states actually include medical data within their own definitions of “personally identifiable information” (PII), and states like California only exempt an organization if it complies with federal law in the first place. In other words, a company that falls short of federal law may face the double whammy of federal and state liability.

• Third, the HITECH Act imposes reporting deadlines that may differ from or trump state law. For example, many states leave the timing open-ended and simply require notification in the “most expedient time possible and without unreasonable delay.” The HITECH Act, however, is more specific and requires companies to report a healthcare data breach to victims within 60 days of its discovery.

• Finally, the HITECH Act adds another layer of potential financial penalties on companies that fail to give proper notice of a breach. States can impose fines ranging from $500 per victim to $500,000 per breach. The HITECH Act allows the Department of Health and Human Services (HHS) to impose even higher fines, between $25,000 and $1.5 million per year depending on the culpability of the company.
More Data to View

Healthcare data breaches often require analysis of more data, in part based on the broad definition of a “breach” and “protected health information” covered by the HITECH Act. Many state laws do not trigger a reporting requirement unless there has been unauthorized “acquisition” of personal data. Even then, some states only require victim notification if it is reasonably likely that “misuse,” “fraud” or “identity theft” will occur. In contrast, the HITECH Act more broadly requires companies to provide notices to victims if impermissible use or disclosure of protected health information poses a “significant risk of financial, reputational or other harm” to individuals.

In addition, while most state laws focus on a person’s name, Social Security number, driver’s license number and financial account number, the HITECH Act potentially covers more categories of data. These include health information and a corresponding person’s name, his/her relatives, employer(s), household members, date of birth, hospital admission or discharge dates, telephone numbers, email addresses, medical record numbers, vehicle numbers, Internet Protocol addresses, full face photos and “any other unique identifying number, characteristic, or code….”

Taken together, these definitions mean that companies that suffer a healthcare data breach often will need to run more extensive searches for personal information across their affected servers. In addition, companies often will need to evaluate more than financial loss and will need to evaluate any “other harm” that could befall breach victims.

More Reporting, and Faster

Healthcare companies often must report their breaches to more regulators and do so faster than non-healthcare companies. All state data breach laws generally require notification of individual victims, and, in some states, notice must go to consumer reporting agencies and the Attorney General’s office as well. On top of this, companies suffering a healthcare data breach must report to HHS or the Federal Trade Commission (FTC) at the federal level and to local media outlets if more than 500 victims have been affected. In addition, state health commissioners and insurance regulators may have independent reporting requirements. For example, Virginia law requires that companies report a healthcare data breach to both the Attorney General and the state Commissioner of Health, and the Connecticut Insurance Commissioner now requires that insurance companies report a breach within five days.

More Preventive Measures

Finally, any company that handles healthcare data now must move more aggressively to protect it. In June 2012, the Office of Civil Rights at HHS announced that it was auditing companies based on 165 newly revealed compliance categories – 77 related to data security and 88 related to privacy and breach notification. While companies previously may have given lip service to the aspirational goals of the HIPAA Security and Privacy Rules, times have changed. Now companies must do more than read the rules and respond to a breach; they must seek to get ahead of the curve and implement real measures aimed at preventing a breach in the first place.

Paul Luehr is Managing Director and Chief Privacy Officer of Stroz Friedberg, a global digital risk management firm that specializes in digital forensics, data breach response, electronic discovery, and business intelligence and investigations. Mr. Luehr is a former federal cybercrimes prosecutor and FTC Assistant Director who worked on matters ranging from Internet fraud and consumer privacy to the post-9/11 search of terrorist Zacarias Moussaoui’s laptop. He has appeared on national television, in The Wall Street Journal, The New York Times, and was featured by Business Week as one of the nation’s top cyber-cops.

