



## INSIDER DATA THIEVES ARE THE WORST

**When good employees go bad and steal other employees' data, they usually try to buy cell phones.**

August 1, 2008  
By Richard Adhikari

While crime fighters are buzzing about malware (define), SQL injections (define), phishing(define) and other similarly fascinating acts by cybercriminals, the really bad guys are within the corporate firewalls.

A study conducted in late 2007 by ID Analytics, which offers identity intelligence on demand, found that from three to 36 percent of identities stolen by internal data thieves were misused. "Compared to that, only 0.01 to 0.5 percent of identities stolen in external data breaches was misused," Cooper Bachman, an ID Analytics product analyst, told InternetNews.com.

This is because an external breach is more obvious to a company than one employee quietly stealing information on the inside. When identities are stolen from the outside, the identity is then sold on underground sites that trade in identities, credit cards and such, and that takes time, perhaps enough time for the information to be protected from misuse. Internal thieves tend to use the information themselves and act very quickly after making their heist.

The study examined more than a dozen incidents of internal data theft involving more than five million identities from consumer and employee files across organizations in the government, education and commercial sectors.

Eight of these incidents led to more than 1,300 cases of attempted fraud. The criminals targeted bankcards, retail cards and wireless providers. Most of them applied for cell phones under other people's names.

Most of the misuse took place between two and 20 miles from the location where the data was stolen, indicating that the thieves didn't try to sell the data to others.

Insider thieves have changed their pattern of fraud recently. "In the past, fraudsters preferred to target bank cards; now we've found a larger proportion of fraudsters targeting the wireless industry than expected," Cooper said.

Bachman said data thieves apply for cell phone accounts using stolen identities, then sell the phones, either on eBay or on the street. "They're not interested in setting up a false account under your name, they want the hardware so they can make a quick buck," he explained.

The trend will worsen as more consumers adopt smart phones, because these are more valuable than traditional cell phones, Bachman said.

Enterprises are combating the problem with hardware and software solutions to control access to hosts and applications, Bachman said. Also, IT security often bans mobile devices like USB thumb drives, which "are one of the main tools to pull out data because they're quick, and they're easy to conceal and use," Bachman added.

If that's the case, why is internal data theft on the rise? "There's always the fact that there's a human being is at the center of data security, and that's going to be a challenge because it's not something you can replace with automation or software or hardware," Bachman said.

The City of San Francisco found this out the hard way when Terry Childs, a computer network administrator for the city's Department of Technology, was arrested earlier this month.

Childs, who was supposed to safeguard the city's computer systems against attack, instead created a password that gave him exclusive access to its new FiberWAN (Wide Area Network) network, shutting out other authorized administrators.

He also set up devices to gain unauthorized access to the system, which stores records such as officials' e-mails, city payroll files, confidential law enforcement documents, and jail inmates' bookings.

Childs was arraigned on four counts of computer tampering. After his arrest, he gave the police a fake password to the system, and refused to give up the proper one until San Francisco mayor Gavin Newsom personally visited him in jail.

Childs' actions could have been prevented if the city had implemented separation of duties, better known as SoD. This basically divides business-critical duties into four types of functions -- authorization, custody, record keeping and reconciliation -- and requires that one person handle only one type of function.

SoD ensures that people do not have improper or uncontrolled access to any system in the enterprise. Role and access management control are two of the ways SoD can be enforced.