

Data Theft Common By Departing Employees

By Brian Krebs, Washingtonpost.com Staff Writer

Thursday, February 26, 2009; 12:15 PM

Many people who are either laid-off from their job or simply moving to another opportunity often secretly take proprietary data from their employer on their way out the door, a study released this week found.

Nearly 60 percent of employees who quit a job or are asked to leave are stealing company data, according to report by the Ponemon Institute, a Tucson based research group. The survey was based on interviews with 945 adults who were laid off, fired or changed jobs in the last year.

Seventy-nine percent of those who admitted to taking data said they did so despite knowing that their former employer did not permit them to take internal company information.

Sixty-five percent of those who took data from their former employer grabbed e-mail lists. The next most frequently stolen data included non-financial business information (45 percent), customer contact lists (39 percent), employee records (35 percent) and financial information (16 percent).

The institute's founder, Larry Ponemon, said several factors may contribute to such cavalier attitudes toward data theft, including a lack of employee loyalty and telecommuting.

"What's interesting is more and more people seem to feel entitled to information they create on the job, and an increase in mobility in the workforce means many employees don't have a lasting relationship with their employers," Ponemon said. "Also, as you have more employees working from remote locations and on home computers, the concept of who really controls this data isn't often clear to people."

Roughly 67 percent of those who acknowledged taking company data from their old employer said they did so in order to leverage a new job. But Gavin Manes, chief executive of Avansic, a digital forensics company that often is hired to investigate employee data theft, said individuals who hand confidential data over to a new employer or competitor are putting themselves -- as well as their former and prospective employers -- at grave legal risk.

"Some people who do this think they're helping their next employer, but in reality they are probably punishing them, because there is constant litigation on this," Manes said. "The new employer may get secret information, but that company the person just left might very well sue the new employer."

In an era when more employees are storing their business and customer contacts online at services like LinkedIn.com, some employees may not believe they are doing anything wrong when they take customer lists and other internal company data when they move on to a new job.

But Jon Groetzinger, a law professor at Case Western Reserve University Law School in Cleveland, said most companies explicitly bar employees from taking internal or proprietary data in contracts that employees sign as a condition of their hiring. What's more, employees who take such data when they leave a job may also violate state and federal laws, which can result in fines of as much as \$5 million for a new employer caught using or profiting from it.

"Usually, customer lists are specifically called out as being company proprietary, as are strategic plans and financial statements that haven't been made public," Groetzinger said.

In cases where non-disclosure agreements (NDAs) prohibit departing employees from revealing trade secrets, those employers often will follow up with the former employee's new boss.

"In those cases, it's not uncommon to for a new employer to get a letter saying 'You should know that this employee is under an NDA not to discuss certain information, and we intend to enforce that,'" Groetzinger said.

Of those surveyed, approximately 37 percent were asked to leave, 38 percent found a new job and 21 percent moved on because they are anticipating a layoff. Immediately after leaving their former company, 61 percent took paper documents or hard files, 53 percent downloaded information onto a CD or DVD and 42 percent downloaded information onto a USB memory stick, the Ponemon study found.

An alarming finding from the survey showed that 24 percent of responders said they still had access to their employer's computer network after they left or were let go.

Kevin Rowney, founder of data loss prevention division at Symantec, which commissioned the Ponemon study, said many companies do not have the technology in place to be able to see when well-meaning employees inadvertently send out e-mails containing proprietary data, let alone the systems to detect an employee who may be doing so intentionally.

"Far too many companies seem to be very sloppy with network access governance," Rowney said.

Still, if a company is motivated enough, they usually can find out if former employees steal privileged data when they leave, Manes said.

"I get a lot of people who work at big companies sending me resumes through Hotmail and Gmail, thinking that this is going to cover their tracks at work," Manes said. "But the reality is that if the employer decides to find out if an employee stole data, they quite often can and will."