Don't be a data loss victim

Disclosure laws provide a goldmine of information on the causes of data breaches and ways to avoid a costly incident
By Linda Musthaler, Network World, 02/09/2009

Somebody was siphoning customer financial data from a chain of gas station/convenience stores.

Watch a slideshow of the 10 worst moments in network security history.
Read a story about seven ways to stop data breaches.

The perpetrator covered his tracks so well that the company which owned the stores didn't even know it had a data breach until customers began complaining about experiencing fraud just days after using a credit card or writing a check at one of the stores.

Verizon's Business Investigative Response team was called in to try to unravel the mystery and track down the hacker. The team, led by managing principal Bryan Sartin, took forensic images of the systems at several store locations and did an in-depth analysis of the information.

Related Content

Subtle clues in the data pointed toward the point-of-sale vendor that processed payments. In fact, the thief turned out to be an employee of the POS vendor. The hacker had cleverly devised a way to capture a customer's personal financial data at the time of a sale, remove the data from the server, cover his tracks, and then sell the information to other criminals.

He didn't cover his tracks well enough, and ultimately was apprehended and convicted for his crimes.
This sophisticated hack required a high level of technical expertise. But in many cases, the contributing causes of data breaches are so simple that you wonder how the incident could even happen.

For example, in early December 2008, paperwork containing personal and financial information of customers of a mortgage company was found in an office recycling bin in Florida. There were more than 200 file folders containing data that could lead to identity theft. Rather than shred the documents, someone opted to toss them in the bin, showing a complete and stunning lack of common sense.

And the state of New Hampshire's Department of Health and Human Services accidentally exposed the personal health information (PHI) of more than 9,000 people in December when someone mistakenly attached a file containing the data to an e-mail sent to 61 healthcare providers and other organizations.

The attachment contained names, addresses, Medicare Part D plan information, Social Security numbers and the amount of each person's monthly premiums — all data supposedly protected under the Healthcare Insurance Portability and Accountability Act regulations.

**Breach blog bonanza**

Until about six years ago, we rarely heard anything about harmful data breaches. And that wasn't because there weren't any. It was simply that organizations that were hit with embarrassing data losses kept them secret, or tried to.

That all changed in 2003, when California enacted a disclosure law that requires entities that suffered a data breach to notify individuals whose information may have been exposed or compromised. Since then, 42 more states have adopted similar legislation.

The fear of public humiliation clearly has not resulted in a decrease in data breaches. Quite the opposite. More than 162 million records were reported lost or stolen in 2007 — a 330% increase over the reported 49 million records of 2006.

But these disclosures have provided a treasure trove of information, which a number of groups have used to analyze data breaches and their causes. These data breach sleuths include the Verizon Business RISK Team; the Open Security Foundation, which posts a database of breaches, DataLossDB; and FRSecure CEO Evan Francen, whose blog (The Breach Blog) highlighted the Florida and New Hampshire cases cited above.

**Related Content**

**Can you hack me now?**

The Verizon Business RISK Team conducted more than 500 forensic investigations of security lapses and data breaches over the past few years, many involving suspected criminal behavior. The "lessons learned" in the [Verizon report](http://www.networkworld.com/news/2009/020909-data-loss.html) can help you determine where to focus your mitigation resources. Here are some of the key findings:

- Nearly three-quarters of the breaches investigated by Verizon were instigated by external sources.
- Just 18% of the breaches were caused by insiders; however, the insider incidences were much larger in terms of the amount of data compromised.
- Over the years, the investigators observed a sharp increase in breaches originating through the assets of trusted business partners who are part of the extended enterprise. This doesn't necessarily imply that the partners are
stealing data; rather, their entry points into the victim's computer may be compromised, allowing hackers to usurp trusted connections and accounts. This tells us that stronger defense needs to be built around the data, not just around the network perimeter.

- Data breaches often result from a combination of events rather than a single action. In a majority of the cases that Verizon analyzed, some sort of significant error contributed to the breach; for example, not applying a patch to a known vulnerability, or misconfiguring software or a device, thus allowing exploitation of the error.
- In many cases, the forensics experts determined that a hacker exploited a known vulnerability for which there was a patch available – but never deployed – for up to a year prior to the breach. To build a better shield, organizations need a formal program for patch management, configuration management and change management.
- The Verizon investigators observed some commonalities of the breaches. For instance, 66% of the time, the breach involved data that the organization didn't even know was on the system.
- Three-quarters of the attacks weren't discovered by the victimized company; often, it was law enforcement agencies or individual victims who pointed out the problem.
- And in most cases, the attacks were not particularly sophisticated and would likely have been prevented if basic security controls had been in place at the time of the attack. These last two observations are significant, because they tell us that a comprehensive and well executed security plan should prevent most breaches.

Verizon's Sartin says the nature of the criminal attacks is changing – and not for the better. "Cybercriminals have become much more sophisticated in the last decade," he says. "At first we saw directed attacks against specific companies that processed lots of sensitive data — banks, [automated teller machine] operators, data processing companies. Then we observed a shift toward fully random attacks using botnets, SQL injections, authentication bypass and scans for vulnerabilities. Just recently, the criminals have shifted techniques again to pursue softer targets like data in transit or in the computer's running memory because it's not encrypted."

"People think data security is an IT issue, but it's really a business issue," Francen adds. "People want to fit this thing called 'data security' into a box and be done with it. Instead, companies need to take a holistic and continuous approach to protecting data, starting at the top. It needs to be tied to a CEO's responsibilities. It's really about the preservation of business assets."

In his work as a security consultant, Francen often encounters people who equate "compliance" with "information security." "Companies spend lots of money on compliance issues and make the assumption that if they comply with regulations [like SOX, HIPAA and PCI DSS], their data is secure," Francen says. "Those regulations are a good start, but they don't mean data is secure. Your computer systems can be 100% compliant but you can still have a data breach."

Francen points to the 2008 breach of the Hannaford Bros. grocery chain. The company had passed a recent PCI DSS audit but still experienced the theft of consumer credit and debit card numbers.

Preventing breaches can seem like a daunting task. The Verizon Business RISK Team reminds us to "achieve 'essential' and then worry about 'excellent'." A key recommendation from these experts is to identify a set of essential controls and ensure their implementation across the organization without exception and then move on to more advanced controls where needed. Such a strategy will address the accidental breaches such as lost laptops as well as the intentional attacks from hackers and cybercriminals.

Musthaler is a principal analyst at Essential Solutions Corporation. She can be reached at lmusthaler@essential-iws.com/