About Stroz Friedberg, LLC: Stroz Friedberg is a leading global digital risk management and investigations firm. The company specializes in digital forensics, data breach and cybersecurity response, electronic discovery, security risk consulting and business intelligence and investigations. Working at the crossroads of technology, law and behavioral science, the company provides technical assistance and strategic advice to help manage the inherent risks and responsibilities of doing business in a digital era. Learn more about the firm’s capabilities and experience at www.strozfriedberg.com.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.
Recent Trends in Data Breach Legislation

While most states have a data breach notification law in place, high-profile breaches continue to occur. And while data breaches can occur even when a company has good data security systems in place, there is concern among some policy makers that existing laws are insufficient and have not kept pace with the increasing use of consumer information in the economy.

Shifting expectation of sensitive information

At the heart of all notification laws is the breach of personal information that can uniquely identify an individual and pose a risk for identity fraud. Generally, personal information is composed of a first name/initial and last name in addition to another piece of identifying information, such as a Social Security number, credit or debit card number or an account number. Over time, policy makers have begun to consider whether additional identifying elements should be considered sensitive information.

Some states have expanded the law to include medical and health insurance and taxpayer identification numbers. There is also a blurring of the distinction between identifiable information and anonymous or de-identified information. This has led to the consideration of notification in the event of a breach of sensitive information independent of a name, such as email addresses that could be associated with a financial account.

Protection of healthcare data

The use and protection of personal health information has largely been regulated at the federal level under the Health Insurance Portability and Accountability Act (HIPAA), but the requirements have been expanding. Changes to the law in 2009 drastically increased the penalties for data breaches and widened the scope by requiring third parties, such as a billing company or offsite storage provider, to follow the HIPAA privacy laws and report data breaches.
State law has also shifted toward protecting health information. To date, five states and Puerto Rico have included medical information in what is considered personal information and is protected under breach notification laws.

**Expansion of notification content**

Policy makers are also considering expanding existing breach notification laws by being more prescriptive about what information must be included in a notice. This includes information such as the time of the breach and the type of data affected.

**Attorney General notification**

As state attorneys general have gotten more involved in the oversight of breach notices, a number of states have proposed a new requirement to report breaches to the attorney general's office. Proposals have ranged from notification in the event of any breach, no matter the size, to setting thresholds, such as the information of 500 individuals breached. Legislation has also looked at the timing of when notices are made available, from as soon as reasonably possible to a more prescriptive number of days.

**Focus on penalties**

As the number of data breaches and the impact on consumers increase, regulators are focused on the appropriate level of fines for companies that are not compliant with breach notification laws. Recent proposals would set fines for each breach of an individual's information while others look at leaving the fines up to regulators with a large cap.

**New Data Breach Notification Laws in 2011**

In 2011, at least 12 states considered an expansion to the existing data breach notification laws and three approved new requirements.

**California**

New laws took effect January 1, 2012 that require organizations to provide additional content in data breach notifications, including a general description of the incident, the type of information breached, the time of the breach and toll-free telephone numbers and addresses of the major credit reporting agencies in California. The notice must include the following information if such information is possible to determine before sending the notice:

- The date, estimated date or date range of the breach
- Whether notification was delayed as a result of a law enforcement investigation
- A general description of the breach incident

In addition, the law requires data holders to send an electronic copy of the notification to the California Attorney General if a single breach affects more than 500 Californians.

**Illinois**

In 2011, Illinois joined a growing number of states that dictate what content, at a minimum, must be included in notices to individuals regarding a compromise of their personal information. As of January 1, 2012, security breach notices to Illinois residents must include contact information for credit reporting agencies and the Federal Trade Commission, along with a “statement that the individual can obtain information from these sources about fraud alerts and security freezes.” The law also expands the reach of the state’s breach notice requirements to include service providers who maintain or store but don’t own or license personal information.

**Texas**

Recently passed legislation focusing mostly on healthcare providers would require additional breach notification to residents outside of the state. Texas amended its breach notification law so that its consumer notification obligations apply not only to residents of Texas, but to any resident of a state that has not enacted their own notification law (Alabama, Kentucky, New Mexico and South Dakota).

