THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

Data Protection: A Case Study on How to Assuage Theft of Data

Samson Oluwaseun Fadiya
PhD, Management Information System, Girne American University, Cyprus
Akpesiri John Olotewo
PhD, Marketing, Girne American University, Cyprus
Oyeneyin Taiwo
MSc, Management Information System, Cyprus International University, Cyprus

Abstract:
The massive theft of customer records (Data or Information) from organizations is a widespread problem in today's large-scale businesses. Therefore, we may resolve that data or information theft can be defined as a set of data or information theft contain within another set of unauthorized removal of confidential information business data warehouse.
In the immediate past, the thefts of data or information that have reached a greater number of companies have caused business worry. For an instant, this theft of data is perpetrated through the corporate network and reach the central database storing consumer information and credit card numbers. And these thefts activities were stimulated by organizations or companies' lack of ability and proper planning to fix dangers linked with the breach and security of their data before or when it happens. It is necessary for companies to perform current happening risk analysis to secure their systems because theft of data or information is a management issue.
Mainly caused by decisions made by the management of these organizations and not necessarily a technology deficiency. This paper examines theft of data or information on companies, in order to explain the defects of management pattern that lead to the theft, the types of attack launched on company information from these hackers and vital roles that management acts in the security of data or information.

Keywords: *Hackers, Information security, Management, Policies, Technology*

1. Introduction

Theft of information is a break open for hackers who decipher corporate information of large organizations and the bit of expects profits for this stolen information is on a rampage, it is, therefore, necessary for organizational information systems can defend this worthful data or information asset.

The growth in globalization and a deficiency of cyber environ allow for an environment to mature for identity thieves to function from within the environs, as well as from outside. More so, identity theft is frequently connected with several other vicious activities. Such activities range from bank fraud, employment fraud and credit card. Individuals and companies who had fallen prey to information theft are still victims of great loss and financial burden, and it is critical that identity theft had affected greatly the national security, and it's economical. In addition, these fraudsters can also open new accounts in their victim's name in order to attack victim credit card accounts of both existing and future credit card accounts.

Identity theft has become dominant in today's global connections as it effects long lasting and its impacts can be personally painful and financially crushing. These can stretch not only to individual victims, but also businesses, governments, and our society in general [2]. Immediate past breaches of information systems that have led to thefts of identity or information have demonstrated that management practices were components issue and the primary cause of the information theft, not technology. For example, risk analysis can be used to avoid the information or identity theft when third party tries to lunch or commit a crime.

Now, It is becoming an essential that companies, business and individual examine their practices and policies to avoid risks consorted with information theft. Therefore, the answer or revolution to theft of identity or information does not require technology alone, but also commands an understanding by management of such business and the risks associated with it. This paper analyses and test the stealing of information from a different source, ranging from individual to companies, in order to explain practices of management and the defects that lead to the theft and technology tools necessary to combat information theft. The Identity Theft Resource Center (ITRC) has predicted that engineered crime groups will become more convoluted in identity theft related activities and increasingly transnational crime such as credit card fraud [4].

For Instant, identity or information thieves are stealing millions of dollars through unauthorized transactions and new accounts of credit card opened fraudulently in their victim names of ignorant consumers using social engineering scams and other illicit methods. Financial losses from offline and online identity theft have declined slightly [5].

2. Case Studies

2.1. Case I: International Retailers

In 2010, it was discovered that all major international retailers were the victim of one of the largest known data thefts on record. It was revealed that the attackers had been able to steal the credit card information from hundreds of thousands of customers located all over the world. The information had been stored on a server located at the business' corporate headquarters, meaning that, once the attackers gained access to the server, they had access to all the personal information that is available. The exact method of attack was never disclosed, though it was widely assumed that a wireless network at one of the corporation's retail outlets had been the initial point of attack.

So, was this retailer running an IDS on its network? Initially, the response is might seems "No." Because, it may be hard to recognize if or not the retailer was using an IDS. Recall the major weakness with name-based IDSs—the reliance upon attacks that have been previously observed and cataloged. In other words, if the vendor of an IDS has not encountered a particular type of attack before, there would be no way to craft a signature to defend against it. Customers would, therefore, be vulnerable to that form of attack. In the case of a major retailer, it is entirely possible that it was using an IDS, but the attackers used a new and never-before-seen type of attack, completely bypassing the signature-based IDS.

