

With the Loss of One Laptop

Some lessons from a general counsel who learned the hard way. **BY ADAM PALMER AND TIM S. MCCLAIN**

If you are an in-house counsel, you probably don't question whether you will experience a serious data loss at your company, but rather when the loss will occur. It's pretty clear that the loss of trade secrets, personal employee data, or confidential customer information can cause serious harm to a company's reputation. It could even lead to civil litigation if the data loss breaches nondisclosure obligations.

Recent case law has proven just how much of a legal duty companies have to properly safeguard data. And states have started to pass laws requiring companies to warn those who may be affected by data security breaches.

Despite increasing security efforts, the Internet today remains the Wild West of data security, where employees and their friends often freely discuss information that may be highly confidential. An even more elusive threat may be people outside the companies who overhear or inadvertently learn confidential information. In the wrong hands, this information can circulate the globe on the Internet in a matter of hours. For corporate counsel, the importance of understanding the benefits of a sound data security program has never been greater.

IN-HOUSE COUNSEL

THE FIREWALL APPROACH

A 2006 study of security breaches prepared for Congress by the Congressional Research Service found that 20 percent of all security breaches at U.S. medical centers were the result of "employee malfeasance." Many companies falsely feel secure because they have an expensive computer firewall or perhaps a "blogging and e-mail" policy. The reality is that such defenses, while commendable, are really just scratching the surface of proper data protection. These defenses only address superficial and unsophisticated threats. They will be nearly useless against a malicious employee or outside person spreading false or confidential information about your company across the Internet from a deliberately obscured Web site. Even the best firewall is not going to stop the human



resources manager who keeps staff data backed up on an external flash drive connected to her key chain.

An effective anti-blogging policy will have no effect on the neighbor of a department manager who overhears a confidential phone call and writes about it on his blog. The examples are endless, but they illustrate the critical need for a comprehensive approach to data security. A strong approach recognizes the scope of the company's Internet "footprint," the various physical forms of data storage, and the need for a quick reaction program to respond to breaches once they are recognized.

How many companies open a new facility and spend thousands of dollars on expensive physical security measures but budget only a fraction of that amount for data security? Recent headlines provide ample evidence of the danger posed by employee negligence and theft of confidential data. This summer, Fidelity National Information Services announced that a senior-level database administrator had stolen the records of millions of customers and sold them to marketing companies.

Consider, for a moment, your company's response if a similar incident were to occur. Perhaps a sales manager is stealing client information. Maybe even a senior executive is disclosing insider information that might affect the sale of securities. Maybe you consider these to be rare examples of betrayal by criminal employees.

However, one need only recall the media storm last year over the loss of information at the Department of Veterans Affairs to understand that simple employee negligence can be as great a threat as theft. The story of the VA provides a great example of a good organization that fell victim to a series of unexpected events resulting in a very serious loss. The story of the VA and the lessons learned from that crisis are invaluable for any in-house counsel. During the data loss crisis at the VA, the co-author of this article, Tim McClain, served as general counsel of the VA.

WHAT HAPPENED AT THE VA

Consider how you would handle one of your worst nightmares. You receive a call early in the morning and are told that the personal information of 26.5 million of your customers has been lost and potentially compromised. What do you do? Whom do you call, and how do you discover the cause?

While the details described here are all a matter of public record, appearing in many investigative reports and transcripts of congressional hearings, a few facts may not be well-known. It's important to remember that the stolen laptop was a personal laptop, not a VA or government computer; all of the lost data were on an external hard drive, which was personally owned; and the only items stolen from the owner's home were the laptop, the external hard drive, and some pocket change.

The employee involved in the VA laptop loss had 34 years of exemplary federal service and was a Harvard-trained Ph.D. statistician. His job involved statistical analysis and working with very large databases, and he had access to huge amounts of personal information. He used that access to perform sophisticated analysis of trends and provide forecasts to assist in planning. Over the course of several months he downloaded portions of the data onto CDs and DVDs, carried them home, and loaded them on his personal hard drive for a special project that he was working on with the hope that it would ultimately benefit the VA.

The employee's residence was burglarized on May 3, 2006. The laptop and hard drive were not password-protected. The employee immediately reported the loss to his supervisor and the VA security office that same evening. He also reported the fact that the hard drive contained a lot of personal information. The secretary of Veterans Affairs was not notified of the loss until May 16—13 days later. The public was not notified of the loss until May 22. Why?

