

# BREACH PATROL

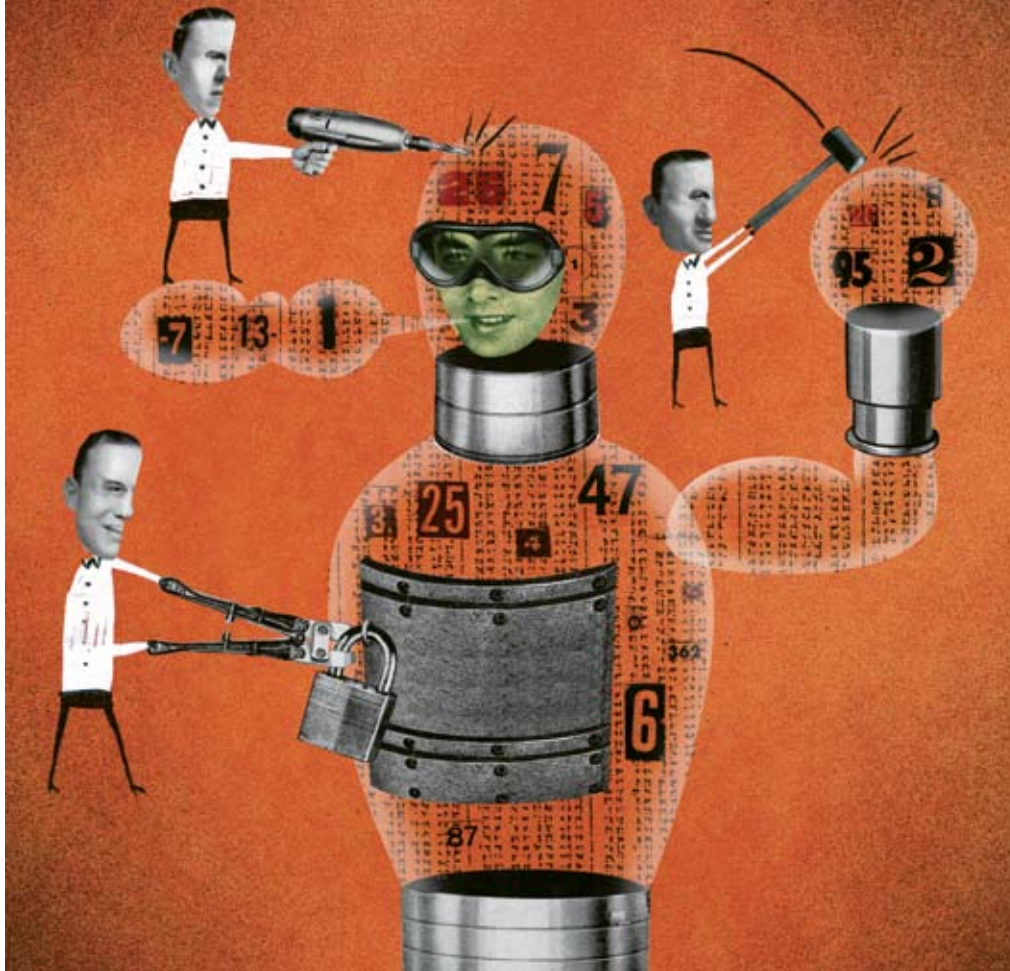


Illustration by David Plunkert

**I**n today's digital world, most Americans leave long electronic trails of private information wherever they go. But too often, that data is compromised. When they shop—whether online or at brick and mortar stores—retailers gain access to their credit card numbers. Medical institutions maintain patient records, which are increasingly electronic. Corporations store copious customer lists and employee Social Security numbers.

These types of data frequently get loose. Hackers gain entry to improperly protected networks, thieves steal employee laptops or disgruntled workers pilfer company information.

"More and more people are putting their data in electronic form," says Deirdre Mulligan, the faculty director at the Berkeley Center for Law and Technology. "[This] means the number of instances where we might have a breach is going up."

On the following pages, *InsideCounsel* takes a look at fallout from some major data breaches, recent legislative and regulatory developments in data privacy law and ways to prevent a data breach before it's too late.

By Christopher Danzig, Mary Swanton and Lauren Williamson

# Data Disasters

A “global cyber fraud operation” sounds like something straight out of a James Bond movie. But when cyber crooks recently infiltrated Heartland Payment Systems’ processing system and accessed potentially tens of millions of credit card numbers, company executives learned that type of criminal activity is very real.

In January, MasterCard and Visa notified the credit card processing company that suspicious activity occurred during 2008. Heartland launched a forensic investigation with help from the U.S. Secret Service. They found malicious software spying on transactions and recording credit card information as it passed through the processor’s network.

