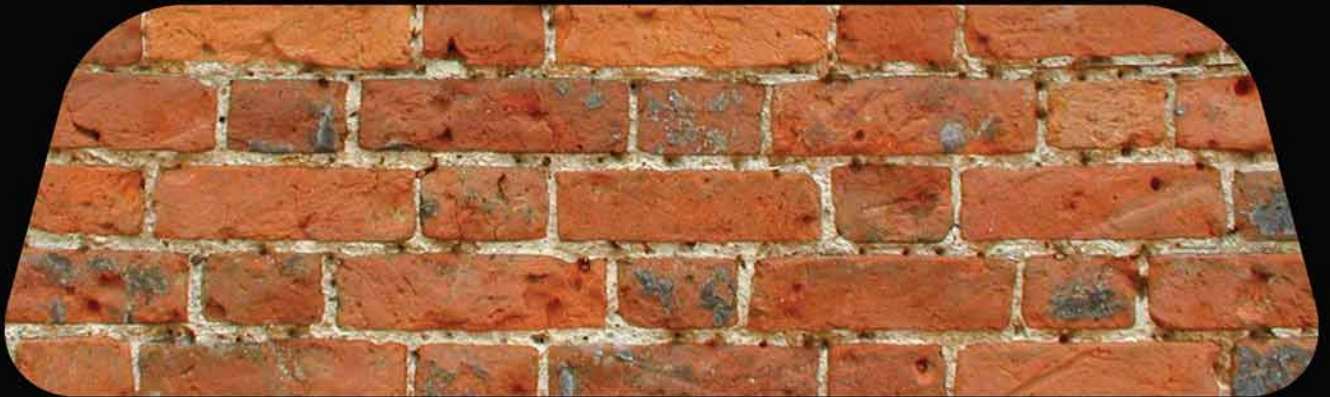


# *Executive* COUNSEL

C-LEVEL INSIGHTS FOR BUSINESS LEADERS



## Addressing Data-Breach Before and After the Fact

By Brian Lapidus

---

# Addressing Data-Breach Before and After the Fact

By Brian Lapidus

Identity theft is the fastest growing crime in America, according to the FBI, although what we are seeing may not be an increase of frequency as much as an increased level of awareness and detection. A stolen laptop used to be viewed as a loss of hardware. Today, both organizations and individuals are acutely aware of the real risks from a lost or stolen laptop: the loss of the sensitive information stored on it. With increasing technology and sophistication, there are extensive networks of identity thieves whose sole purpose is to gain access to poorly secured organizations and extract such information, and their entree might be something as simple as an unguarded laptop.

Damages resulting from data-breach can be extensive. Some of it is obvious – notification costs, loss of customers, lost new business, and damage to the brand that can take years and millions of dollars to repair.

One of the most costly and least publicized

consequences of a data breach is the extensive disruption of business continuity during and after the exposure. To avoid what sometimes amounts to operational paralysis, an organization's leaders need to follow some basic guidelines.

The basics are: Be aware of new attack methods. Stay current on security breach legislation. Establish a comprehensive pre-breach response plan that will enable decisive response and prevent operational paralysis if and when a data breach occurs.

#### LEGISLATION

In 2006, 25 state laws and 34 bills were introduced in the U.S. Congress related to identity theft resulting from corporate data breaches. The California Security Breach Information Act, the basis for all other state laws, requires organizations that store personal information to inform those whose information has been compromised. The California law and its counterparts in other states require companies to notify residents whenever their personal information is reasonably believed to have been obtained by an unauthorized person.

Under the law, "personal information" generally means an individual's first name or first initial and last name, in combination with one or more of the following data elements: (1) Social Security number, (2) driver's license number or state ID card number or (3) account number, credit or debit card number, in combination with any required security code, access code or

office with file folders, where sensitive data is stored and destroyed, who has access to sensitive data, and whether employees are required to surrender keys and badges upon leaving the company's employ.

Pre-breach preparedness is key. Because corporate data breaches often cause panic and highly emotional reactions, it is recommended that a third party corporate breach and data security expert be retained to analyze the level of risk and exposure. Experts can generally move very quickly, sometimes within 48 hours, to help contain the damage and help the CIO or risk manager with the latest methods of attack and recovery.

A tested response plan should be part of such an analysis and should be disseminated throughout the management structure. Everyone should know what to do if a breach occurs.

Organizations that can demonstrate that they have taken prudent, anticipatory steps to address the threat are more likely to be viewed in a favorable light by consumers and regulators alike should a breach occur.

To begin devising a critical response plan, start with these key steps:

---

## NEGLIGENCE IN CORPORATE SECURITY CAN NOW LEAD TO CLASS ACTION LAWSUITS AND COSTS IN THE MILLIONS, TO ADDRESS BOTH LIVES THAT HAVE BEEN HARMED AND DAMAGE TO THE BRAND.