The main reasons for the delay were the lack of a written policy for response to a data loss or breach and a lack of urgency on the part of supervisory personnel in determining the scope of the loss. Although the employee's supervisor interviewed him the morning following the burglary, the supervisor did not ascertain the scope of the loss and did not notify his own superiors of the loss.

The extent of the loss was not fully realized until investigators from the VA Inspector General's Office interviewed the employee. They immediately notified the VA

chief of staff of the potential magnitude of the loss. The chief of staff formed an ad hoc crisis response team to handle the situation and notified the secretary of Veterans Affairs of the loss.

Significant problems with the case were immediately identified. First, the employee had no firm idea exactly what information was on the hard drive, how many people it might affect, and whether the data contained medical information protected by the Health Insurance Portability and Accountability Act. Second, the department did not have current addresses on the millions of veterans, dependents, and active-duty military personnel whose personal information was on the hard drive. There was no established crisis response plan or crisis communications plan.

The hard drive was recovered through some excellent police work, and it was later determined that no one had accessed the data. Investigators determined that none of the information had been used for criminal purposes, especially identity theft. So how did the laptop incident affect a federal agency as large as the VA when there was no hacking, no inside criminal activity, and no identity theft? It consumed senior management and paralyzed the department for many weeks.

LEARN THESE LESSONS

The lessons to be learned from the VA incident and various other government agency incidents were listed in a Government Accountability Office report, released this April, called "Privacy—Lessons Learned About Data Breach Notification." The lessons apply equally to every company and include the following points:

- Rapid internal notification of key senior company or government officials is critical.
- A core group of senior officials should be designated to make decisions regarding the appropriate response.
- Mechanisms must be in place to obtain contact information for affected individuals. (If your company or federal agency maintains a database with personal information, for instance, ask your privacy and information professionals if they have current addresses for everyone in that database.)
- Determining when to offer credit monitoring or other services to affected individuals requires risk-based management decisions.
- Interaction with the public requires careful coordination and can be resource-intensive.
- Internal training and awareness are critical to a timely response, including notification.
- Contractors to your company or agency should have their obligations if they experience a data breach clearly defined.

The need for increased vigilance with data protection is increasing. Adding to the importance of action is the pending adoption of Internet Protocol Version 6. Internet protocol is the system of addresses that computers use to identify each other and communicate. It is this system that supports the entire Internet. For almost 20 years, this system has been the same and is referred to as Internet Protocol Version 4.

But technology experts have long been calling for an update to IPv4 with a system that can better handle the massive amounts of Web traffic and also fully support other needs, such as Wi-Fi and next-generation wireless services like Wi-Max. Put more simply, IPv4 is a system built on “telephone numbers” 32 characters long. As the Web grows and starts to run out of numbers, it eventually needs a new system. IPv6 uses 128-character numbers and provides a vast upgrade in capacity. While there are many other significant features of IPv6, at its core it represents an expansion of the number of potential Internet addresses.

Federal regulations now require that all government agencies be IPv6-compliant by mid-2008. For government contractors and others working with the government, IPv6 compatibility is critical. The capacity advantage for IPv6 is significant, but the new system also creates an increased need for security measures. As more data are transmitted or stored on the Internet, the need for data security awareness only increases.

Added to this concern is the increasing movement towards Web-based versions of familiar spreadsheet, document production, and presentation programs. Although business

benefits by having access to information from virtually any computer, with such flexibility comes new concerns about the transmission and security of data.

The Internet is a vast data field and, best practices for data security require much more than just a good firewall, a blogging policy, or the occasional check of an employee’s MySpace page. Threats exist in both the physical and digital security of data. The VA case study is also a good example of how unforeseen events can cause serious damage to even the best organizations. True data security probably requires using outside counsel and other professional resources. Although that may seem costly, the cost of lost customer trust and corporate reputation are far greater if data security measures are ignored or inadequate.

Adam Palmer is the general counsel and chief cyber security counsel for Cyveillance Inc. in Washington, D.C. Tim S. McClain practices privacy, information security, and federal procurement law in the Washington, D.C., office of Womble Carlyle Sandridge & Rice. He was general counsel of the U.S. Department of Veterans Affairs from 2001 to 2006.