SearchCIO-Midmarket.com
TECHNOLOGY MANAGEMENT STRATEGIES
FOR THE MIDMARKET CIO

DATA BREACH!

2 *The Art of Fessing Up*

6 *Bills for a Federal Breach Notification Law Languish in Congress*

10 *CIOs Under Fire and in Front of the Camera*

As data loss from careless employees or thieves becomes ever more common, every organization should have a plan to notify its constituents if personal information is lost. Here's the latest on legislation, how to create a plan and whether you, the CIO, should be in the public eye if the undesirable happens.

By Zach Church

TechTarget
The IT Media ROI Experts

The Art of Fessing Up

Drafting a notification plan before a data breach happens can help you save face—not to mention legal wrangling.

MICHAEL SHERER, DIRECTOR of IT at Goshen College in Indiana, is one of the initiated. Last year, a hacker accessed the college's admission server, compromising the personal data of 7,300 students and parents. Under state law, the college was required to notify all those involved of the breach.

In 2007, there were 329 reported security breaches in the U.S., according to the Privacy Rights Clearinghouse. That's millions of names, Social Security numbers, credit card numbers and other personal information lost by or stolen from universities, government agencies and private businesses (small and large).

A few of those breaches remain high-profile, like the one involving Framingham, Mass.-based The TJX Cos., which reported in January 2007 that credit card information for as many as 94 million customers was compromised. And there were the lesser-known breaches, such as incidents at Goshen College and a bank in Wichita, Kan., where a hacker viewed personal data of some 20 customers.

Whether a breach or data loss makes headlines or not, keepers of personal data are required by state law to notify customers (and other concerned parties) when data has been compromised. California was the first state to require notification, the result of a 2003 law written after hackers accessed state employees' personal information in 2002. Other states soon followed suit, though the laws are far from uniform. Today, 42 states and the District of Columbia have passed some form of data breach notification legislation. The remaining eight states are considering similar bills.

BETTER TO HAVE AND NOT NEED

Security breaches happen even to the prepared, even to the properly secured. But though losing personal data to thieves takes control from the hands of IT, CIOs do maintain some control over what happens afterward. Experts say readiness is the key to a successful breach notification response.

"You shouldn't assume just because you have a crisis communications plan that it actually covers a data breach," said Jim Maloney, president and CEO of Cyber Risk Strategies LLC in Santa Fe, N.M., and a

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

breach notification consultant. "One of the worst things would be to get the call from the media to have to explain this or having to scramble to put together about 20 different breach letters."

A company must comply with the notification law for each state where a customer whose data has been lost resides. And it's complicated. Each law differs, from its definition of "personal information" to the amount of time allowed between breach discovery and notification and to what mitigating factors allow exemption from the law (see "State Laws," page 7).

That's a lot of detail to dig into while simultaneously containing a breach, especially for midmarket companies less likely to have in-

Case Study: Notification in Five Days

WHEN A HACKER gained access to students' personal information at Goshen College in Indiana last May, IT director Michael Sherer had to helm the state-mandated notification process. Staff members at the school managed to complete the process in the first five days. The timeline:

DAY 1 A Sophos product detects an attack on workstations. The source of the attack is a server in the admissions office. The server is taken offline and the breach is determined to be a hack. Internal forensics begin. The nature of the breach triggers the Indiana notification law. Working with admissions, IT determines exactly whose records were viewed. A first-draft notification letter is written. Collaborative work begins with public relations, student life, legal counsel and other school departments.

DAY 2 Legal counsel determines that letters must go to all affected students, not just Indiana residents.

DAY 3 The state attorney general's office is contacted.

DAY 4 A phone hotline is established. The letter is finalized and approved by legal counsel. Public relations develops a set of message points and frequently asked questions for staff speaking with the public. The letter is sent to 7,300 potentially affected people. Public relations statements are released on the college's website.

DAY 5 Unused Social Security numbers are removed from system. Three major credit agencies are notified of the breach. ■

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

house legal counsel, press officers or dedicated information security departments.

Sherer elected to draft just one letter as he faced notification. His 10-person IT staff was consumed with learning how a hacker accessed an admissions server and whose personal information may have been viewed.

"There was in no way any effort to say 'Oh, what is Kansas asking?'" Sherer said. "I think the assumption was 'If we act in good faith, in accordance with Indiana law and we notify everybody, then we'll be OK."

