

Data Theft.....How can it be controlled?

A large financial institution, we will call it Money Bank, requested help in investigating the compromise of user account information, having received hundreds of user complaints concerning unauthorized transactions during the prior week. The internal IT staff was knowledgeable enough to perform analysis of the accounts with fraudulent activity. This led them to suspect the loss of a particular report: Recent_Money_transfer.doc, which contained sensitive information for several thousand of monies, transferred during the week and included account numbers, usernames, temporary passwords and IP addresses. The same diligent IT team performed analysis of the file server access logs and found that only four employees tasked with entering the data had rights to this file. Only one of those four accessed it before the suspected compromise. Furthermore, it was discovered that this access occurred from the employee's computer. But on further investigation, it was found that this employee, has at the scheduled time sought permission, and left to attend a parent teacher meet at the child's school. The data had been downloaded on to another device from the suspect's computer, (which at that point was not locked) - it could have either been a laptop or a mobile phone. Mobile phones now are capable of storing up to 4 GB memory. That's equivalent to physically storing data on 400 boxes of paper in nine filing cabinets with the capacity to retain four million emails

Impacts of Data Theft

- Across the globe, more than 1.4 million users have suffered from identity theft fraud, costing banks, and card issuers \$1.2 billion in direct losses in the past year.
- An outsider attack against a large company cost \$57,000.
- Close to 51% of the Companies, do not reveal their security incidents to law enforcement because this will affect their stock market price or company image.

Reasons for Data Theft

1. Lack of Security Laws with respect to data theft in India
2. Lack of stringent security measures for visitors.
3. Lack of Data Security System in IT companies encourages data theft among employees.

With the implementation of complex IT systems, sophistication of these threats is consistently increasing and the methods employed to combat these threats must match this level of sophistication. As a result, it is necessary for all systems users to be especially vigilant at all times.

How do you think Money Bank could have solved the issue?

To start with, it is advisable to have a fool proof visitor management solution installed at every office complex, so that photographs of all visitors along with their details are captured for any verification purposes at a later stage. The details of the individuals including gadgets carried with them, e.g. mobile phone, laptops (with the serial no) etc are also captured along with their personal info. This makes tracking down easier.

Money Bank could have made at least some break through if only they had a visitor management software installed. But alas.... They did not have one....and as for the data lost.....well they are yet to solve the case!

About the Author

Author: MdFaizullah

Email: faizullah@cogentmail.com

Website: <http://www.usetouchpoint.com>

Source: <http://www.articletrader.com>