REAL WORLD CASE 2

Harrah's Entertainment and Others: Protecting the Data Jewels

In the casino industry, one of the most valuable assets is the dossier that casinos keep on their affluent customers, the high rollers. But in 2003, casino operator Harrah's Entertainment Inc. filed a lawsuit in Placer County, California, Superior Court charging that a former employee had copied the records of up to 450 wealthy customers before leaving the company to work at competitor Thunder Valley Casino in Lincoln, California.

The complaint said the employee was seen printing the list—which included names, contact information, and credit and account histories—from a Harrah's database. It also alleged that he tried to lure those players to Thunder Valley. The employee denies the charge of stealing Harrah's trade secrets, and the case is still pending, but many similar cases have been filed in the past 20 years, legal experts say.

While savvy companies are using business intelligence and CRM systems to identify their most profitable customers, there's a genuine danger of that information falling into the wrong hands. Broader access to those applications and the trend toward employees switching jobs more frequently have made protecting customer lists an even greater priority.

Fortunately, there are managerial, legal, and technological steps that can be taken to help prevent, or at least discourage, departing employees from walking out the door with this vital information.

Organizations should make sure that certain employees, particularly those with frequent access to customer information, sign nondisclosure, noncompete, and nonsolicitation agreements that specifically mention customer lists, says Suzanne Labrit, a partner at the law firm of Shutts & Bowen LLP in West Palm Beach, Florida.

Although most states have enacted trade-secrets laws, Labrit says they have different attitudes about enforcing these laws with regard to customer lists. "If you don't treat it as confidential information internally," she says, "the court will not treat it as confidential information either."

From a management and process standpoint, organizations should try to limit access to customer lists only to employees, such as sales representatives, who need the information to do their jobs. "If you make it broadly available to employees, then it's not considered confidential," says Labrit.

Physical security should also be considered, Labrit says. Visitors such as vendors shouldn't be permitted to roam freely in the hallways or into conference rooms. And security policies, such as a requirement that all computer systems have strong password protection, should be strictly enforced.

Some organizations rely on technology to help prevent the loss of customer lists and other critical data. Inflow Inc., a Denver-based provider of managed Web hosting services, uses a product from Opsware Inc. in Sunnyvale, California, that lets managers control access to specific systems, such as databases, from a central location.

The company also uses an e-mail scanning service that allows it to analyze messages that it suspects might contain proprietary files, says Lenny Monsour, general manager of application hosting and management. Inflow combines the use of this technology with practices such as monitoring employees who have access to data considered vital to the company.

A major financial services provider is using a firewall from San Francisco-based Vontu Inc. that monitors outbound e-mail, Webmail, Web posts, and instant messages to ensure that no confidential data leaves the company. The software includes search algorithms and can be customized to automatically detect specific types of data such as lists on a spreadsheet or even something as granular as a customer's Social Security number. The firm began using the product after it went through layoffs in 2000 and 2001.

"Losing customer information was a primary concern of ours," says the firm's chief information security officer, who asked not to be identified. "We were concerned about people leaving and sending e-mail to their home accounts." In fact, he says, before using the firewall, the company had trouble with departing employees taking intellectual property and using it in their new jobs at rival firms, which sometimes led to lawsuits.

Vijay Sonty, chief technology officer at advertising firm Foote Cone & Belding Worldwide in New York, says losing customer information to competitors is a growing concern, particularly in industries where companies go after many of the same clients.

He says the firm, which mandates that some employees sign noncompete agreements, is looking into policies and guidelines regarding the proper use of customer information, as well as audit trails to see who's accessing customer lists. "I think it makes good business sense to take precautions and steps to prevent this from happening," Sonty says. "We could lose a lot of money if key people leave."

Case Study Questions

1. Why have developments in IT helped to increase the value of the data resources of many companies?
2. How have these capabilities increased the security challenges associated with protecting a company's data resources?
3. How can companies use IT to meet the challenges of data resource security?

Source: Adapted from Bob Violino, "Protecting the Data Jewels: Valuable Customer Lists," *Computerworld*, July 19, 2004. Copyright © 2004 by Computerworld, Inc., Framingham, MA 01701. All rights reserved.