A Case Study on How to Manage the Theft of Information

Robert M Polstra III
Kennesaw State University
2004 Westwood Rd
Smyrna, GA 30080
404-641-8937
rpolstra@hotmail.com

ABSTRACT
This paper shows the importance that management plays in the protection of information and in the planning to handle a security breach when a theft of information happens. Recent thefts of information that have hit major companies have caused concern. These thefts were caused by companies' inability to determine risks associated with the protection of their data and these companies lack of planning to properly manage a security breach when it occurs. It is becoming necessary, if not mandatory, for organizations to perform ongoing risk analysis to protect their systems. Organizations need to realize that the theft of information is a management issue as well as a technology one, and that these recent security breaches were mainly caused by business decisions by management and not a lack of technology.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**] General – *Security and protection.*

K.3.2 [**Computers And Education**] – Computer and Information Science Education – *Curriculum, Information systems education.*

K.4.1, .2, & .4 [**Computers and Society**] - .1 Public Policy Issues – *Abuse and crime involving computers, Computer-related health issues, Ethics, Intellectual property right, Privacy.* .2 Social Issues – *Abuse and crime involving computers.* .4 Electronic Commerce – *Security.*

K.6.5 [**Management of Computing and Information Systems**] – Security and Protection – *Authentication, Invasive software, unauthorized access.*

General Terms
Management, Security, Human Factors, Standardization, Legal Aspects.

Keywords
Information Security, Security Management, Information Security Management.

Information Security Curriculum Development (InfoSecCD) Conference '05, September 23-24, 2005, Kennesaw, GA, USA.

1. INTRODUCTION
After counter-terrorism and counter-intelligence, cyber crime is the third highest priority for the U.S. Federal Bureau [4]. With the rise of the theft of information and the lure of big profits for this stolen information, it is necessary for information systems to have the ability to protect this valuable asset. It is estimated that a credit card number unsupported by any other documentation is worth $10, and a credit history report retails for $60 [2]. Recent breaches of information systems that have lead to thefts of information have shown that management practices and not technology was part of the issue and in some cases the primary cause of the theft of the information. With each of these thefts, there is a third party committing a crime, but in each case, risk analysis could have been used to avoid or to help mitigate the theft. It is becoming a necessity that companies examine their business practices and company policies to avoid risks associated with information stealing. The solution to information stealing does not reside in technology alone but also requires an understanding by management of the business and the risks associated with it. This paper examines the theft of information from different companies in order to explain the short coming of management practices that lead to the theft. .

2. CASE STUDIES

2.1 Case I: Citigroup
In May of 2005, Citigroup lost computer tapes that were being sent to the credit bureau via UPS that included Social Security numbers and payment history information for 3.9 million customers. After this event, this New York based company has decided that it will start sending its data to the credit bureau electronically using encryption [8].

Citigroup should have learned a lesson from Time Warner who lost a shipment of backup tapes that contained personal information of 600,000 employees that was being sent to an offsite data storage company in March of 2005 [9]. But the question remains, why was Citigroup sending sensitive information unsecured? Why did they not encrypt the data in the first place, and why did they realize that these tapes could get lost or stolen as evident to what happened with Time Warner? The answer is because they did not correctly identify the risk. Citigroup believed that UPS was a secure method for sending this information and that the data would be difficult to retrieve off the tapes because of the hardware needed to read the tapes. Citigroup needed to evaluate this risk of properly protecting confidential information while in transmission. Now, Citigroup has the issue of dealing with the negative public associated with this event, and the loss of any potential customers/revenue it will lose because of

it. This issue would have been avoided if Citigroup would have properly identified this risk and taken the steps to protect this information. If the tapes were lost and the data was encrypted, then this story would have never happened.

2.2 Case II: ChoicePoint

Choicepoint has made more than 50 acquisitions since 1997 to make it one of the largest collections of personal data in the United States. Choicepoint sells data "to clients doing background checks on job and loan applicants and conducting criminal investigations" [10]. On February 16, 2005, ChoicePoint went public to tell 145,000 people that identity thieves may have gained access to their personal information including their Social Security numbers and credit reports. "Authorities believe it was the work of a group of people who used IDs stolen from legitimate business people to set up phony businesses that contracted with ChoicePoint for ID checks, Bernknopf (ChoicePoint's spoke person) said" [5].

With ChoicePoint's security incident, there was no firewall hacked, or an IDS fooled. This was a deceptive scheme that took advantage of security holes in the business process. ChoicePoint's CISO, Rich Baich, stated "The mislabeling of this event as a hack is killing ChoicePoint. It's such a negative impression that suggests we failed to provide adequate protection. Fraud happens everyday. Hacks don't" [10]. ChoicePoint seemed to push that they were the victims of fraud, and not at fault. The bottom line is that confidential information was stolen, and the individuals who had their information stolen do not care if it was hacker or if the company was a victim of fraud. ChoicePoint failed to identify holes in the business process to allow this event to happen. Which if someone hacked into their system, it would have lead to the same result, the theft of information. ChoicePoint needs to recognize that identifying risks with their business process is just as important as securing their information system from an external hacker.