For the most part, his team was. Although the hacker could have viewed personal information, no one has reported identity theft or credit fraud, Sherer said. Both the state attorney general and FBI were notified, but neither elected to open a criminal investigation, he said.

Sherer drafted his letter, which was sent to most people by email, by researching other data breach letters and mimicking them where he thought it was appropriate.

"We'd actually gotten a similar type of disclosure from a dental insurance company that had exposed our students' data, so we had been familiar with that kind of communication," he said.

The college's initial response was quick, Sherer said, because it already had a crisis response team in place, meaning it was simply a matter of assembling the players, including legal counsel, public relations and the student affairs office.

PRE-EMPTIVE STRIKE

Maloney suggests CIOs develop a pre-emptive plan, one that includes a sit-down with IT, a lawyer and whoever would direct media relations for the company in the event of a breach.

Many state laws require some description of how the breach occurred. The CIO should bring technical expertise to the table, ensuring the statement is accurate and that it doesn't compromise any active criminal investigation. Attorneys should be on hand to make sure the statement protects the company from any potential litigation.

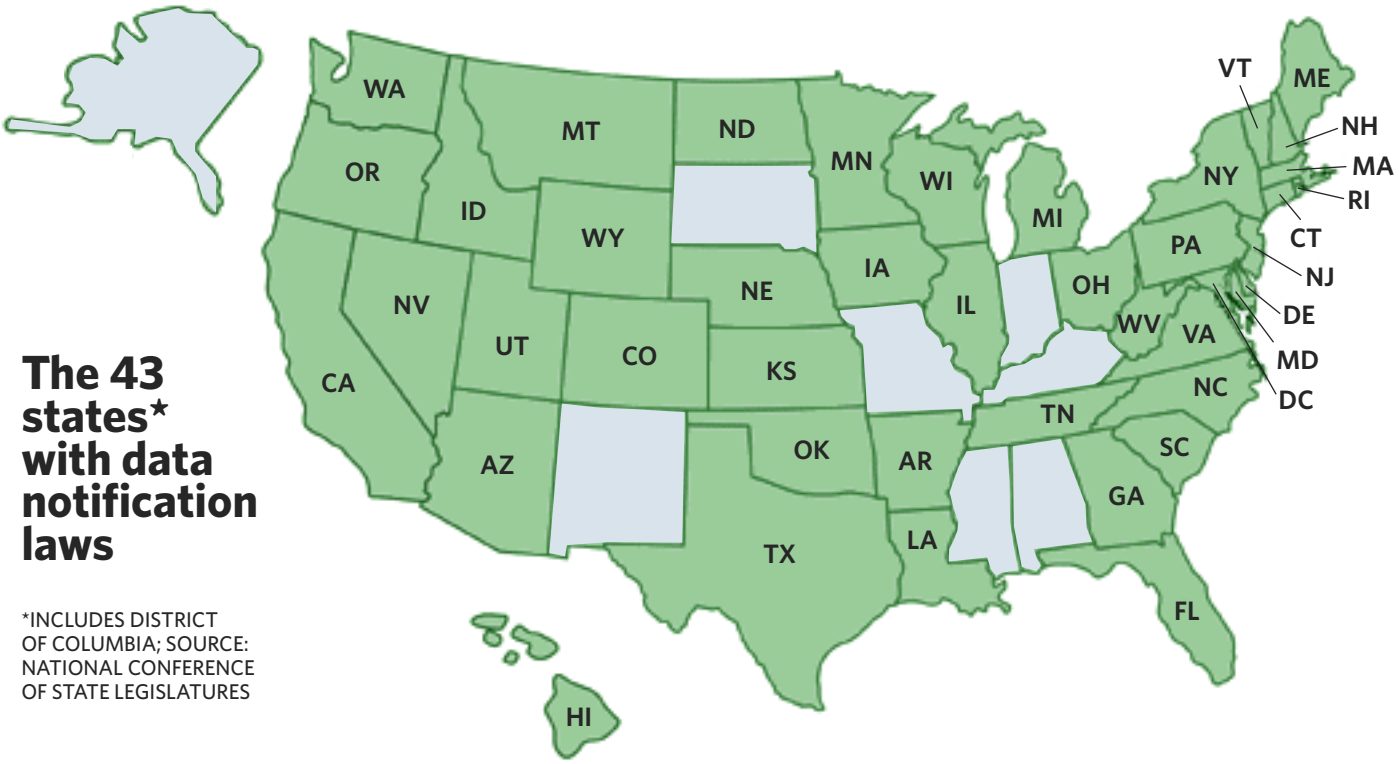
"Because it's that three-way thing, you don't want to get those people together in a room for the first time to craft some of these letters," Maloney said. Time and money can be saved,