**Federal Legislation**

In response to this continuing and changing landscape, there is a growing consensus among policymakers at the federal level that businesses must do a better job of protecting consumer information. At the same time, the specter of an uneven regulatory environment that may hurt both businesses and consumers has led to a robust discussion across multiple congressional committees and federal agencies. In response, there are a number of data security and data privacy proposals that would place new restrictions on how businesses collect, use and protect consumer data. Following are a few of the proposals before congress.
Legal Considerations Continued

House of Representatives

The SAFE Data Act (H.R. 2577) was approved by the Commerce, Manufacturing and Trade Subcommittee in July 2011 and is now awaiting consideration by the full Energy and the Commerce Committee.

- Definition of Personal Information: Personal Information (PI), as proposed, is an individual’s first and last name in combination with any two of the following: home address or telephone number, mother’s maiden name and date of birth. Unique biometric data, unique account identifiers and government-issued unique identifiers are also defined as PI.

- Notification requirements: Consumers would need to be notified “as promptly as possible.” Notice must be delivered in writing or by electronic means and include: a description of the PI that was breached; information on consumer credit reports and monitoring that consumers are entitled to; and contact information for the FTC and credit bureaus. The bill allows for entities not to notify consumers if a risk assessment is conducted and concludes there is no risk of harm to the individual.

- Penalties: Federal officials and the FTC would need to be notified without delay and the media must receive notice if the breach exceeds 5,000 individuals or involves a database that is either owned by the federal government or includes the PI of 500,000 people nationwide.

The Obama Administration

The White House’s cyber security draft proposal released in May 2011 also includes a data breach provision.

- Definition of Personal Information: PI, as proposed, is the same under H.R. 2577 and S. 1151, but this proposal authorizes the FTC to modify the definition of PI by rule.

- Notification requirements: Notice must be provided to consumers no later than 60 days, unless the entity can demonstrate that a delay is necessary. Federal officials would need to be notified if the breach exceeds 5,000 individuals or involves a database that is either owned by the federal government or includes the PI of 500,000 people nationwide. Credit bureaus must be notified in the event that more than 5,000 individuals are informed of a breach.

- Penalties: State attorneys general could bring civil actions to recover the penalties in the amount of $1,000 per day, up to $1 million per violation.

Senate

The Judiciary Committee approved the Personal Data Privacy and Security Act of 2011 (S. 1151) in September 2011. The bill is now awaiting debate on the Senate floor.

- Definition of Personal Information: The PI definition, as proposed, is similar to H.R. 2577 and also includes a safe harbor if a risk assessment finds no risk of identity theft, economic or physical harm.

Consensus has not yet fully emerged about the future of a comprehensive, national data protection framework. Policymakers still need to fully consider each approach and whether it fits into a national framework that protects consumers while facilitating innovation and competition. Meanwhile, commercial entities that are not already regulated should be prepared to engage in industry best practices and effective self-regulatory regimes in order to protect themselves from increased regulatory oversight and liability.

Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.
Preparedness Plan Audit

Once you’ve created your preparedness plan, you’ve cleared one of the major hurdles in setting up your organization for success if a data breach occurs. But your preparedness plan can only help you succeed if it’s comprehensive and current. Each quarter, make it a priority to update, audit and test your plan. Consider the different scenarios that could occur and whether your plan would help address each one, including an internal breach, external attack, accidental data sharing and loss or theft of a physical device.

Most Overlooked Details

Here’s a look at a few commonly overlooked details that should be on your radar during a preparedness plan audit.

Call center

Getting your call center up to speed on a data loss incident or bringing external resources on board to help handle the high volume of calls is an important part of data breach preparedness. In the time following a data breach is not when you want to hide from or alienate your consumers. Instead, be readily available to answer their questions in order to reinforce the value of your brand and your commitment to their security.

