BakerHostetler

Brief

The best response to a data breach is before it happens.

You may not be able to prevent a data breach.

But you can definitely prepare for it.

A data breach can come from almost anywhere, inside or outside your company. While the consequences—financial havoc, legal liability, negative PR—can be dire, the impact of a breach can be minimized through meticulous preparation. The key is to make sure your entire company—not just your IT department—is truly serious about data security.

1. Review policies and procedures

When it comes to data security, preparation is your first line of defense. A company-wide audit of policies and procedures should be conducted and updated as often as necessary. These include:

- **Incident and Breach Response Policies**—Key personnel need to be kept informed on the latest threats and possible responses, response plans need to be formulated, and a response team named
- **Information Security and User Policies**—All users of sensitive data must understand limitations on password usage, use of proprietary information, internet usage, system use, and remote access
- **IT Policies**—Policies must clearly cover: logs, data backup, server configuration, patch updates, modifications, firewalls, wireless, VPN, router, switch security, and email retention
- **Social Media Policy**—Is it clear to your employees what types of information may not, under any circumstance, be posted on social media sites, even personally? How often do you remind them of this policy?

2. Identify your risks

Risk assessment is an ongoing responsibility, entailing periodic review of all safeguards currently in place. These safeguards fall into four broad categories, and the questions being asked here are the tip of the iceberg:

- **Administrative safeguards**—Do employees understand the importance of correct data handling? Are your workflow procedures secure? Are password procedures optimal? Is sensitive information accessible from home computers? From mobile devices?
- **Physical safeguards**—Are your facilities—offices, factories, labs, data centers—secure? Are employees' laptops and mobile devices protected from intrusion?
- **Technical safeguards**—Are IT policies and procedures strictly enforced? Is encryption up to the latest industry standards? Are data backup procedures secure?
- **Information safeguards**—What is the nature of information being collected? Has it changed? Is it subject to new regulatory requirements?

3. Put a team in place

Your Incident Response Team (IRT) designates the company's "first responders" in the event of a data breach. These are the people who must assess the threat, attempt to contain it, notify the necessary authorities, and document every step taken. The IRT consists of both internal and external personnel and should include at least one member from each of the following:

- IT
- HR
- Executive suite
- Legal counsel
- Insurance
- Public relations

Depending on your industry, its regulations, and the potential consequences of a breach, your company should add additional team members as needed. Note that this team cannot just exist on paper. It should meet at least quarterly to review recent incidents, updated requirements, or areas of concern.

4. Make a plan

Key to your company's response is an Incident Response Plan (IRP) outlining the steps needed in the event of a breach.

Your IRP should contain:

- **Background information** on all applicable laws concerning data security in your industry, including who needs to be notified—law enforcement, regulatory agencies, credit reporting agencies, SEC, customers, etc.—in the event of a breach
- **Detailed procedures**, including step-by-step guides to managing an incident
- **Contact details** for every member of the IRT, both internal and external
- **Documentation procedures**, so that all discoveries can be thoroughly documented for future evidence

The IRP must be a "living document." It will need to be upgraded periodically as requirements and/or situations change.

5. Vet your vendors

Preparing for a data breach involves identifying all points of vulnerability, starting with due diligence on your vendor relationships. Vendors that require scrutiny include service providers: cleaning and janitorial, security services, off-site storage and shredding services, and data processing and storage facilities. Particular attention must be paid to benefits administrators and your various banking and financial services providers.

With each vendor, check to ensure that:

- Their protective safeguards are at least as effective as your own
- Those safeguards meet the legal requirements of their own industries, as well as yours
- They have adequate insurance and the resources to pay in the event of legal action against them
- You can produce evidence of due diligence regarding your vendors in the event your company is challenged in a regulatory proceeding

It is further advisable to negotiate new provisions in your service contract to cover security awareness and education.

6. Strengthen your data security

Every employee who handles customers' personal information needs to understand both the proper way to handle that information and the reasons why proper handling is important. In addition, basic data security questions that need to be answered and constantly reviewed, including:

- **Data identification and classification**—Is all collected information going where it is supposed to go? Is it stored securely?
- **Data hygiene**—Are you collecting the data you truly need, and—just as important—not collecting data you don't need?
- **Document retention and destruction**—What are your document retention policies? How long are you required to store data? Where do you store old data and how secure is it?

Based on how these questions are answered, data policies and procedures must be formulated and consistently enforced.

WHEN A BREACH OCCURS:

The First 48 Hours

In the event of data breach, your company's response in the first 48 hours can make a major difference in the outcome and ultimate consequences. In general, this involve your Incident Response Team (IRT) dealing with the following questions:

Identify the nature of the breach
Has a server been compromised? Has a laptop, smartphone, or thumb drive been lost or stolen? Did the breach come from inside—through employee carelessness, ignorance, or maliciousness? Or did it come from outside—through hackers, thieves, phishers, or vendors?

Determine which data is comprimised
Is the information personal and/or confidential? Does it include names, addresses, usernames, passwords, etc? Credit card numbers? Social Security Numbers? Is it financial? Is it healthcare-related?

Ascertain who is affected
Does the breach have a potential impact on your customers? On your employees? Does it affect internal trade secrets? If the information falls into the wrong hands, how is your business affected?

Decide who needs to be notified
Should you notify legal counsel? Your insurance carrier? Your public relations team? Which regulations apply? Do customers need to be notified? Law enforcement? Government agencies? Credit reporting agencies? SEC?

Figure out next steps
Once these questions have detailed answers, you can then address the issues of containing the breach, investigating the causes, assessing and remedying the damage, and incorporating what was learned into new policies and procedures.

Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Washington, DC

www.bakerlaw.com