How Ready Is Your Company to Respond to a Data Breach?

5 key questions to test your company's responsiveness

Harry A. Valetk
Special to Law.com
July 10, 2008

Everyone is grappling with self-reported data spills. Indeed, organizations of every size, public and private, here and abroad, are feeling the fast-paced, disruptive economic sting of an unauthorized sensitive information leak. According to the Privacy Rights Clearinghouse, since 2005, over 800 data breaches have been made public, affecting over 229 million U.S. customer records.

And while organizations strive to navigate the complex regulatory landscape, they also struggle to inform their customers soon after an incident occurs. In April 2008, for example, the Ponemon Institute published findings from a study of 1,800 data breach notice recipients.

That study found that most organizations take an average of four weeks to report an incident. That's twice as long as California's recommended 10 business days. And four times longer than consumers expect: those same Ponemon study respondents expected notice within a week of an incident. Last year, New York's attorney general even sued CS Stars LLC for waiting seven weeks to self-report a data spill.

This suggests two desired outcomes. The first is obvious: avoid a data breach in the first place by adequately protecting your personal information. Especially, since according to a 2008 Verizon Data Breach Investigation report, 87 percent of data breaches occurring in the past 4 years were considered avoidable through reasonable controls. The second, however, is to plan ahead. Think about how you can help your organization respond before an incident occurs.

With this in mind, here are five key questions to see if you're ready to respond swiftly and effectively in case the inevitable occurs.

1. Do you really know the law?

With over 45 varying U.S. laws (including the District of Columbia, Puerto Rico and the Virgin Islands), keep a watchful eye on the regulatory scheme. Knowing what and when to do it is critical to how you respond. Some jurisdictions modify or add new requirements to existing law. And some have unusual requirements.

For example, unlike most statutes, New Jersey's data breach notice law requires you to notify law enforcement *before* notifying your customers.

Attorney Harry A. Valetk

ARTICLE TOOLS

Printer-friendly Version
Email this Article
Comment on this Article
Reprints & Permissions

Under §56:8-163c(1):

> "Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Policy in the Department of Law and Public Safety ..."

In practice, this means that if you're involved in a multi-jurisdictional incident, you may need to hold all of your notices, or segregate notices to New Jersey residents, until you reach New Jersey authorities. Maryland's data breach law (§14-3504(h)) also has a similar requirement.

Other states have a broader definition of sensitive information. North Dakota, for example, requires notice even when companies lose seemingly harmless information like an individual's name combined with date of birth.

A handful of states (Hawaii, Indiana, North Carolina, Wisconsin, Massachusetts and South Carolina) also have specific notice requirements for hard copy materials. This means you must notify residents of those states if a document containing sensitive personal information is somehow misdirected by mail or any other means.

2. Do you have a ready list of contacts?

Obviously, you should maintain a list of key players. But don't limit yourself to only internal sources. To react promptly, keep a list of external contacts too.

Take, for example, law enforcement personnel. Connecticut allows you to avoid notifying victims about an incident if the breach will not likely result in harm to those individuals. But the statute requires you to consult law enforcement authorities at every level for your harm analysis. Specifically, under §36a-701b(b):

> "[Consumer] notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state, *and* local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."

Scrambling to find the right law enforcement contacts in the throes of a data breach investigation can add to your delay. Instead, consider doing the legwork ahead of time. For this purpose, InfraGard can be a good source for networking within the law enforcement community.

But that's not all. Most next-day delivery carriers (e.g., FedEx, UPS, DHL) have investigation teams devoted to package recovery. If your organization is unable to find a package containing sensitive personal information, these teams may help beyond the traditional tracking channels.

3. Do you have easy-to-use templates?

We learn from experience. So use templates to manage your incidents consistently. For example, as part of your initial fact gathering, create templates asking questions that will help you efficiently chart your organization's next steps.