Recall that IDSs also suffer from another problem: high false positive error rates. In other words, both anomaly and signature-based IDSs can claim that an attack is occurring when, in fact, there is no attack. It is common for weary network administrators to decrease the sensitivity of IDS systems to avoid these false positives. So, in the case of our retailer, it is entirely possible that the IDS may have recognized the intrusion, but the administrator had configured the device only to sound an alarm when it was extremely confident that an attack was happening. To put it plainly, the administrator may have told the IDS, not to sound the alarm unless something is happening. As it turns out, the retailer was still utilizing WEP to protect the wireless networks in its stores as late as 2006. Although, this was happening long after the discovery of the flaws in WEP (2001) and the release of the replacement WPA protocol (2002-2003). It is possible that an attacker used a regular laptop and wireless card compromised their WEP encryption. Once the attacker had his/her foot in the door, he/she was able to cause much more damage than anyone at the store ever anticipated.

In the Challenge we learned of a retailer that had its database system compromised, resulting in the stealing of credit card information along with personal information on its customers. It is believed that the attackers' initial point of entry was a wireless network in one of the retail stores. In the Challenge, we discussed a major retailer who had its network compromised by hackers. The hackers entered through a wireless network and eventually were able to work backwards through the corporate network and reach the central database storing consumer information and credit card numbers.

All indications are that the victim did not have an IPS installed. Or, if there indeed was an IPS installed, it failed to detect the intrusion. The fact that the attack succeeded would seem to support such a conclusion. It is certainly possible that an IPS may have detected the attack, but failed to stop its progress, though this is unlikely. Most IPSs alert administrators whenever actions are taken, regardless of the outcome. Recall from the Challenge that most experts believed that the initial penetration of the retailer's security system involved an improperly secured wireless network. Given everything that you have learned here, what seems like the most-plausible explanation?

2.2 Case II: Universities Administrator

Over the past decades, tertiary education has increasingly used computer systems to track sensitive information, such as the grades earned by students. The computer systems a tempting target to desperate students looking to improve their grades by any means necessary. Imagine that you are a system administrator at a large state university. One of your responsibilities is to defend the grade reporting system against attacks by students seeking to alter their transcripts. The school you work for has a reputable computer science department, so it is safe to assume that some of the attacks could be quite technically sophisticated.

If you were sure your systems were always configured correctly, and that security incident could not possibly occur, and then logging, and auditing would have very little point. For this reason, logging and auditing must become part of the ordinary routine for all security-minded administrators. Though they are sometimes used synonymously, logging and auditing is different things. It is easy to realize how they are able mistaken for each other, however. As we will learn shortly, logging and auditing both involve a careful examination of detailed, technical information. There are, however, fundamental differences between logging and auditing. Logging is a concept most people are familiar with, is the action of storing essential data for review at a later time. As most people have probably observed at one time, or another, log files can be a critical part of determining what happened after an incident or failure.

While auditing, on the other hand, is an activity that many administrators may not have ever performed, though they should have. Generally speaking, auditing is the process of periodically inspecting something (a computer, database, Ledger, etc.) with the goal of ascertaining the actual status of that item. In the financial arena, audits are a necessary control against fraud and theft. They ensure that accounts are in order and inventories match the goods on hand. An information security professional will perform audits against account activities, permissions, settings, network activity, etc.

To illustrate, suppose that our attacker can steal, observe, or guess one of his/her professor's passwords, obviously the professor's account has now been compromised. As a database system administrator, your goals, is to minimize that cost. Yes, the student will probably be able to change the grades awarded by that professor. We need to prioritize our security in a high -level, in order to make sure that the student cannot change every grade in every course. That is where permissions come in—by restricting the professor's grade-changing permission to only courses (s) he teaches, the damage has been effectively contained.

The obvious solution to this challenge is through the judicious use of auditing and logging. Auditing serves as a means of identifying deviations from standard system configurations, which could cause vulnerabilities, and also as a means of discovering attacks after they have occurred. Logging enables you to figure out what went wrong, possibly who did it, and what possible defenses could be erected to prevent future compromise. Regarding the Challenge, it is crucial to protect user credentials and set user's permissions correctly. If, you are placed in the role of a systems administrator at a college. Your job is to ensure that grades and other sensitive information are protected from highly skilled and motivated attackers (i.e. Students). With the vast amounts of data and personnel to manage, though, knowing when and if you have been compromised a real challenge.

Now if you are handed a role of a database system administrator who is charged with defending the database system from unauthorized access by highly skilled, highly motivated college students. Honeypots could be a technology that might be of great use to you for a variety of reasons. First, students who are attacking your honeypot is (probably) not attacking your real systems. At the very least, they are distracted and having to spread their energy between assaults. Secondly, it is very possible that you might be able to gather enough forensic information from your honeypot to have disciplinary action taken against those students.