Whether you plan to use internal or external resources, be sure you:

• Are prepared to swiftly pull together training materials, such as incident FAQs. Highly knowledgeable and emphatic call center representatives can make a positive impact on your brand during a crisis.

• Are able to scale the call center portion of your preparedness plan to fit any incident. In addition to identifying needed call center resources in advance of a breach, also create a call center script template specifically geared toward crisis management.

• Conduct ongoing crisis training for your regular call center, whether it’s internal or external, so representatives are trained in handling sensitive information as well as emotional callers.

• Oversee several test calls to confirm the call center is ready to handle incident-related calls.

Vendor negotiations

With companies being plagued by data security breaches at the hands of their vendors, take steps to ensure your company isn’t headed down the same road. Select vendors that have appropriate security measures in place for the data they will process. Then take it a step further by contractually obligating your vendors to maintain sufficient data safeguards. Assess whether they are meeting the contract requirements on a regular basis.

In general, it makes sense for companies to require that vendors:

• Maintain a written security program that covers the company’s data.

• Only use the company’s data for the sole purpose of providing the contracted services.

• Promptly notify the company of any potential security incidents involving company data and cooperate with the company in addressing the incident.

• Comply with applicable data security laws.

• Return or appropriately destroy company data at the end of the contract.

Operational challenges

So you’ve determined all of the steps and precautions you’ll need to take if a data breach occurs. But, responding to one can take significant company resources. Does your preparedness plan address the operational challenges of managing a breach in conjunction with managing day-to-day business?

For example, if your head of security and/or IT is tied up with breach response, who oversees the department in the meantime? Answering questions like these truly helps to illustrate that data security, data breach preparedness and data breach response requires company-wide awareness and involvement.

As part of your preparedness plan, have every member of the response team prep their departments on what to expect and how to operate during data breach response. Everyone on staff should understand how their roles might change during a breach in order to maintain operations.

Always seek advice from legal and compliance when drawing up vendor contracts, especially ones involving data management or transfer.
# Preparedness Plan Audit

## Preparedness Audit Checklist

Auditing your preparedness plan helps ensure it stays current and useful. Here are several recommended steps you may want to take, but be sure to tailor your audit to fit the full scope of your company’s individual response plan.

<table>
<thead>
<tr>
<th>Step Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update data breach response team contact list</strong></td>
<td>Quarterly</td>
</tr>
<tr>
<td>• Check that contact information for internal and external members of your breach response team is current.</td>
<td></td>
</tr>
<tr>
<td>• Remove anyone who is no longer with your company or with an external partner and add new department heads.</td>
<td></td>
</tr>
<tr>
<td>• Re-distribute the updated list to the appropriate parties.</td>
<td></td>
</tr>
<tr>
<td><strong>Verify your data breach response plan is comprehensive</strong></td>
<td>Quarterly</td>
</tr>
<tr>
<td>• Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies.</td>
<td></td>
</tr>
<tr>
<td>• Verify each response team member and department understands its role during a data breach. Create example scenarios for your response team and departments to address.</td>
<td></td>
</tr>
<tr>
<td><strong>Double check your vendor contracts</strong></td>
<td>Quarterly</td>
</tr>
<tr>
<td>• Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors.</td>
<td></td>
</tr>
<tr>
<td>• Verify your vendors and contracts still match the scope of your business.</td>
<td></td>
</tr>
<tr>
<td><strong>Review notification guidelines</strong></td>
<td>Quarterly</td>
</tr>
<tr>
<td>• Ensure the notification portion of your response plan takes into account the latest state legislation.</td>
<td></td>
</tr>
<tr>
<td>• Update your notification letter templates, as needed, to reflect any new laws.</td>
<td></td>
</tr>
<tr>
<td>• Verify your contacts are up to date for attorneys, government agencies or media you’ll need to notify following a breach.</td>
<td></td>
</tr>
<tr>
<td>• Healthcare entities need to ensure they have the proper Department of Health &amp; Human Services contacts and reporting process in place.</td>
<td></td>
</tr>
<tr>
<td><strong>Check up on third parties that have access to your data</strong></td>
<td>Quarterly</td>
</tr>
<tr>
<td>• Review how third parties are managing your data and if they are meeting your data protection standards.</td>
<td></td>
</tr>
<tr>
<td>• Ensure they are up to date on any new legislation that may affect you during a data breach.</td>
<td></td>
</tr>
<tr>
<td>• Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it.</td>
<td></td>
</tr>
<tr>
<td>• Healthcare entities should ensure business associate agreements (BAAs) are in place to meet HIPAA requirements.</td>
<td></td>
</tr>
<tr>
<td><strong>Evaluate IT Security</strong></td>
<td>Quarterly</td>
</tr>
<tr>
<td>• Ensure proper data access controls are in place.</td>
<td></td>
</tr>
<tr>
<td>• Verify that company-wide automation of operating system and software updates are installing properly.</td>
<td></td>
</tr>
<tr>
<td>• Ensure automated monitoring of and reporting on systems for security gaps is up to date.</td>
<td></td>
</tr>
<tr>
<td>• Verify that backup tapes are stored securely.</td>
<td></td>
</tr>
<tr>
<td><strong>Review staff security awareness</strong></td>
<td>Yearly</td>
</tr>
<tr>
<td>• Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard.</td>
<td></td>
</tr>
<tr>
<td>• Review how to spot and report the signs of a data breach from within everyday working environments.</td>
<td></td>
</tr>
<tr>
<td>• Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months.</td>
<td></td>
</tr>
</tbody>
</table>
Resources