While Heartland is still trying to determine how many records were compromised, some speculate this is the largest data breach incident ever. A class action lawsuit filed in New Jersey Jan. 27 seeks to recover the cost of replacing credit cards and reimburse banks for expenses related to any fraudulent activity connected with the breach.

Though the Heartland incident is a dramatic example of a data security breach, malicious software placement is just one cause—and not nearly the most common. Only 22 percent of breaches occur as a result of outside hacking, according to a study released in March analyzing breaches by sector.

“The categories are virtually limitless,” says Kirk Nahra, a partner at Wiley Rein and chair of its privacy group. “Any company that has information about either customers or employees has to worry. [When I say that,] people stop and think for a second, ‘Well, every company has either customers or employees.’”

## PDA Problems

Data compromises occur most often through lost or stolen hardware such as laptop computers or PDAs, though many people don’t realize it because those inci-

dents get less attention.

“It’s a juicier story if someone was monitoring the wireless network and stealing credit card information,” says Robert Scott, managing partner at Scott & Scott. “Those megastories get big because there are a lot of people affected, and there’s some sort of drama that’s different than just losing a PDA.”

The health care industry has the highest percentage of breaches from lost hardware, says Matt Curtin, founder of the Web consulting firm Interhack. Curtin co-authored the recent breach study.

“It’s a reflection of the kind of environment they’re working with,” he says, noting the quantity of small devices such as smart phones used in health care.

Losing a BlackBerry might not seem like a big legal deal, but without quick action what first appears to be an inconvenience can soon spiral into major litigation.

A massive breach hit the Department of Veterans Affairs in 2006 when two teenagers stole a laptop from a VA employee’s home. The data included Social Security numbers, birth dates and spousal information records from 26.5 million veteran and active military personnel.

Authorities successfully recovered the laptop before any of the data leaked, but in January the VA reached a \$20 million settlement in one of several class action lawsuits filed after the theft. Every potentially affected person can claim up to \$1,500 in damages for emotional harm and credit monitoring



expenses, even though no actual identity theft occurred.

“This really wakes up the government on what kind of liability can be involved here, and how liability can exceed the harm,” Scott says.

That’s significant because most lost hardware incidents requiring public notices to people with potentially jeopardized personal information do not result in actual harm to anybody. “There are many, many cases in which there is a notice with no injury,” Scott says.

## Insider Attacks

One of the most distressing types of data breach is also the most difficult to prevent: dishonest people who either work for a company and steal information internally or pose as a trustworthy business partner and convince a corporation to hand over personal records.

That’s exactly what happened to consumer data broker ChoicePoint, now a division of LexisNexis, during a 2005 security incident many experts say played a crucial role in shaping privacy law.

The company sold consumer information from more than 163,000 individuals to identity thieves who pretended to be legitimate businesspeople. The Federal Trade Commission connected more than 800 cases of identity theft to the compromised Social Security numbers, employment information and credit histories. In the resulting litigation, ChoicePoint reached a \$15 million settlement that included \$10 million in civil penalties and \$5 million for consumer redress.

The case netted such a large settlement because the afflicted consumers suffered demonstrable harm, according to Nahra.

“The wrong people were let in the front door,” he says. “It was a blatant situation. The reason [the thieves] went in was to get information that could then be used for identity theft.”

Such incidents involving employees form the largest percentage of breaches in the financial sector, Curtin says. It’s not that there are more crooks in financial jobs than in other industries—but an inside attack is the best way to navigate past the sophisticated software protecting financial data.

“If you think about the regulatory scrutiny [the financial sector] is under, it makes sense,” he says. “They have a lot of controls around their computer systems and technology because everybody’s worried about it. On the other hand, there’s only so much screening you can do to keep out someone with a motive and inclination to take advantage of a position of trust.”

In April 2008, online loan company LendingTree sent a letter to customers alerting them to such an insider breach. Several former employees shared confidential passwords with mortgage lenders so the lenders could access LendingTree customer information. LendingTree sued the employees, but that didn’t stop several customers from bringing their own class action suit against the company, alleging the incident hurt their credit scores. The litigation is still pending, but the bad press has already spread.

Because relationships between a financial institution and a customer rely on trust, the reputational fallout from a breach situation can be as devastating to a company as litigation.

“You’re giving them information that you expect them to hold confidential,” Curtin says. “If they’re routinely being broken into, at some point you’re going to have some impetus to take your business elsewhere.”