2.3. Case III: American Independent Financial Corporation (AIFC)

Though the firm is over 40 years old and is a mid-size financial services firm, the recent passage of many new auditing and accounting laws like the Sarbanes-Oxley Act has caused a rapid expansion of business. In the past, the firm outsourced most of its IT functions to local providers, but now management has made the decision to bring these functionalities back in-house. As the company software development and database report writer, you have traditionally not been involved with the maintenance and upkeep of the firm's IT resources. As the company's only employee with any extensive IT experience, though, you are being counted to play a decisive part in getting the system setup and functioning in a secure manner.

It is not essential for you to interpret all of the "ins and outs" of securing the company's IT as additional staff will be hired to fulfill these roles. However, it is necessary for you to explain the big picture of what is occurring, since you are now the effective Chief Information Security Officer (CISO) of the firm. It is also vital to perform IT functions in the event that new staff members do not remain with the firm.

As you prepare to shift IT operations back "in-house," your main security concern is outside attackers. Most of those in senior and mid-level leadership of the company have been with the organization for years, and a high degree of trust has developed between the employees. Regular, thorough audits also offer assurance that outsiders, not insiders, pose the greatest threat to the company's security. The content in this module is primarily concerned with protecting systems from outside threats. Although insider threats may be as common and also pose a significant risk to any organization, this module is focused on outsider threat protection. We will cover server, client, and router security, along with a discussion of principles and best practices for system protection.

The need for server security for your organization should, hopefully, be self-apparent. The servers that your company will house will be involved in the creation, transmission, and storage of your organization's sensitive information—information that could, if disclosed or destroyed, lead to the closing of your firm. As the de-facto CISO, your role in the process is not necessary to understand how to lock down each and every server on your network, but is instead to know enough to supervise and manage the IT staff who will be performing this work. As an administrator, you must remember to secure your clients (i.e. Desktop computers). Every computer on your network, both server and client, represents a potential launching pad for attacks. Systems that may be protected against direct frontal attacks might still be vulnerable to attacks on the local network, and attackers recognize this. For this reason, every client system on your network has to be as locked down as possible since each system could represent the final tool needed by an attacker to breach your security successfully.

Though often overlooked, router security is extremely critical to the overall security of the system. An attacker who can seize control of the router can change or drop any packets that (s) he wants to. It could lead to DoS attacks, or worse, man in the middle attacks as the captured router begins forwarding sensitive packets to some system that you do not control. In the event that an attacker takes control of one of your routers, your best case scenario is probably to hope for a breach of confidentiality. Unless all of the data flowing over your internal network is encrypted, an attacker will be able to eavesdrop, modify, retransmit, or other malicious deeds to the data on your network. It means that, despite your best efforts to secure your servers, data breaches could still occur, placing the survival of your firm in jeopardy.

However, knowledge of how systems operate is not exactly the same as knowing how to manage systems. Now, it is a good idea to use best practices. Best practices represent the knowledge gained by the trial and failure of others (ex: the need for patch management). As a new CISO, the use of best practices is an absolute requirement; without them you will probably make unfortunate errors that will disrupt business activities, or worse, result in a security breach. The need for server security for your organization should, hopefully, be self-apparent. The servers that your company will house will be involved in the creation, transmission, and storage of your organization's sensitive information—information that could, if disclosed or destroyed, lead to the closing of your firm. As the de-facto CISO, your role in the process is not necessary to understand how to lock down each and every server on your network, but is instead to know enough to supervise and manage the IT staff who will be performing this work.

2.4 Case IV: Convectional Identity Theft Case

Dorothy is a manager in the IT department of Telecommunication company in Europe. She has a health insurance plan that insures treatment at the same hospital as all her family does. Afterwards, Dorothy's husband was diagnosed with heart related disease; he was, therefore, admitted to the hospital for about a month. Her husband's condition becomes worse, and he eventually died in his deteriorating condition. And then, Mrs Dorothy relocated to live with her brother. And for some months after, she was contacted by a distributed agency who asked her of the payment of on the new-industrial photocopy machine she purchased, at a specified location and time.

Mrs Dorothy was surprised as she was not aware of purchasing such photo-copy machines, so she refused and expressed that, she has no debts after her husband's death, as her claim to have cleared all debt and have no credit account open anywhere. The distributed agency is persuasive that she is obliged to repay on the debt, and she claimed to have no idea. They verify her identity, previous information of where she had lived and her bio data.