---

password that would permit access to an individual's financial account.

The California law, which went into effect July 1, 2003, was created to help reduce the incidence of identity theft as well as provide response guidelines to companies that experience it.

#### AWARENESS AND DEFENSE

Awareness of data-breach methods and ways to thwart an attack are key to reducing exposure. Following are some simple steps to elevate awareness and establish a better defense:

- Educate employees about appropriate handling and protection of sensitive data.
- Consistently enforce policies and procedures, physical safeguards, and IT security. All three are required.
- Review and revise physical security practices as needed, in both bricks-and-mortar and virtual operations. Address all the critical areas, such as who can leave the

- Identify and involve people who will have a role in reviewing policies and procedures on a predictable timetable.

- Pinpoint physical security elements. Determine when and how they need to be tested.

- Partner with a corporate breach and data security expert to map a response strategy.

Your response plans should detail, among other things, who is in charge of any internal investigation, which law enforcement agencies to contact and when, and how to deal with the media.

Maintain a good relationship with local, state and federal law enforcement throughout the investigation. A positive report about a company's cooperation with law enforcement goes a long way toward maintaining brand integrity.

Sound cyber-security practices enable a company to determine quickly when an attack occurred, who might be responsible, and what data was compromised. This helps the company provide more

information to law enforcement and can result in the case getting greater priority.

A corporate data-breach response plan must include procedures for notifying individuals whose personal information has been exposed. Each situation is unique and needs to be treated with extreme caution and consideration. A third-party expert can be an important ally here, by helping to ensure the scope of the breach is accurately assessed, providing resources for high-volume notifications and offering call-center support for the hundreds, if not thousands, of concerned consumers who will need information about what has happened and how they can get help.

Data minimization should not be overlooked as an element of preparedness. Organizations often collect as much client information as possible and store it indefinitely, on the grounds that it will help them better understand the client base. But companies are starting to realize that large volumes of information increase the likelihood of a breach.

Data minimization needn't result in the loss of "customer intimacy." Companies should collect only the information they need and use regularly,

making the decision to notify persons whose information has been leaked.

It is critical that third-party vendors with access to personal data also abide by appropriate information security procedures. Breach notification laws make no exception if a third-party contractor compromises sensitive data. Organizations must confirm that their contracts require vendors or subcontractors to provide immediate notification of suspected breaches. They also should allow the organization to participate in the investigation and exercise control over decisions regarding external reporting.

#### **MORE CONVENIENCE, BIGGER THREAT**

Market demand for speed and convenience has created business systems that accommodate data portability and transfer for almost any type of transaction. But such widespread use of sensitive personal information has allowed identity theft to escalate way beyond mere hacking. In the past several years, dozens of companies have suffered security breaches that negatively impacted their brand and economic future. The toll continues to rise.

---

### **ONE OF THE MOST COSTLY AND LEAST PUBLICIZED CONSEQUENCES OF A DATA BREACH IS THE EXTENSIVE DISRUPTION OF BUSINESS CONTINUITY DURING AND AFTER THE EXPOSURE.**

---

keep it in as few places as possible and only for as long as is necessary, and dispose of it responsibly once it's no longer of use.

Some practices can result in unexpected kinds of liabilities, and should be addressed with special care. For example, it is best to encrypt personal information, but it's foolish to rely on encryption as a method of defense. Although the majority of state statutes require notification only if a breach compromises unencrypted personal information, encryption alone is not enough and gives many organizations a false sense of security.

Keep in mind that organizations that encrypt personal information may avoid initial notification obligations, but will face harsh penalties when the data is then unencrypted by a professional data thief.

The data-breach response plan should require that key decision-makers be alerted immediately when an incident is detected. The statutes come into play as soon as the IT department detects the intrusion, so an organization's response plans should include timely reporting to those responsible for

Ignorance is no longer a defense. Negligence in corporate security can now lead to class action lawsuits, as well as the millions of dollars often required to address both lives that have been harmed and damage to the brand.

To avoid those expensive negative outcomes, companies need effective pre-breach response plans, focusing on employee education and awareness, as well as security audits and reviews. They also need action plans for when a breach occurs, plans that address business continuity, notification and all crisis-communication issues.



*Brian Lapidus is vice president, strategic development, at Kroll Fraud Solutions. In a former consultancy he reorganized the Chief Information Office of the U.S. Department of the Treasury and created a program for Goldman Sachs analysts that is still in use. He helped establish Kroll's identity theft restoration unit in Canada and is now working on the pending establishment of a Kroll Fraud Solutions presence in the UK.*