### Just a Little Peek

An emerging area of privacy concern stems from one of the most basic elements of human nature: curiosity. “Peeping” refers to incidents where people who have access to a variety of private records snoop into files they have no business seeing. Many times the perpetrators act with innocent intentions—for example, a nurse who checks on the records of a hospitalized neighbor. But in a spate of recent cases, people sought to profit from releasing personal medical information.

Celebrity tabloids paid a former UCLA Medical Center employee to supply the magazines with information about famous patients, including Britney Spears and Farrah Fawcett. The employee resigned in the midst of UCLA’s investigation but had already accessed 61 confidential records.

Similar incidents occurred during the 2008 election when State Department employees inappropriately peeked at President Obama and Sen. John McCain’s passport records.

“Even if there’s no risk of identity theft, even if no one outside the organization gets the data, there was a lot of national outrage after the passport incidents were discovered,” says Peter Swire, a law professor at The Ohio State University and senior fellow with the Center for American Progress.

There are fairly simple solutions to this simple form of a breach, he says. Implementing an audit trail that records who looks at which files is one way to monitor who’s peeping and who’s legitimately authorized to see the information. That’s exactly what UCLA did, in addition to further restricting employee access based on that worker’s role in the hospital.

“We all understand the human temptation to peep this way,” Swire says. “But as databases spread through our organizations and remote access becomes more common, companies should be thoughtful about not exposing their most important files.” n

# And Then Come the Lawsuits...

Litigation following a data security breach generally falls into two categories, says Peter Swire, a law professor at The Ohio State University and senior fellow with the Center for American Progress.

Litigation occurs between businesses when one suffers financial harm as a result of the breach incident, such as a bank seeking reimbursement from a retailer victimized by credit card fraud. Swire says it’s easy to prove financial harm between companies because there’s a record of the fraudulent transactions—and those monetary losses can total millions of dollars.

Class action lawsuits spring up almost immediately after word gets out about major data incidents, says Kirk Nahra, a partner at Wiley Rein and chair of its privacy group.

“It’s a race,” he says. “And most of them are filed before anything bad has happened.”

Often, companies reach settlements before the case ever goes to trial, even if there’s no evidence of actual harm.

But when there is proof of negligence or actual damage, the consequences for companies can be severe.

“Where companies lacked security practices and computers were put at risk of identity theft, it’s a pretty sympathetic case for the plaintiffs,” Swire says.

# Rigorous Rules

Massive data breaches like the one that hit Heartland Payment Systems in January spark costly class action lawsuits, negative media coverage and potentially devastating loss of business for the afflicted company. They also trigger the obligation to notify affected individuals under various state laws. And they often spur new legislative and regulatory action, designed to protect consumers from identity theft and exposure of personal information.

In fact, were Congress and the media not preoccupied with the economic crisis, consumer outrage over this huge theft of credit card information might finally drive action on a federal law mandating breach notification. For several years, efforts to pass such legislation have stalled due to committee turf wars and disputes between privacy advocates and business groups over key provisions. One particular area of disagreement involves pre-emption of state law, a priority for businesses frustrated by the proliferation of varying state requirements. A business coalition formed to push federal data breach legislation recently withdrew from the fray, saying it would concentrate on industry self-regulation. A Microsoft official reportedly told a privacy forum in March that the coalition concluded a bad federal law would be worse than none.

But President Obama clearly has consumer privacy protection on his agenda—even if a comprehensive federal bill must await brighter economic times. Tucked away in his massive economic stimulus bill was a stringent breach notification addition to privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which covers the health care industry and companies with self-insured employee health care programs.

And the Federal Trade Commission (FTC) has issued controversial new “Red Flag Rules” for financial institutions and a broad array of other entities. Those rules mandate a procedure for identify-

ing and mitigating data breach risk.

With momentum clearly on the side of more data breach controls, most observers think comprehensive federal legislation is only a matter of time.

“It’s not a question of if, but how much,” says Colin Zick, a partner at Foley Hoag. “How much more is going to happen? Once the economic legislation is dealt with, all it will take is one more big breach that gets constituents calling.”

## States Step In

With such a hot consumer issue in play, it’s not surprising that state legislatures stepped in when Congress failed to act. Since 2003, 45 states and Washington, D.C., have enacted laws requiring companies to provide written notification of a data breach to people whose personal information, such as Social Security and credit card numbers, has been compromised. The specifics of what must be included in the notice vary. For businesses that operate in multiple jurisdictions, this results in conflicting regulations that multiply the cost of compliance.

Now Massachusetts has raised the ante, passing the most comprehensive of all state data privacy laws. It covers any business that has information about a Massachusetts resident and is likely to set the stage for a new round of state legislation. In fact, New Jersey already proposed a law mimicking Massachusetts’ statute.

