Into The Breach: How To Prevent Data Breaches And Respond To The Aftermath

Insights
11.01.16

Employers have a legal obligation to safeguard and protect a variety of information hosted in the workplace. Unfortunately, when it comes to workplace data breaches, the question is not if you will suffer one, but when.

Although outside threats and hackers tend to dominate the news, many data breaches are actually inside jobs, whether the result of negligent data security practices, human error, or intentional breach of private data by employees. Employers of all sizes, including small businesses and nonprofits, have found themselves in the midst of expensive and disastrous data security breaches. While nothing is foolproof, you should prepare for the worst by implementing best practices for protecting private information from both outside hackers and trusted insiders alike.

Why Is Data Privacy Important?
In the course of doing business, an organization may compile, receive, create, or maintain three categories of information for which a legal obligation to safeguard applies: personally identifiable information defined as private by particular statutes or regulations; private information protected under the terms of a contract with a third party; and other information for which a common law or constitutional right to privacy applies.

Ensuring the privacy of data in all three categories is important because the risks and costs of a data breach can be devastating. First, when an unauthorized person gains access to or obtains personally identifiable information of employees or third parties from your workplace, the law will likely require you to notify the affected individuals. Depending on the number of affected individuals and other factors, the law may also require you to notify your state attorney general, certain law enforcement agencies, consumer credit monitoring agencies, and even the media in some cases. Some states also require you to offer 12 months of identity theft monitoring through a third-party service to all affected individuals.

The cost of compliance with data breach laws is significant. A recent study estimates that a data breach in the U.S. costs an organization approximately $214 per compromised record.

Second, beyond the cost of compliance with notification laws, a data breach can disrupt business operations, damage brand reputation and customer relationships, and attract unwanted attention

from government agencies. Even a small data breach can wreak havoc on a business, as one cannot "unring" the bell once certain private information is leaked, taken, or misused.

For example, a departing manager may download and take personnel files – often containing Social Security numbers and other personally identifying information – and then use the information to recruit your top talent to a competitor. In such an example, the departing manager's actions would compromise confidential information and may violate the common law or constitutional privacy rights of the affected employees.

When the dust settles, the loss of top talent to a competitor may be more devastating to your business than the cost of notifying the affected employees of the data breach.

Are You Prepared For A Data Breach?

Privacy laws are numerous across the country and can be quite complicated. That's why you should not wait until after a data breach to learn about what laws apply to your company's data. The first step to prevention is to learn which laws apply to your organization, especially because these laws often impose an affirmative duty to take reasonable steps to safeguard private data.

To date, 47 states, the District of Columbia, and the U.S. territories of Guam, Puerto Rico, and the Virgin Islands have enacted data breach notification statutes. These statutes require businesses to safeguard certain types of employee and consumer information, and to notify affected individuals and government agencies in the event of a data security breach. Businesses in the financial and healthcare industries are also subject to federal laws, including regulations and guidance issued by federal agencies.

Prevention is not, however, simply meeting the minimum legal requirements. You should also allocate resources to identify and implement best practices to secure private data in your workplace. Just as hackers have evolved and become more sophisticated, so too have the best practices necessary to shore up your cyber defenses. What was sufficient five years ago may be inadequate to protect you today.

You put yourself at risk if you simply maintain written policies and protocols but do not conduct regular training, security testing, monitoring, and retraining. You should also provide reminders to employees to be vigilant when handling sensitive information.

Responding To A Data Breach

As it is only a matter of time, eventually you will find yourself having to respond to a data breach. What will you do? Much like getting caught in a rip current at the beach, the worst thing you can do is panic. Breathe deeply and calm down, and then assemble a team to help you through the breach.

IT consultants refer to such a team as a Security Incident Response Team (SIRT). Ideally, your SIRT should be in place prior to a data breach. A SIRT typically includes an IT manager, HR manager, an attorney (whether in-house or outside counsel), the CFO or Controller, and an executive assistant.

