

Forbes

MAY 10 2004

ALSO ►

IS YOUR BEST
EMPLOYEE A
CYBERTHIEF?

The Insider

When a top employee is suspected of stealing data, things can get messy.

BY CHANA R. SCHOENBERGER

THE RING OF THE PHONE AT her Laguna Beach house, near Los Angeles, woke Denise DeMan-Williams at 7:30 on the Saturday of the July 4th long weekend in 2003. It was her lawyer, telling her that five policemen from East Whiteland Township, Pa. had just raided the home of one of her employees, Dr. John Goldener. The cops searched for four hours and left with armfuls of documents, electronic equipment and CDs.

DeMan-Williams, who runs a personnel recruiting firm, Bench International Search, out of Beverly Hills, was shocked and angered at the news of the police raid, but assumed it was nothing more than a thuggish tactic from a courthouse opponent. Goldener was being sued by his former employer, James Young, owner of Young International Group in Malvern, Pa. Young accused him of steal-

mate their firms have each lost \$3 million in stolen data, lost business and legal and computer-forensics fees.

Goldener denies the allegations in both suits and is suing right back for defamation. "I have nothing of DeeDee's or Jim's," says Goldener, who now runs a personnel search business from his home.

This tangle of litigation, with accusations of sexual harassment, lies and betrayal, underscores the ethical dilemmas facing any company with a PC and an Internet connection. How much access should employees have to computer systems, and how stringently should employers police them?

IT managers have spent billions of dollars on software firewalls and anti-virus and intrusion-detection systems, all aimed at warding off the classic hacker, the vandal who invades over a phone line. Have they paid too little attention to the dangers from within? Insider network

very clear what the expectation of privacy is, which in most cases is none," says Thomas Fedorek, senior managing director at Citigate Global Intelligence & Security in New York City.

The recruiters' tale of woe began in 1999 in a doctor's office in Philadelphia's posh Main Line suburbs. When Colleen Young went to see Dr. Goldener, the family pediatrician of many years, they chatted about Colleen's husband, James Young, a pharmaceutical and health care executive recruiter. The doctor bemoaned falling insurance reimbursements and was eager to make a career change. In April 2000 Young hired Goldener to help bring in new clients and find executives to fill job slots.

Goldener, a ruddy, likable gladder, made a sharp recruiter, both execs say. Young recalls Goldener's practice of visiting nearly every one of his coworkers in their offices on a daily basis.

The Insider

When a top employee is suspected of stealing data, things can get messy.

BY CHANA R. SCHOENBERGER

ing trade secrets by downloading client contact lists from the company's computer network. Goldener had long maintained that he had taken nothing with him when he left. DeMan-Williams believed him.

A few weeks later her anger turned toward Goldener. She found out, she says, that he had the entire Young database, right down to the company's Christmas card list. Within a few months, according to her own suit against him, she would discover that Goldener had also copied chunks of the Bench database and attempted to delete the files to cover his tracks. "It's a case of cybertheft," says DeMan-Williams. "Everybody here feels raped." She and rival James Young esti-

mate abuse ranks second only to viruses, according to the annual Computer Security Institute-FBI survey. Employees often keep duplicate versions of sensitive data on their PDAs, BlackBerrys and home computers. Of the companies in the FBI study that reported insider abuse—and 80% did—one-third didn't even know how many times their systems had been compromised. Integrity, not ability or the fear of getting caught, is all that separates a conscientious employee from a thief.

Employers, in turn, have raised their spending on snoopware, including keystroke-monitoring software and employee access logs, from \$6 billion in 2002 to \$9 billion this year, according to IDC. "We recommend that companies make it

But early on, Young had questions about the doctor's loyalty. In 2001 he was ready to promote Goldener, but Goldener refused to extend his noncompete agreement from one year after leaving to two years. Young held Goldener at his current level. Goldener says he declined the promotion because it came with a less favorable commission scale.

Around that time Young started to fret about the security of his database. Built up over 23 years at an estimated cost of \$1.5 million, Young's database contained tens of thousands of contacts and companies. Records included résumés, salaries and often sensitive family histories, such as child-custody issues. The database had a keystroke logger to record

who visited and what exactly they saw, but Young wanted a higher level of security. In the summer of 2001 he installed software to capture every key touched, in or out of the database, in a tamper-proof encrypted log on a separate server, accessible only to Young.