Experian's Robust Online Resource Center

Data breach laws and risks are constantly changing. So is our online Resource Center, where you’ll find the latest webinars and whitepapers created in partnership with some of today’s top experts in privacy, data breach legislation and other key areas. Here’s a quick look at some of the free resources we offer online:

Studies

- Healthcare Information Security Today Survey
  Information Security Media Group, co-sponsored by Experian®

- Reputation Impact of a Data Breach
  Ponemon Institute, LLC

Whitepapers

- Security as Business Risk: How Data Breaches Impact Bottom Lines
  **EXCERPT** “The huge number of high-profile data breaches in the past few years has provided statistically valid data to better measure the connection between a company’s security and its bottom line.”

- An Investigative Approach to Data Breaches: From Incident to Resolution
  **EXCERPT** “It is of vital importance to swiftly address the many looming vulnerabilities that could manifest in reputational injury and, moreover, fraud. Synchronizing an effective incident response, one that bears minimal disruptive impact on operations, requires the wherewithal for timely fact-finding and risk mitigation at all levels.”

  **EXCERPT** “There’s no doubt that the healthcare industry is under a great deal of scrutiny when it comes to data breaches. So much so that an organization may find it difficult to determine which legislation and regulations govern a particular data breach at a particular time.”

Webinars

- Medical Identity Theft Trends: The Importance of Securing Healthcare Data
  **LEARN** Findings from the Second Annual Survey on Medical Identity Theft.

- A 360° View of a Data Breach
  **LEARN** What to do when there is a data breach, from investigation to notification.

- State Legislation Effects on Data Breach Resolution
  **LEARN** Trends in data security legislation and regulation.

- Cyber Security and Its Role in Data Breach Preparedness
  **LEARN** Threats facing businesses today and appropriate precautions to prevent data loss.
FAQs

What is a data breach?
A data breach occurs when secure data is released to or accessed by unauthorized individuals. The lost data may be sensitive personal data the company has collected on employees or customers or proprietary and confidential data regarding business operations and trade secrets. Data breaches can involve the loss or theft of digital media or physical data and devices, such as computer tapes, hard drives, mobile devices and computers. The incidents pose serious risks for organizations as well as for the individuals whose data has been lost.