2.3 Case III: Egghead.com

Egghead Software was a company that opened in 1984 to sell computer hardware and software that grew to have more than 205 stores worldwide. Then in 1998 the company moved its business to the internet as Egghead.com.

In December of 2000, Egghead.com stated that "a hacker has breached its computer system and may have gained access to its customer database" [6]. Jerry Kaplan, Egghead.com's co-chairman, stated that there was "no evidence" to support that the database with the credit card numbers for its customer was stolen but, he also could not give confirmation that they were not stolen. "Egghead's inability to determine how many of it's customers credit cards had been compromised may mean that the company does not have a real-time auditing system in place, said Paul Robertson, senior developer for security service firm TruSecure Corp. 'If you don't know how many credit-card numbers you lost, you are giving a quick, blanket, worst-case answer--and then finding out what happened afterwards,' he said." [1]. The way that Egghead.com handled its security incident showed that they did not have a good plan to manage the theft of information, and it appeared as if they made the plan to handle this situation as it happened. This lack of planning and risk analysis by management caused Egghead.com's business to suffer tremendously. Shortly thereafter this event, Egghead.com went into bankruptcy, and on November 26, 2001, Amazon.com acquired Egghead.com's assets in the Bankruptcy Court [6].

It appears the inability for Egghead.com to successful determine with certainty the extent of information stolen caused more damage to the company's reputation then the actual event itself. If Egghead.com had a well developed incident response plan in place to handle this security breach and a way to handle the media that followed, Egghead.com may have been able to weather the storm and stay in business. But all customer confidence was lost and Egghead.com was not able to recover.

2.4 Case IV: New Jersey Crime Ring

Bank employees for Wachovia Corporation, Bank of America Corporation, Commerce Bancorp Inc., and PNC Bank stole information on 676,000 customer accounts that are all New Jersey residents. It is considered the largest banking security breach in history by the U.S. Department of the Treasury. "The suspects pulled up the account data while working inside their banks, then printed out screen captures of the information or wrote it out by hand, Lomia (a New Jersey Police Detective) said. The data was then provided to a company called DRL Associates Inc., which had been set up as a front for the operation. DRL advertised itself as a deadbeat-locator service and as a collection agency, but was not properly licensed for those activities by the state, police said" [13].

With this security breach, there was no technology involved. No hackers breached the information system. This was completely an inside job. The question becomes of how this could have been prevented? The answer is that in some cases the theft of information can not be prevented. The only the thing that management can do is be prepared for when it does happen. Because of incidents like this, it is becoming a duty of management to have an incident response plan in place long before a security breach happens. From a risk analysis viewpoint, an incident like this is difficult to detect and almost impossible to stop before it happens. But when it does happen and the criminals are caught, it becomes a necessity to punish the ones responsible to the full extent of the law to deter others from following suit.

2.5 Case V: LexisNexis

LexisNexis is provider of legal and business data. In March of 2005, LexisNexis announced that the information on 32,000 people was stolen. These breaches occurred at one of the subsidiary companies, Seisint Inc. Seisnt Inc. was the company who was the provider of data to the Multistate Anti-Terrorism Information Exchange (MATRIX) system. "LexisNexis, which acquired Seisint of Boca Raton, Florida, in September for $775 million, expressed regret over the incident and said that it is notifying the individuals whose information may have been accessed and will provide them with credit-monitoring services" [12]. In this incident, hackers stole username and passwords of legitimate users to access the confidential information. In a statement, "Kurt Sanford, president and CEO of LexisNexis Corporate and Federal Markets, said that the company will improve the user ID and password administration procedures that its customers use and will devote more resources to protecting user's privacy and reinforcing the importance of privacy" [12]. This security breach is very similar to the incident that happened at ChoicePoint who is one of LexisNexis's competitors.

There are several policies that should have been implemented that could have reduced the risk of this security breach. Since LexisNexis gives third parties access to its confidential information, there becomes a need to educate these organizations on certain practices to protect the data. Where was this education, and was there a lack of education due to the possible effect that it could have on business? Also, what was the password policy for its customers? LexisNexis has not elaborated on the details of the security breach, but considering the statement of the CEO of LexisNexis after the incident, there clearly seems that there was a failure to detect the risk associated with their customer's password policy that could result in a theft of information. LexisNexis inability to properly assess this risk caused the security breach. Through education and a secure password administration policy, this event could have been avoided.

