



ANALYSIS OF INTERNAL DATA THEFT

by Steve Ragan - Aug 1 2008, 21:16

A new study looks at how [data](#) stolen internally at a business is used. (IMG:J.Anderson)

ID Analytics recently released the results of their internal data theft study, which looks at the criminal behavior patterns associated with the misuse of identities stolen from the workplace by employees. Companies are spending what they can to curb the risk of insider threats as more and more C-Level executives focus on the "human element" of [network security](#).

Businesses will, and are, spending millions to secure their data. Information on employees, customers, and other sensitive information must be secured for several reasons. These reasons are not limited to just government compliance regulations but also to protect the reputation of the company itself. In addition to perimeter security, common internal security measures include education programs, [data access](#) monitoring, and strict policies regarding use of USB ports and portable devices.

With that said, intentional data theft and unintentional [data loss](#) by authorized employees continue to be top sources of reported data loss. ID Analytics said that organizations continue to struggle with the threat of the "human element" (employees with access to a company's most valuable information). However, to date, little has been done to study and understand how stolen data is exploited once it leaves an organization.

ID Analytics' study, Analysis of Internal Data Theft, sought to expose how, where, and when employees misuse data stolen from the workplace. The research 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. Of these, eight incidents ultimately led to more than thirteen hundred cases of attempted fraud targeting bank card, retail card, and wireless providers.

"In today's data rich environment, organizations continue to struggle with the human element at the heart of data security," said Mike Cook, co-founder and chief operating officer, ID Analytics, Inc. "Companies should be on the alert for what may be the biggest security threat to their customers—employees with access to sensitive customer data. Given the balance between the need to grant employees access to information to complete their job functions and the need to protect sensitive customer data, we encourage companies to implement strategies that increase visibility and reduce the risk of data loss."

Some of the findings in the study included the analysis of the eight internal data breaches where harm was found, and organized misuse ranging from three percent (data leak caused by mishandling data) to thirty-six percent (targeted employee data theft) of the identities stolen. Misuse of the stolen identities occurred in close proximity to the site of the internal data theft. Fraudulent activity relating to each incident of internal data theft took place within twenty miles of the source, indicating that the stolen identities had not been sold or distributed.

In addition, identities involved in internal data theft were misused in similar patterns to those taken via external attacks in terms of period of use and using the Internet to commit fraud. Most of the stolen identities in the study were used very briefly—over a period of two weeks. The internal theft activities also

focused mainly on online channels. In five of the eight internal data breach cases, eighty percent of the fraudulent application activity was online.

If you want to read the full report, you will need to request it from <http://www.idanalytics.com/whitepapers/>.