

## First we had identity theft, now it is Identity Sale!

Over the last couple of years, there has been increased coverage of the amount of fraud that is being perpetrated as a result of identity theft. There have been cases of credit card skimming, online banking credential theft through phishing etc.

This has taken a new twist in the recent weeks with the rise of "Identity Sale". This relatively new phenomena is where corrupt insiders are taking large databases of customer details from their employer and selling them to external organisations. This has come to light in a massive investigation in the New Jersey where the police have arrested and charged up to nine people.

Seven of these were employees at Bank of America and Wachovia and the others were involved in companies that make information on an individual's financial status available for a fee. These legitimate services provide a service like a credit or background check, but the source of their information in this situation was the illegally gotten data from the banks.

Unfortunately, this is not the first time that some of these financial institutions have been in the spotlight due to the loss or compromise of the personal information of their customers.

In February 2005, Bank of America admitted publicly that it had lost tapes that contained the personal details on more than 1.2 million Americans that were customers.

This followed the admission by ChoicePoint, an electronic data-warehouse of personal information that is supplied to insurance companies and other businesses that the identities of almost 150,000 American citizens had been stolen. By the time of the disclosure, almost 1,000 of these stolen identities had resulted in identity fraud based crime.

In March of this year, consumer database specialist LexisNexis in the United States was broken into, and more than 30,000 electronic identities of American citizens were compromised.

These recent incidents highlight the increased risk that organisations face from insiders as well as external threats when it comes to compromising the identities of their customers.

So much data is now centralised in data warehouses today that a weakness in the security configuration of one of these databases would expose huge amounts of sensitive information. Even on internal networks, there is a growing requirement for the encryption and protection of database content. This would at least make it more difficult for malicious internal, trusted users to steal large amounts of data as in the Bank of America case outlined above.

It also highlights the need to focus attention of the treatment on backup media, and the encryption of the data stored on this media. In many organisations, record and archive management specialist companies collect the media from the computing facilities. While their integrity is not in question, there are many organisations that do

not check the credentials of the couriers used to collect the media, and it is not a huge leap to see identity theft criminals pretending to be couriers for these management companies. If an organisation enters into an arrangement with an off-site storage specialist company to manage their backup media, they should have agreed in advance identification procedures for the couriers that are collecting the media.

Any organisation today dealing with the storage of personal information of their customers, especially if that includes credit/debit card data, should be investigating the use of robust encryption. This would ensure that even if the tapes fell into the wrong hands, or unauthorised users could access the databases, the information would remain secret.

These incidents in the United States are not isolated. These stories must serve as a wake up call to all organisations to be vigilant when dealing with the personal information of others.