3. RESULTS AND DISCUSSION:

When analyzing these case studies, an important thing to ponder is that for every security breach reported, how many go unreported? These security breaches could have been avoided with proper risk assessment and risk analysis, or at least the probability of a security breach could have been reduced greatly. For all security breaches, the prevention or at least the reduction of the probability of the 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 a security breach happens to evaluate their security policies and analyze their risks. Companies need to have an ongoing risk analysis that is continually developed and re-developed. They need policies that are ever changing to meet new threats and new security weaknesses from a both business practices and technology viewpoints. Looking at the incidents that happened at ChoicePoint, LexisNexis, and Citigroup, 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. This showed in their inability to properly evaluate the risk 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. There is an age old saying that is a wise person learns from their mistakes, but an even wiser person learns from the mistakes of others. Citigroup needed this advice. With Citigroup's loss of their backup tapes, they should have learned from the mistake that Time Warner made just months earlier, but they did not. Security policies and practices need the flexibility to change, and management has a responsibility to make these changes when new threats or new weakness surface so that they can protect their data.

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 Egghead.com, they did have security systems in place to protect their data from being stolen, "but it lacked the kind of coordinated organizational response necessary to convince customers and shareholders that their sensitive data were actually secure." Egghead.com lost 25% of its stock value when their customer data was stolen [7]. Egghead.com was not ready for the media storm that followed the security breach which ultimately caused their collapse. By making information security a business issue, as well as a technological one, companies can add strategic, operational, and organizational defenses to protect their data.

4. CONCULSIONS:

As more identity thefts occur, companies that make their money from storing this information are going to become liable. " 'The ChoicePoint scandal has been a wake up call for how vulnerable consumers are to identity theft because of the lack of security standards for the largely unregulated information broker industry,' said Gail Hillebrand, Senior Attorney for Consumers Union's West Coast Office. 'This bill will ensure that information brokers are held accountable for enforcing tough 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' [3].

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 some sort of reputation? Companies own and manage consumer 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 regulator standards that may force companies to give this reputation to individuals who have their identity stolen.

Today, there are only laws to protect data in certain industries. This includes the Health Insurance Portability and Accountability Act for healthcare and the Gramm-Leach-Bliley Act for financial services. With consumer groups voicing their opinions regarding the theft of information from companies, the US Congress and other state legislators are getting prepared to pass broader data privacy protection to protect consumers [11].

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. This is achieved by companies having the organizational structure that allows management to fully understand the business processes and technology that expose their information systems to threats. Also, companies need the ability to change and adapt to new threats that oppose their information. It is not possible to prevent all security breaches that lead to a theft of information, but companies will need to have policies and practices in place to better protect the

data. Companies will need not only to weigh technology risk to their information, but also understand 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] Charny, Ben and Lemos, Robert. December 22, 2000. Egghead Scrambles to Guage Damage. Retrieved 06/19/2005 from http://seclists.org/lists/isn/2000/Dec/0134.html

[2] Crawford, Michael. June 16, 2005. Criminals Grasp the Metrics of Information Value. Retrieved 06/20/2005 from http://www.computerworld.com.au/index.php?id=550545875&eid=-255

[3] ConsumersUnion.org. Consumers Union applauds Nelson (FL) bill to extend federal oversight to information brokers like ChoicePoint. Retrieved 06/28/2005 from http://www.consumersunion.org/pub/core_financial_services/002027.html

[4] Easen, Nick. April 21, 2004. Cyber Crime is Right Under Your Nose. Retrieved 06/25/2005 from http://www.cnn.com/2004/BUSINESS/04/20/go.cyber.security/index.html

[5] Gross, Grant. February 23, 2005. ChoicePoint's Error Sparks Talk of ID Theft Law. Retrieved 06/22/2005 from http://pcworld.com/news/article/0,aid,119790,00.asp

[6] Liu, Bob. December 3, 2001. Eggheacd.com Becomes Amazon.com Property. Retrieved 06/22/2005 from http://www.internetnews.com/ec-news/article.php/932871

[7] McKinsey & Company, Inc. June 6, 2002. Managing Information Security. Retrieved 06/22/2005 from http://news.com.com/2009-1017-933185.html

[8] McMillian, Robert. June 7, 2005. Citigroup to Encrypt Data Sent to Credit Bureaus. Retrieved 06/20/2005 from http://www.computerworld.com/hardwaretopics/hardware/story/0,10801,102315,00.html

[9] Mearian, Lucas. May 2, 2005. Time Warner Says Data of 600,000 Workers Lost. Retrieved 06/21/2005 from http://www.computerworld.com/databasetopics/data/story/0,10801,101500,00.html

[10] Mimoso, Michael. April 2005. Damage Control. Retrieved 06/21/2005 from http://informationsecurity.techtarget.com/magItem/1,291266,sid42_gci1073914,00.html

[11] Rasmussen, Michael. March 3, 2005. ChoicePoint Security Breach Will Lead to Increased Regulation. Retrieved 06/25/2005 from http://www.csoonline.com/analyst/report3416.html

[12] Robert, Paul. March 9, 2005. Hackers Grab LexisNexis Info on 32,000 People. Retrieved 06/24/2005 from http://www.pcworld.com/resource/article/0,aid,119953,pg,1,RSS,RSS,00.asp

[13] Weiss, Todd. May 20, 2005. Scope of Bank Data Theft Grows to 676,000 Customers. Retrieved 06/24/2005 from http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101903,00.html