How do data breaches happen?
Data breaches occur due to: accidental mishaps, such as an employee losing a mobile device or sending out sensitive data in an unsecured email; purposeful and malicious criminal attacks by someone inside or outside your organization; or a system failure or glitch that compromises security and leads to data loss.

How could a data breach impact my business?
A data breach has both direct and indirect financial consequences. First a business must allocate the budget and resources to resolve a data breach and address the underlying problem that led to the breach. In 2010, the average cost of a data breach was $7.2 million with an average cost per compromised record of $214. Then a business must deal with the financial repercussions related to negative press, loss of customer loyalty, diminished brand reputation and possibly even litigation. In 2011, 76% of surveyed companies that had experienced a data breach believed the incident had a moderate or significant impact on the organization’s reputation.

How do I protect brand equity after a data breach?
In the face of a data breach, organizations have the opportunity to quickly implement sound decisions that will ultimately result in preserving brand equity and customer relationships. In a 2009 whitepaper, Javelin Strategy & Research outlined that, “The most effective way for an institution to demonstrate its sympathy and concern is to proactively offer complimentary fraud protection in the form of identity protection services, which can encompass credit monitoring, fraud alerts and personal information monitoring.” Experian makes it easy by offering a variety of consumer protection products, all backed with superior fraud resolution, for you to provide affected individuals.

What are my legal requirements regarding a data breach?
Working with internal and/or external legal counsel can help you determine your obligations, which is something you should explore before a data breach ever occurs. Your legal counsel will help you navigate the different state laws and determine whether they apply based on where the affected individuals reside, not where your business is located. Some industries, such as healthcare, have special considerations for reporting a data breach and notifying affected individuals. Be sure you work with a data breach resolution provider that can help you take all of the vital steps your legal counsel recommends. Even if your counsel determines you are not obligated by law to notify affected individuals, doing so can help preserve and even strengthen your relationship with consumers.

Do all data breach resolution vendors offer the same services?
No. Among the different vendors, there are different levels of service and different solutions to consider. Plus, you need to think about the integrity and security standards of a vendor before aligning your brand with it. For example, Experian’s 30 years of global leadership and experience reflect positively upon another brand, especially during a data breach. As the world’s largest credit bureau, we offer superior business and consumer services that millions rely on. Our trusted identity protection products can help you meet the needs of affected individuals for credit monitoring and alerts of potential identity theft. We also back our products with proven fraud resolution services, offering consumers professional guidance in resolving identity theft. And, since we are the world’s largest credit bureau, we can securely access your consumers’ credit data (with their permission) and enact credit alerts to discourage new credit activity in their names. Your dedicated data breach resolution account manager can help explain the different options available to you. These options include: individual or family protection; 1-bureau or 3-bureau credit monitoring; length of membership in the protection product; advanced features, such as Lost Wallet to help consumers act quickly in the event of lost or stolen credit, debit and medical insurance cards and Internet Scan to monitor websites known for selling or trading compromised Social Security, debit and credit card numbers.

54% of companies believe it can take 10 months to more than two years to restore its reputation following a breach of customer data.

4 2010 U.S. Cost of a Data Breach, Ponemon Institute
5 Reputation Impact of a Data Breach, Ponemon Institute (2011)
7 Reputation Impact of a Data Breach, Ponemon Institute (2011)
About Experian Data Breach Resolution

Drawing on the global power of Experian®, the largest credit bureau in the world, Experian Data Breach Resolution helps businesses of all sizes navigate the stormy waters of a data breach. We have handled thousands of high-profile data breaches in nearly every industry, from medical to government. Our industry-leading service and consumer protection products help companies manage the stress of a data breach while mitigating damage to their reputations and customer loyalty. For questions or to provide feedback about this guide, please contact us at databreachinfo@experian.com.

The word ‘Experian’ is a registered trademark in the EU and other countries and is owned by Experian Ltd. and/or its associated companies.