



## STUDY OF STOLEN IDENTITY USE PATTERNS OFFERS SURPRISES

Source: IT Business Edge | Priority: Fortifying Network Security | Topic: Cybercrime  
Date Published: 8/13/2008

Carl Weinschenk spoke with Cooper Bachman, product analyst for ID Analytics. In late July, the company released a study of employees' criminal misuse of stolen identities.

Weinschenk: What did the study explore?

Bachman: The purpose of the study was to get a more granular view of differences between internal and external data theft. We looked at more than 12 data breaches due to an internal event. Using our proprietary ID Network, we used that data to analyze the relationship between identities involved in a data breach and those that weren't. For example, [suppose] there are three identities with no relationship to each other, with no shared phone number or shared address. If there is a breach event and we start seeing these identities share elements and produce anomalous identity behavior, then you can say that these are not normal consumer patterns.

Weinschenk: Does this happen a lot?

Bachman: What we have seen in the past could be on the level of hundreds of identities and thousands [of such behaviors]. They could use the phone number or the address and apply for credit cards and goods and services. Out of these suspicious relationships, we did case study analysis. On one level, we ran large breach files to isolate the riskiest groups of identities that began to demonstrate suspicious or anomalous relationships with each other. The second part is a case study analysis on those risky groups of identities to determine if there is organized misuse. "The industry targeted most during internal data breach analysis was the wireless industry. In the past, we have seen much more of a focus on the bank card industry. This is the first time it has shifted to wireless. We expect that trend to continue."

Weinschenk: What did you find?

Bachman: We found over a dozen breaches, eight had incidents of organized misuse. Four major themes were found.

Weinschenk: What was the first?

Bachman: The first was that the identities that were stolen by employees or fraudsters were used in a close proximity to where the data was original stolen, from two to 20 miles. That suggests that once bad guys started to misuse identities, they did not often use Internet channels or online. They are not moving out of the geographic areas. This suggests that they are not selling the data and having it disseminated. They are using data for applying for goods and services, not distributing the data over the Internet.

Weinschenk: The second finding?

Bachman: The second is that rates of misuses for victims of internal data breaches were much higher than external data breaches. They were 24 times more likely to be abused than the average U.S. consumer's identity. The internal breaches studied in this analysis were cases where employees took the data maliciously with intent to use it for personal gain.

The third finding was that once criminals began to misuse the data, it was used for less than two weeks. If a fraudster gets a large group of identities, they can use each one sparingly; each is used for a short period of time to prevent suspicions. Then they move onto the next one. It does not necessarily mean that more internal data breaches are happening because of the short period of time. It does mean that portions of identities stolen are used at the beginning of the scam and perhaps reused later. Companies generally offer one year of credit monitoring. What sophisticated fraudsters do is sit on identities for that window and begin to use that data again.

The fourth finding was that the industry targeted most during internal data breach analysis was the wireless industry. In the past, we have seen much more of a focus on the bank card industry. This is the first time it has shifted to wireless. We expect that trend to continue. One reason is that the value and popularity and functionality of handsets have increased dramatically. Cell phones five years ago were used for calling and occasional text messaging. Now they can do whatever a computer does ... The interest around wireless handsets is much more targeted from the ID theft standpoint. Secondly, they will apply for wireless phones or accounts with no intent of paying the bill -- and turn around and sell the physical device. Bank card theft is not necessarily going down, but there is a focus on more wireless.

Weinschenk: What was the most surprising finding?

Bachman: The most interesting aspect is that the IDs were used in locations where they were initially stolen and the fact that they did not sell or distribute the data. We always thought once IDs leave the walls of the organization they are disseminated across the Internet. It is interesting to see that though that may take place eventually, the thieves originally use it themselves. And it is interesting that they might not be as sophisticated and may not know the right avenues to distribute the data.

Weinschenk: How does this track with other studies you have done?

Bachman: This is the first time we analyzed specifically internal data breaches. We've done two studies on generic data breaches, but this one was predominately on external data breaches. There are similarities between first two studies and this one. There also are several instances of dramatic differences in areas such as rates of misuse, proximity of use and which industries were targeted. There were definitely discrepancies between the studies.

Weinschenk: It seems that despite all the technology, the key to data security is the people handling the data.

Bachman: As we discussed in the paper and during the Webinar, there are many ways to go about protecting data: software and hardware network approaches, application access and other approaches. There are security policies, such as preventing people from using USB devices. At the center of all this, though, there will always be a human in control. That human is the most difficult to manage.