In October Young was reading through the logs and noticed that Goldener had accessed and printed 25 client reports over a two-month period. There was no reason for him to care about those clients, based on his assignments, says Young. "I confronted him, and he denied it," Young says. Goldener said that he regularly printed out reports to work from home. Relations soured between the two men. In May 2002 Young fired Goldener.

By then, the doctor was already planning an exit. Goldener had approached a Bench staffer at a neurology conference in March 2002, looking for a new job. In his interview with DeMan-Williams and a deposition as a defendant in the Young lawsuit, he said he was desperate to escape a sleazy office environment made toxic with sexual chatter, bullying and oft-repeated stories about all-night debauchery. (Young says that characterization is false; DeMan-Williams says she naively never checked out Goldener's story.)

Bench hired Goldener that June and gave him full access to its 25,000-candidate database. The 20-employee company was on track to do \$6.4 million in revenue for 2002, the same as the previous year. Goldener, though he was commuting every week or so from Philadelphia, seemed to fit right in. DeMan-Williams even bought a Culver City, Calif. condo for him to use.

In April 2003 DeMan-Williams was unexpectedly hit with a lawsuit from Young, accusing Bench and Goldener of breaching the doctor's non-compete, citing, among other accusations, Goldener's use of Young's data to benefit a rival.

After filing his lawsuit, Young had his IT staffers comb through the computer logs, looking for unauthorized network access incidents they had

missed before. They found, Young says, that on the weekend of Feb. 23, 2002 Goldener had come into the deserted office, downloaded the entire database into Excel spreadsheets and copied the files onto CDs. Goldener maintains all of his downloads were for Young recruiting work. The evidence nonetheless persuaded the district attorney to get the search warrant.

Confronted, Goldener told DeMan-Williams that the CDs contained data he had used to work from home while he was on Young's payroll but hadn't used while in Bench's employ. He also says now that the database was useless to him anyway because Young had laced it with

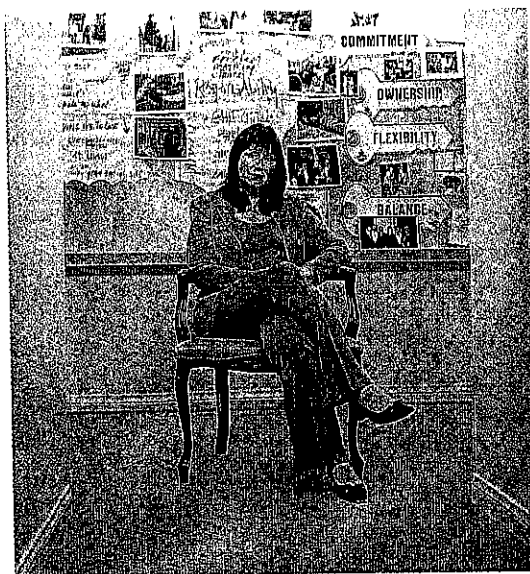
names of friends or relatives who would tip him off to any illicit users.

In July 2003 Goldener resigned from Bench, citing the arduous commute and discrepancies between what he made in commissions and what he was owed. Now scared for her own data, DeMan-Williams called in forensics experts to dig into Goldener's laptop hard drive. The techs found a trail of e-mails between Goldener and David Krause, a computer consultant and personal friend. Goldener had told Krause that he was planning to quit Bench in June and start his own firm. He also noted that he had been downloading and copying contacts and e-mails from his office Outlook account and asked Krause's advice about buying his own computer to store his data. DeMan-Williams spent three weeks that August in Australia on vacation with her family, sobbing as she read copies of Goldener's e-mails detailing what she says was his theft of her database.

The doctor, according to Bench's suit against him, had also tried to hide improperly deleted files in unallocated space on the hard drive. That was an attempt, says DeMan-Williams, to cover his tracks. Analysis of her network's backup tapes this spring also revealed, she says, that Gold-

ener's PDA contained 10,000 pages of data from both Bench and Young, an accusation Goldener denies. Now DeMan-Williams is testing monitoring software and has warned her employees that they are being watched.

Young's company dropped its suit against Bench; Goldener is now defending himself from both Bench and Young. The prosecutor in East Whiteland Township has yet to file any criminal charges. Judges in both civil cases declined to grant preliminary injunctions that would keep Goldener out of the recruiting business before the trials. The doctor says it's all a big witch hunt. His new firm took in just \$45,000 in revenue last year but spent \$100,000 on expenses, including \$60,000 to defend against the two suits. **F**



Headhunters Denise DeMan-Williams and James Young say they're victims of data theft.