The Massachusetts law, whose implementation date was delayed from



Jan. 1, 2009, to Jan. 1, 2010, after businesses complained about the cost and complexity of compliance, goes far beyond data breach notification.

“The heart of the Massachusetts law is a requirement for a comprehensive written security program,” says Thomas Smedinghoff, a partner at Wildman Harrold. “A lot of companies have security policies, but a security program requires you go through a process.” That includes identifying information assets, assessing risks that threaten information’s security and determining and implementing the best options for mitigating the risks.

Massachusetts also requires encryption for any personal information stored on a laptop or “portable device”—PDAs, cell phones and flash drives—or transmitted “across public networks” or “wirelessly.” This presumably includes even wireless communication within a corporate network, according to Smedinghoff.

## Surprise Package

At the federal level, the health care privacy provisions tucked into the stimulus package came as a surprise. They ended up there because the bill provides \$20 billion in funding for electronic health records, which Obama sees as one way to rein in medical costs. The act includes beefed up privacy regulations to address concerns that digitized medical records will lead to more stolen personal information, according to Reece Hirsch, a partner at Morgan, Lewis & Bockius.

“This is the most significant health care privacy and security regulation since the enactment of HIPAA in 1996,” he says.

*continued on page 68*

# Lock Down

Corporate data breaches can lead to lawsuits, damaged reputations, costly breach notification procedures or the loss of competitive edge. But Verizon's 2008 Data Breach Investigations Report concluded that 87 percent of breaches were preventable through "reasonable controls."

Most frequently, external thieves cause damaging losses of customer, employee or corporate information by hacking into networks or stealing laptops or other mobile devices. Preventive techniques range from such simple steps as limiting access to a need-to-know basis to installing state of the art software that can detect potential breaches before they happen. The solutions keep evolving as the thieves become more sophisticated.

In the recent massive theft of credit card information from card processor Heartland Payment Systems, for example, the thieves used malicious software that recorded credit card information as it passed through Heartland's system.

The company has since created a new department dedicated to protecting consumer and merchant information and providing end-to-end encryption of data passing from credit card swipe points to the company's switch so malware cannot steal the data in motion. Such software programs may prevent leaks before they happen.

"Software can alert that somebody has done something they're not supposed to," says Brian Weiss, vice president of information governance at Autonomy, an e-discovery provider.

But Heartland realizes it will have to remain vigilant.

"This software [used by cyber thieves] was extremely sophisticated," says Jason Maloni, a spokesperson for Heartland. "There needs to be greater information sharing between companies so the next person doesn't become a victim."

## Encryption Protection

Unfortunately, many companies haven't gotten the message yet. A January study from Motorola showed 44 percent of retailers' wireless devices—including laptops and barcode scanners—could be compromised. The study examined more than 4,000 stores, where 32 percent of wireless access points were unencrypted and 22 percent were wrongly configured.

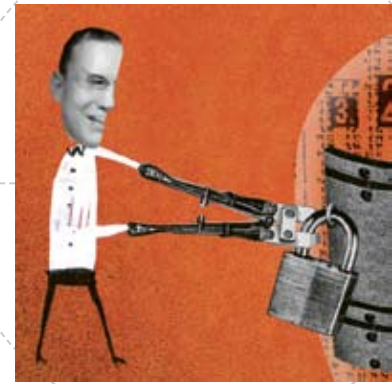
Both network and laptop encryptions are crucial to protecting sensitive data.

If wireless networks do not require passwords, hackers can see—and download—every piece of data passing across the networks with "surfer" software. This applies to both business networks and public networks like those common to coffee shops. Although large companies usually protect their networks, Roy Hadley, of counsel at Bryan Cave, says a surprising number of smaller businesses do not properly encrypt their networks. And even if a public network charges a fee to obtain a password, hackers can pay to join.

On laptop computers, many employees may not realize that encryption means more than a username and password.

"The bottom line is password protection is inadequate," says Paul Stephens, director of policy and advocacy at Privacy Rights Clearing house. "It can be easily cracked."

Some passwords simply let a user into the computer's operating system but don't protect information contained on the hard drive. If that hard drive is removed from the computer, data can easily be extracted. Hadley explains that



effective encryption software decrypts every document individually each time it is opened and then automatically locks it back down within the hard drive after it's closed again. To enable access, the user inputs a passkey (which should be random digits) when he turns on the computer. From there, each decryption and encryption happens seamlessly while the user is logged in. After logging out, everything on the hard drive is protected, even if the drive itself is removed. If someone steals an encrypted computer, "They've got a computer, but there's nothing they can do with the data," Hadley says.