Sometimes you may also need a public relations consultant at the table. Each member of the team plays a different role in responding to the crisis.

When there is a suspected data breach, the first course of action is to immediately lock down your data to secure it from any "aftershocks" while you investigate. Your company may later be required to demonstrate that it took prompt and reasonable steps to investigate the breach, attempted to retrieve and secure the information, and notifiED affected individuals.

A data breach can happen even to the best of us, regardless of how much money you spend on computer security. The good news is that there is no absolute strict liability for loss of private data. Where liability often arises is not from the breach itself but from how the company reacts to it, and whether the company had taken reasonable steps prior to the data breach to protect the information.

Follow-Up Steps To Mitigate Damage

In addition to complying with applicable state and federal notification laws, responding to a data breach involves taking follow-up risk mitigation steps. One such step is to consider extending identity theft protection coverage to all affected individuals.

Although not required in most states, companies that experience a data breach often choose to purchase identity theft services for victims, as the coverage provides an added measure of protection and can positively influence victims' perceptions of the reasonableness of the company's response to the breach. However, businesses in Connecticut (which requires 12 months of identity theft coverage at no cost to the victims of the breach), as well as California (which requires that a company that chooses to provide identity theft coverage provide it for a minimum period of 12 months) face mandatory obligations.

Another post-breach mitigation step is to undergo an independent security vulnerability assessment or audit by a third-party IT consultant. This should be done as a routine best practice, but in the absence of an existing practice of conducting security assessments, you should consider undergoing such assessment immediately in the aftermath.

The assessment will identify any gaps in computer security and data breach preparedness and provide recommendations for improvement. While an internal study may help identify some of the issues, such a study could lack the credibility and objectivity of an external and independent consultant whose job is not on the line. Of course, if you are going to commission a security assessment, you should be prepared to implement the consultant's recommendations to prevent or prepare for future data breaches. This is a golden opportunity to create positive evidence of your efforts to understand what went wrong, and your commitment to take the necessary steps to protect private information.

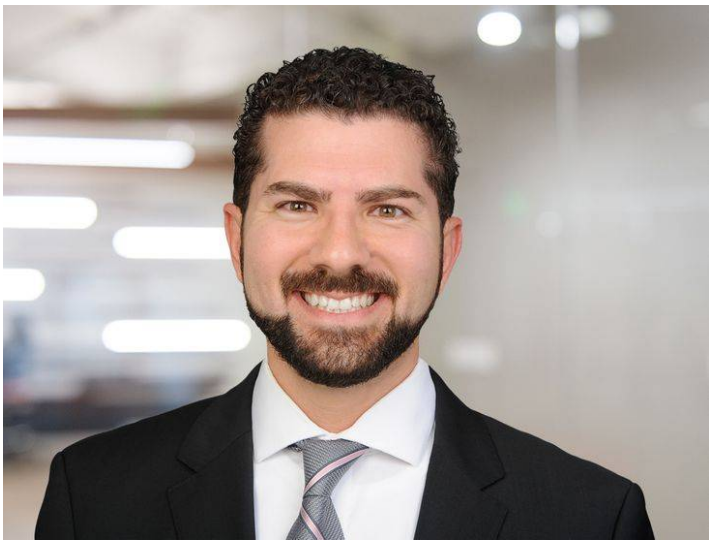
Conclusion

If you are interested in delving deeper into this subject, join us for our complimentary 60-minute webinar: "Data Breach Prevention & Triage: Legal Compliance Before and in the Aftermath," on

webinar: "Data Breach Prevention & Triage: Legal Compliance Before and in the Aftermath," on November 9 at 3:00 p.m. ET / 12:00 p.m. PT. You can register for the session here or at fisherphillips.com/newsroom-events.

For more information, contact the author at UKahf@fisherphillips.com, or 949.798.2118.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber

Counseling and Advice