AWARENESS FROM ATTACKS ON INFORMATION AND ITS SECURITY

Vishwas
Vishusem.22@gmail.com

A small step to know the theft in computer world

Theft word in computer world is describe that when data is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers. Information theft is a growing problem. Lots of technologies have been used to prevent data from the black hat hacker like firewalls and intrusion-detection systems. The damage caused by theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices and other hand-held devices. Data thefts are emerging as compliance and computational risks for organizations. According to new research over 60% of data breaches originate from an internal source or event. One reason for this is that today’s data rich environment organizations continue to struggle with the ‘human element’ at the heart of data security. It can be extremely difficult to balance the protection of sensitive data with granting access to employees who need it to complete their daily job requirements.

Companies identified as victims of cyber-attacks in media reports suffered stock price drops of 1% to 5%, which translates into shareholder losses of between $50 million and $200 million. The annual cost of data theft due to online fraud and application hacking is about $6 billion, with the costs to the financial institutions.

Problems faced due to attack

Attacks on information is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as USB flash drives, iPods and even digital cameras. Since employees often spend a considerable amount of time developing contacts and confidential and copyrighted information for the company they work for, they often feel they have come right to the information and are inclined to copy and/or delete part of it when they leave the company, or misuse it while they are still in employment. While most organizations have implemented firewalls and intrusion-detection systems, very few take into account the threat from the average employee that copies proprietary data for personal gain or use by another company. A common scenario is where a sales person makes a copy of the contact database for use in their next job. Typically this is a clear violation of their terms of employment.

The damage caused by data theft can be considerable with today's ability to transmit very large files via email, web pages, USB devices, DVD storage and other hand-held devices. Removable media devices are getting smaller with increased hard drive capacity, and activities such as pod slurping are becoming more and more common. It is now possible to store more than 160 GB of data on a device that will fit in an employee's pocket, data that could contribute to the downfall of a business.

Data theft is information which is illegally obtained from an individual or a
business. This information is usually things like login information, SSN Numbers, sensitive personal information, credit card credentials, or confidential corporate data. It would be critical for people to guard this information to the best of their ability in order to avoid any negative side effects from posting this online. There have been countless instances where people have posted information about themselves and had adverse effects from it. There are a few major cases of personal data theft that stick out when talking about these types of cases. The 2 major episodes of personal data theft are that of the Face Book security breach and the IPAD security breach. The Face Book security breach took place in 2010.

**Types of attack on information**

Data can be stolen in many ways.

**Hacking:** This is by far the most common way of stealing data with least chances of getting caught.

A hacker gets into a system where he or she is not supposed to be, and steals whatever data was aimed at. Hackers find their ‘gate way’ through gaps in the security system or by hoodwinking gullible employees / surfers in order to gain access to a system.

**Posing:** Appearances can be deceiving. The attractive website that has popped up offering you a great Holiday treat may actually be a data thief trying to get into your system under the ‘mask’ of a piece of harmless spam. In a case of corporate data theft last year, the thief posed as a potential customer and got entry to a company’s data bank through the computer of an employee who did not suspect anything in his eagerness to catch a potential client.

**Remote Access:** Is the cursor moving about on its own even when you have not touched the mouse? Does the indicator show that a program is running even when you are not working on anything and have no windows open? Do not ignore the symptoms – a data thief is already sitting in your computer. Remote access allows the thief to gain control of your machine from wherever he or she is and operate it, steal data from it, and even distribute virus from it!

**Spy ware:** Spy ware is often brought in by adware. The thief may not sit in your system, but your key strokes or mouse clicks would be spied upon, revealing what you are doing and ‘reading’ the data as you put it in. And you have opened the gate by clicking on an innocent looking add.

**Pod slurping:** Music is now stored in iPods for almost all domestic users. You would usually not suspect an employee rock to music while working as usual. The thief knows this and is using the iPod to obtain data outputs from the computer where it is plugged in.

**Blue Snarfing:** Bluetooth devices have become popular in a very short while. Using his or her Bluetooth-enabled cell phone or laptop, the data thief lifts data from a restricted computer in silence and mostly unnoticed.

**Thumsucking:** Another tiny and dangerous device is the USB storage drive. All an employee needs to do is plug in a pen drive, and 2 GB of data would flow in quietly into the pocket from the computer. As the global economic downturn takes its toll in the guise of losses and layoffs, a survey released February 23, 2010 revealed that a majority of exiting employees are taking their companies’ information along with them. The survey, conducted by the security company Symantec in collaboration with Poneman Institute, included 950 individuals who lost their jobs during the last year, out of which 59 percent admitted to lifting crucial customer data like contact lists, from their firms once they exited from their jobs.
The workers who lost their job during the past year lifted a variety of crucial information, including email lists, customer details, employee records, and non-financial information, the survey said. Incidentally, these spiteful workers use the data to obtain a new job, start a business of their own, or to take revenge from the company, the study added. The study claimed that a majority of these information theft incidents could have been evaded had the firms employed data-loss prevention measures, as around 82 percent of the individuals surveyed stated that their ex-employer didn’t even perform a document check before they left their jobs. Of respondents who admitted to taking company data, 61 percent also reported having an unfavorable view of their former employer. This survey which was conducted in January 2009 is not entirely breaking new ground when it comes to the disturbing realization that companies are suffering staggering losses and compromises when it comes to stolen data. What business managers and in house counsel do need to be concerned about is that this survey reveals a corresponding increase in stolen data with greater numbers of employee layoffs. It is time for outside commercial lawyers to be offering business clients with precautionary recommendations to handle these circumstances in the prelitigation stage. Why? Because digital ‘fingerprints’ are often left behind by the data thief for a short period of time. Roughly 67 percent of those in the survey acknowledged taking company data from their old employer said they did so in order to leverage a new job. Our experience in investigating employee data theft has had the most favorable outcomes when our forensic examiners were brought in shortly after the employee’s departure. The sooner the better in order preserve and recover electronic evidence that can identify the who, what and when answers that are associated with data theft to support a claim and/or a TRO. Clients can take a few proactive measures to secure the ‘crime scene’ before a computer forensic examiner is retained.

**Prevention from information theft:**
1. Educate the users. Make corporate policies regarding the use of removable media clear by including “iPod” and “MP3 players” in the text.
2. Consider endpoint security products that learn what the organization deems sensitive and blocks that data from being copied without authorization. Note that some of these products only alert an employee when unauthorized action is being taken, others prevent copying.
3. Also consider endpoint security software that captures forensic information, so that a legal case can be constructed against the employee in the event of data theft.
4. An alternative to content-aware software is policy-based encryption, products that can automatically encrypt data based on parameters such as where it is being copied to.
5. In some scenarios, such as a financial services company, it may make sense to ban the use of iPods for employees who come in close contact with sensitive data, like traders, but allow their use in other areas.

**Some important action taking against attacks**

**How to Protect Data:** Installing and maintaining IDS, Antivirus software, firewall, and encryption and tracking systems for internal network access. Granting limited and monitored use of the internet, with policies being reviewed periodically. Banning USB ports and not allowing Bluetooth-enabled devices within the work area. Maintaining updated backup.