Finally, Mrs Dorothy draws a credit account on herself and detect that over 110, 000 USD in charges had been cleared on accounts and she stated at no point in the past she opened it. She remains adamant that she did not purchase the industrial photo-copy machines, neither did she was in the claimed location it was bought.

3. Results and Discussion

Security breaches could have been averted with proper risk assessment and risk analysis, or at least the probability of a security breach could have been reduced greatly [3]. For all security breaches, the prevention or at least the reduction of the probability of a security breach begins and ends with decisions that management makes.

In an organization, when a security breach occurs it causes a company to re-evaluate their policies that guide their information security. With this rash of security incidents that have recently taken place, companies do not need to wait until the security breach happens to evaluate their security systems and analyze their risks. Companies need to have an ongoing risk analysis that is continually developed and re-developed. They need systems that are ever changing to meet new threats and new security weaknesses from both business practices and technology viewpoints. Looking at the events that happened at International Retailers, Universities Administrator, American Independent Financial Corporation (AIFC) and Convectional Identity Theft Case. These companies have technological solutions to protect their data from being stolen, but they failed at weighing equal importance the security of the data from a business issue perspective. It showed in their inability to assess the risk properly in the business practices. In several of the cases, the theft of information occurred because of the business practices of the company, and technology was not even involved.

Also, companies need to learn from the mistakes of others because history will repeat itself if the lesson is not learned. Security policies and practices need the flexibility to change, and management has a responsibility to make these changes when new threats or the new weakness surface so that they can protect their data with the issues that happen in Convectional Identity Theft Case. Companies and organizations need to realize the importance of making information security a business issue, as well as a technological one. With the issue that happened with International Retailers, they did have security systems in place to protect their data from being stolen, but it lacked the kind of coordination require for novel innovation in the IT security. Now, by making information security a business issue, companies must add strategic, operational, and organizational defenses to protect their data.

4. Conclusion

As most identity thefts occur, companies that make their money from storing this information are going to become liable. 'This bill will ensure that information brokers are held accountable for enforcing robust security practices to prevent thieves from gaining access to sensitive consumer data. And it gives consumers important new rights to examine the information maintained about them and to correct any errors they may find' [1]. Companies need to find the importance of protecting their data from both technology and business practices weaknesses. Companies view the protection of their data from a technology issue, but fail to realize the importance that management plays in protecting their systems with the creation of policies and understanding the risks that face their information systems.

From a consumer standpoint, if a company is making profit from someone's personal information and they fail to protect this data, should they not give any status? The companies own and manage customer information, and individuals have little power over their information that is controlled by these organizations. As identity theft continues, and companies fail at protecting their data, legislation will be passed that will force companies to comply with regulatory standards that may force companies to give this reputation to individuals who have their identity stolen.

There are steps that companies and organizations need to take to protect themselves from the theft of information. First, companies need to be prepared when a security breach occurs because a risk to an asset is never zero percent. Organizations need to establish policies and risk assessments that protect their data from both technology risks and business practices well before a security breach occurs. It is achieved by companies having the organizational structure that allows management, to understand the business processes entirely. And the technology that presents their information systems to threats. Also, companies need the ability to change and adapt to new threats that oppose their information. It is impossible to keep all security breaches that lead to the theft of information, but companies will need to have policies and practices in place to better protect the data [6].

Companies will need not only to weigh technology risk to their information, but also understand the business issues that expose their information to theft. It no longer matters how the information stolen, whether it was a hacker or a social engineer that committed the crime; companies need to protect their information from all threats and minimize their risks from all aspects.

5. References

1. Javelin Strategy & Research, 2007 Identity Fraud Survey Report, February 2008.
2. Sean B. Hoar, "Identity Theft: The Crime of the New Millennium" (2001) 80 Oregon L at 1423.
3. eBay, Target security breaches could have been avoided with ... (n.d.). Retrieved from http://finance.yahoo.com/news/ebay-target-security-breaches-could-093600205.html
4. Identity Theft Resource Center, ITRC Forecasts Black Ice Ahead in 2011, December 15, 2010, http://www.idtheftcenter.org/artman2/publish/m_press/ITRC_Forecasts_for_2011.shtml.
5. Online Identity Theft: Changing the Game - SlideShare. (n.d.). Retrieved from http://www.slideshare.net/bluesme/online-identity-theft-changing-the-game
6. Privacy Policy: Centerville Pie Company (n.d.). Retrieved from https://centervillepies.com/privacy-policy/