- What type of information (e.g., name, SSN) was lost, stolen, or misdirected?
- What format was the information in (e.g., hard copy, electronic)?
- Was the information encrypted or anonymized?
- How many victims were affected?
- What states do those victims reside in?
- Did you recover the lost, stolen, or misdirected information?

You should also have approved notice templates ready. That way, you can streamline any time-consuming approval process. Generally, your main template should:

- Explain the facts in *plain English.* This is a public communication with customers. Make it user friendly by avoiding legalese.
- Identify the type of information lost and when it was lost.
- Specify what you're doing to protect your customers.
- Mention if you've recovered lost files or misdirected documents. Most consumers worry about identity fraud, so try to ease their concerns.
- Avoid marketing any products or services. That's just bad timing.

Some states, however, also impose specific content requirements. In Maryland (§ 14-3504(g)), for example, your letter must include:

- Description of compromised information categories
- Your organization's address and telephone number
- Toll-free number for the major consumer reporting agencies
- Toll-free number, addresses, and Web sites for the Federal Trade Commission and Maryland's Attorney General's Office
- A statement explaining how individuals can use these sources to avoid identity theft

Massachusetts has similar content requirements. But, taking a peculiar step in the opposite direction, Massachusetts' law (chapter 93H of § 3(b)) actually prohibits your notice from including details about the nature of the breach or the number of affected residents.

4. Do you have all the right vendor relationships in place?

If you shop now, you'll save later. So ask if you have the right relationships in place. Do you have consumer credit protection services? How quickly can you mail your data breach notice letter? Do you know how much call volume your customer response center group can handle? No doubt, these are resource questions best answered before an incident occurs. That's why it pays to shop the marketplace, and help your organization get desired results.

For example, most companies offer breach victims 12 months of free credit monitoring. But, recently, Connecticut Attorney General Richard Blumenthal and others have insisted on greater protections. Can your existing credit protection services vendor offer monitoring for 24 months? Do they offer identity theft insurance?

While you're at it, examine the nuts and bolts of your mailing process. Work with your team to standardize mailing requirements (e.g., paper type and envelope inventory), streamline your turn-around time (usually 48 hours), and expedite any approval process connected to mailing out those notices.

Once those letters go out, however, your customers will start calling. Again, depending on your organization's size, set up a standard data breach response telephone number. Work with your call center representatives to train a team of operators to handle those calls. And explore options in case your call center team can't handle call volume internally.

5. Do you know what your customers think?

Finally, every incident involving personal information loss presents a reputational risk to your brand. According to the Ponemon Institute's April 2008 study, 31 percent of breach notice recipients said that they terminated their business relationship, and 57 percent reported losing trust and confidence in the organization.

Unfortunately, most companies get so involved investigating and managing compliance that they neglect to measure how the incident impacted their brand. A smart practice here is to work with your public relations and brand reputation partners to survey your customers shortly before and after an incident occurs.

Some organizations even use Omnibus surveys as part of their data breach response plan. Omnibus surveys offer companies experiencing a data breach a way to quickly and cost-effectively measure consumer reaction by buying proprietary content on existing surveys. Those surveys aren't necessarily limited to your customers, but they offer immediate access to a broad consumer pool.

Bottom line, don't wait for a breach to get answers to these questions. As in-house counsel, play a leadership role in helping your organization improve its readiness. Search for key support vendors now. And even if you have existing relationships in place, don't assume you're getting the best products and services. Instead, shop around on a regular basis, and renegotiate any existing terms or fees before a breach occurs.

Remember, if, despite your best efforts, a data breach still occurs, when and how you respond can either mitigate or intensify the legal and economic fallout.

Harry A. Valetk is a new media and privacy attorney in New York City. He has written extensively on Internet safety, identity theft and privacy protection topics. He is also an adjunct assistant professor at the Bernard M. Baruch College, Zicklin School of Business, and a former trial attorney with the U.S. Department of Justice. Email: harry@valetk.com