Computer manufacturers have now started offering hard drives with encryption capabilities included as part of the drive itself, eliminating the need for extra software. On a more basic level, however, Hadley says workers need to learn that when traveling with a laptop, "everywhere they go, that laptop needs to go with them."

IT can also help protect data from hackers by staying in control of software used across a company's network. All software must be kept up to date to minimize opportunities for hackers. IT should be responsible for this task, as opposed to letting employees do it themselves, because for every employee who knows how to update his own software, there are probably several more workers who don't know how to do it. Hadley also recommends preventing employees from downloading any software at work—even seemingly harmless programs such as animation players.

*continued on page 68*

## Rigorous Rules continued from page 64

“It takes what has been learned from the state laws and goes a few steps further.” For example, it sets forth stringent breach notification procedures, requiring notice within 60 days of a breach being discovered. Most state laws don’t have a timeframe.

The changes, which take effect in February 2010, also expand HIPAA’s privacy rules to “business associates” of HIPAA-covered entities, including employee benefit plan administrators and other businesses involved in the transmission, processing and storage of personal health information.

Reacting to criticism that federal agencies charged with enforcing HIPAA aren’t sufficiently aggressive, the new law allows state attorneys general to bring civil actions in federal court on behalf of residents whose health care privacy has been violated.

“Obama is ratcheting it up,” says Joseph Lazzarotti, a partner at Jackson

Lewis. “The federal government is getting more serious about HIPAA, and the AGs in the states will help with enforcement.”

While the FTC adopted its Red Flag Rules before Obama took office, they will provide another data security enforcement lever for the new administration. The rules mandate a process for identifying possible data breach risks and adopting “reasonable and appropriate procedures” for dealing with them. But it’s not clear yet how widespread the impact will be.

“The Red Flag Rules apply to creditors and financial institutions,” says Hirsch. “It’s clear that financial institutions are banks and credit card companies. The definition of creditor creates a lot of controversy.”

The FTC has taken the position that a creditor is any organization that regularly accepts payment after it delivers goods or services to customers, “even in the normal course of a traditional billing process.” That would include health care provid-

ers, car dealers and telecom companies, among others. The health care industry—which some believe is sufficiently regulated under HIPAA—argued that doctors are not “creditors.” In response to such protests, the FTC delayed implementation for entities other than financial institutions from Nov. 1, 2008, to May 1, 2009. But in a February letter to the American Medical Association, the FTC reaffirmed that “creditors” include physicians, lawyers, repair people and even “a local store where a customer runs up a tab.”

While the rules impose significant burdens, particularly on small businesses, they may prove beneficial in the end.

In fact, privacy experts say many data security laws make good business sense.

“Think of it as customer relations,” Zick says. “You want to protect your data because it’s the right thing to do, and it’s good for business. That makes it easier to implement the changes.” n

## Lock Down continued from page 66

“Animation software may not be harmful in and of itself,” he says. “But it may have a certain mechanism for viewing animations a hacker may exploit that allows that hacker into that software and then correspondingly onto that computer and then into the network.”

### Employee Restrictions

But guarding against external hackers is only one part of the equation. According to a recent study from Symantec Corp. and the Ponemon Institute, of nearly 1,000 respondents who left jobs in 2008, 59 percent admitted to stealing confidential company information. And, the median insider breach compromises more than 10 times as many records as an external one, according to the Verizon study.

“Hackers ... are just getting in and getting whatever they can,” says Hadley. “With internal breaches, a lot of times

they know what they’re looking for, and they know what they have because they work with that data every day.”

So experts say limiting employee access to data is a crucial part of preventing data leaks. It starts with a basic premise: Not all employees should have access to all data. Personal data should never be stored on widely accessible servers. And just because an employee can see a document doesn’t mean he or she should be able to print it or save it to a personal folder—using read-only documents can be a helpful security tactic.

“You really need to limit the data to a need-to-know basis,” says Hadley, a former general counsel. “If you don’t have a need to know the customer list, you shouldn’t have access to it.”

One tool for controlling access is redaction technology that hides sections of documents containing sensitive

information. Informative Graphics Corp. (IGC) makes role-based redaction software that lets different groups throughout a company see predetermined sections of different data. Christine Musil, IGC’s director of marketing, says by using that type of redaction software an accounting employee would be able to view all of a customer’s data—including credit card information—but a customer sales representative would not.

Experts say avoiding data breaches also involves helping a workforce understand the big-picture importance of protecting data.

“You can have all the technical aspects put in place,” Hadley says. “But if an employee is not thinking data security, then you’ve got a problem.” n

Read about data security in higher education at **InsideCounsel.com**.



FIND MORE ONLINE