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

The costs of the notification procedure have gone down, dropping from $25 per customer in 2006 to $15 per customer last year, although companies lost, on average, $197 per record lost or stolen in 2007. —SOURCE: THE PONEMON GROUP



The 43 states* with data notification laws

*INCLUDES DISTRICT OF COLUMBIA; SOURCE: NATIONAL CONFERENCE OF STATE LEGISLATURES

he suggested, by analyzing the spectrum of state laws in advance to find a sort of highest-bar standard that can be met with only one or two different notification letters (some state laws also allow phone calls and emails).

All of the advance work goes to cost savings. Companies lost, on average, $197 per record lost or stolen in 2007, an increase from $182 the year before, according to a recent study by the Ponemon Institute. Of that, $128 per record is the result of "customer churn and acquisition" in the wake of a breach.

Surveying 35 companies that experienced a breach, the study found the average total breach cost to be $6.3 million, which includes $4.1 million from lost business. The costs of the actual notification procedure have gone down, though, dropping from $25 per customer in 2006 to $15 per customer last year.

Sherer said the actual cost of his notification process was low, mostly because the college was able to send emails to most of the affected people. The time investment, he said, was huge. But going through the notification helped improve record-keeping at the school, with staff ditching unused personal information the school no longer had reason to keep, he said.

"When you have just taken every leader in the college and you've had to eat humble pie before all sorts of constituencies, that becomes a good opportunity to talk about how you're going to improve your security protocol," Sherer said. ■

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

Bills for a Federal Breach Notification Law Languish

Congress isn't short on options for a federal data breach notification law. But it doesn't appear to be a priority.

THE CORNUCOPIA OF state data breach notification laws—only eight states are without notification requirements—makes for a confusing process.

CIOs prepping a notification in the wake of a breach of personal information must comply with the law for each state in which a customer lives. That could potentially mean following at least 43 different laws (the District of Columbia has also passed legislation).

Yet federal lawmakers have yet to pass a similar law, though not for lack of trying.

Currently, Congress has its hands on no fewer than nine different bills that would establish some sort of uniform notification procedures. Three of those are specific to federal agencies and would not affect private businesses.

But the other six would. And from a response perspective, that could be a good thing.

"These federal bills, almost all of them, would pre-empt the state ones," said Tanya Forsheit, a partner at Proskauer Rose LLP in Los Angeles.

"A federal omnibus data protection law would obviously impose uniformity and greatly simplify the issue of when notice has to be provided and under what circumstances," said Forsheit, who specializes in privacy and data security compliance law.

That could be especially beneficial to midmarket IT departments, which work with smaller staffs and may not have legal counsel on hand in the company.

Forsheit singled out two Senate bills as having the most traction right now. S. 495, known as the Personal Data Privacy and Security Act of 2007, is sponsored by Sen. Patrick Leahy, D-Vt., but is given equal support by Texas Republican Sen. Arlen Specter.

S. 239, known as the Notification of Risk to Personal Data Act of 2007, is sponsored by Sen. Dianne Feinstein, D-Calif. The bill made it through the Senate Judiciary Committee last year and has been untouched since then.

"There hasn't been any action on most of these for a very long time," Forsheit said. "Most of the bills have been languishing for almost a year, or in some cases, a year now."

Many of the bills are simply updated versions of legislation that stalled in Congress in previous sessions.

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

Leahy's bill, too, has been in limbo since last May, when it was reported out of the judiciary committee and placed on the Senate calendar. Along with Feinstein's bill, it now awaits scheduling for floor discussion by Senate Majority Leader Harry Reid, D-Nev.

But neither bill has received that shot at moving forward, despite a recent push from Leahy and Specter to bring their bill to fruition.

On March 25, the two senators revived their calls for a law, citing the news that State Department employ-

State Laws: Watch out for These Key Elements

COMPANIES THAT LOSE personal data are required to follow the law set by the state in which the data's owner lives. Here are some idiosyncrasies to watch out for:

- **Definition of "personal information":** Most laws define this as part of a name combined with a credit card number, Social Security number or other identifying digits.

- **Breach procedures:** Pay attention to how quickly notification must be made and exactly what information a letter or call must include.

- **Exemptions:** Many states exempt companies already beholden to the notification guidelines in the Health Insurance Portability and Accountability or Gramm-Leach-Bliley acts. Some states also allow an out if the compromised data is properly encrypted.

- **"Likelihood of harm":** Some states don't require notification if it's unlikely any fraud or identify theft will be committed using the lost information.

- **Delays:** Most states allow a delay in notification if law enforcement authorities request one to complete an investigation.

- **Safeguards:** A handful of the state laws also require security measures before a breach. In Texas, for example, personal information must be disposed of by "shredding, erasing or otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means." **—z.c.**

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

ees had snooped into the passport records of the three major presidential candidates. That was just one of their examples.

"This week, front-page headlines have delivered news about the theft last month of personal information from the National Institutes of Health," the Senators wrote in a March 25 letter to Reid and Mitch McConnell, the leading Senate Republican, of Kentucky.

Busting Compliance Myths

SECURITY BREACH NOTIFICATION laws generally require a company to notify individuals whose personal information may have been compromised after a security breach. There are 45 laws on the books (including 42 states, two cities and one territory). Three of the state laws take effect by mid-2009 (Virginia, West Virginia and South Carolina). While these laws are similar in many respects, there is often confusion about how or with which to comply. Here are three commonly held myths, debunked:

Myth 1: Every security breach requires notification of all consumers whose information was lost.
To the contrary, if certain conditions are met, several of the 45 laws relax notification requirements (for example, if the lost information is encrypted or otherwise inaccessible, or if it's determined that the breach is unlikely to cause harm).

Myth 2: A company must comply with only the law of the state or territory where information was lost or where the company is incorporated.
The residence of the individuals whose information was lost, coupled with the location of the company in some states, determines the applicable law, and each state's, city's or territory's law applies to only its residents. If the information of residents in Ohio and Tennessee is compromised, a company must comply with the Ohio law for affected Ohio residents and the Tennessee law for affected Tennessee residents.

Myth 3: If I comply with the California law, I have complied with all state laws.
California's security breach notification law was the first, and is perhaps the most well known, but it is not the most stringent. There is no single law with which you can comply in order to comply with all others in all circumstances. It is critical to comply with each law applicable to your situation. ■

—Matt Karlyn, Foley & Lardner LLP, Information Technology & Outsourcing Practice Group

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

"Earlier reports have involved virtually every department of the federal government," they wrote.

The two argued their bill would "provide protections for consumers, including a timely notification of data security breaches." The bill would also require government contractors to properly safeguard personal information, the senators wrote.

Senator Barack Obama, D-Ill., became a cosigner of the bill on April 1. The bill was introduced in early 2007.

S. 495 would require consumer notification "without unreasonable delay" if "sensitive, personally identifiable information" is lost, stolen or otherwise viewed.

That is defined as a person's first and last name, or first initial and last name, combined with a complete Social Security number, driver's license number, passport number or alien registration number. Financial account and credit card numbers combined with a security code or password also qualify. There are also provisions for certain combinations of names and addresses, telephone numbers, birthdays and a mother's maiden name. Finally, data like fingerprints and iris images are also covered by the bill.

Reasonable delay is defined as time required to determine how large the breach was and prevent a further breach. Delay is also acceptable with the OK of federal law enforcement agents.

Exemption from notification is also allowed if the information is encrypted in such a way that creates "no significant risk" in harm.

The bill allows for notification by mail, phone or email. Media notice is required if more than 5,000 people could be affected in a particular state. The notification must include a description of what information has been taken and toll-free numbers to contact the business and credit reporting agencies. It allows for states to require the business to provide information about victim protection assistance.

Credit reporting companies would also need to be notified if more than 5,000 people could be affected—an increase from 1,000 in a previous draft of the bill. Law enforcement notifications are also required in certain circumstances.

Feinstein's bill closely mirrors S. 495. It does not, however, include the Leahy bill's requirements for businesses to establish a "data privacy and security program."

Forsheit said there is some talk from consumer groups looking for a law that would require notification in the event of any data breach, though most of the bills have requirements like the encryption exemption.

But otherwise, she said she sees no major sticking point or debate that is holding the bills back. Breach notification does not appear to be a partisan issue, as evidenced by the dual support from Leahy and Specter.

Forsheit's best guess for the lack of movement? Congress has other issues to deal with. ■

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

CIOs Under Fire and in Front of the Camera

CIOs, qualified to speak accurately about data loss, may make the best spokespeople in a time of crisis.

THERE'S NO MISTAKING the CIO during a data security breach. He's the guy scrambling to figure out what happened and how to rectify the problem. But it appears the days when the CIO was the scapegoat for a breach are behind us. In fact, some experts suggest that the CIO is the best executive to handle questions from the media in the event of a data leak. If the idea catches on, CIOs could find themselves in front of the camera, instead of facing a firing squad (although that may seem like the same thing).

So they need to be ready.

With 42 states (as of press time; see sidebar) requiring public notification in the event of a data security leak, how a company handles itself is critical. Running from the TV cameras and news reporters could negate all the business value that comes from a swift, lawful notification process. In most cases, it's the public relations executive handling the press, but Jim Maloney, president and CEO of consulting service Cyber Risk Strategies LLC in Santa Fe, N.M., said companies might want to rethink that strategy.

"I think [customers] would appreciate it if the CIO, the CSO were the spokesperson as opposed to the PR person. I think they'd like to see that person up front facing the music," he said. "It can send the wrong message if it's marketing or PR."

Putting a CIO out front as a media contact could be a good idea, said Mark Bernheimer, principal at Los Angeles-based MediaWorks Resource Group, a media training agency.

"It's much more advantageous [for the news] to come from the company itself than from a furious customer or authorities."

—**MARK BERNHEIMER**, PRINCIPAL, MEDIAWORKS RESOURCE GROUP

But allowing a CIO who lacks media savvy to speak for the company is a bad idea.

"C-level executives have to always remember they can do everything the law requires and do exactly what the law requires of them and simultane-

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

ously lose the PR battle," said Bernheimer, a former CNN reporter. "If this is going to be a case where it's only a matter of time where it becomes a public matter, then it's much more advantageous [for the news] to come from the company itself than from a furious customer or authorities."

By leading the IT department, Maloney said, CIOs are uniquely qualified to speak accurately about exactly how a data breach occurred and how the company has since secured itself. The presence of the top IT officer would ideally add a weight of authority to the company's public comments.

As with the legally mandated notification, a company spokesman will have to speak accurately without giving out more information than is necessary to inform the public and assure customers that the company is back in control.

But Bernheimer said the preparation of a media plan can't be reactive. There simply isn't enough time after a data breach to determine who will speak for the company and prepare that person for challenging confrontations with reporters.

THE ART OF FESSING UP

BILLS FOR A FEDERAL BREACH NOTIFICATION LAW LANGUISH IN CONGRESS

CIOS UNDER FIRE AND IN FRONT OF THE CAMERA

FESS UP, CLEAN UP, DON'T LET IT HAPPEN AGAIN

Bernheimer said a data breach response should contain three elements:

- The company must first take responsibility for what has happened, a tricky line to walk if there is the potential for litigation.

- The spokesman must be able to show the company knows and can explain what has happened. That's where Maloney said the CIO could make a positive impression.

- The company must also explain how it will stop a data breach from happening again, another spot where the top IT officer carries weight.

Media training programs like Bernheimer's usually consist of a day of training, as well as time for follow-up consultation. At MediaWorks, C-level executives face professional television cameras and Bernheimer pelts them with tough questions. Executives learn how to carefully phrase answers to questions and find where reporters might "cut you some slack," Bernheimer said.

But as with all other aspects of a data breach response and notification, media training for CIOs is moot if it isn't conducted before a breach actually occurs. In the wake of an incident, the deadline-driven media world won't wait for a company to train executives on how to answer questions.

"In many ways, it's too late," Bernheimer said. "The perception is they've waited to level [with the public]." ■

Zach Church is a news writer for SearchCIO-Midmarket.com. He can be reached at zchurch@techtarget.com.

FROM OUR SPONSOR

About McAfee

With headquarters in Santa Clara, California, McAfee, Inc. (NYSE: MFE) creates best-of-breed computer security solutions that prevent intrusions on networks and protect computer systems from the next generation of blended attacks and threats. Offering two families of products, McAfee System Protection Solutions, securing desktops and servers, and McAfee Network Protection Solutions, ensuring the protection and performance of the corporate network, McAfee offers computer security to large enterprises, governments, small and medium businesses, and consumers.