Managing the Theft and Sabotage of Information: An Organizational Case Study on Information Security Breaches and Rick Analysis

Julius Olusegun Oyelami
University Technology Malaysia
Faculty of Computing
Skudai, Johor Bahru 81310
Jooyelami2@live.utm.my
juliusoyelami@gmail.com

ABSTRACT

This paper revealed the importance and essentiality management role could plays in the protection of information and planning to resolve information security breach when sabotage or theft of information occurred. Recently, thefts and sabotage of information that have hit major and minor companies and those that where envisage by many organizations have caused loses and concern respectively. Most of these thefts and sabotage were caused by companies' porous management and inability to determine risks that where associated with the protection of their valuable data and lack of planning to properly manage and address security breaches when it occurs. It is becoming paramount, if not mandatory, for organizations to embark and perform a continual risk analysis to protect their systems and data. Organizations need to realize the theft and sabotage of information is a management issue and responsibility as well as a technology but not technology alone. The recent security breaches and sabotage were mainly caused by business decisions and management which is focus on the people, not technology. The approach in this paper is not to reveal the identity of the organizations while identifying common information security breaches confronting them. It is to analyze the theft and sabotage that could have been mitigated or avoided if they learn from the past.

***Keywords*: Information Security, Management, Risk and Threat Analysis, Information Security Evaluation

I. INTRODUCTION

After 9-11 terrorist attack on the twin business building in the United State (US), counter-terrorism and counter-intelligence became the major activities of US and many other countries in Africa, Asia and Europe, as a result of this, cyber-crime became the third highest priority (if not the first) for the most country [1]. With the rise in sabotage and the theft of information which has attracted and lured many crime organization and individual into cyber-crime for big profits for stolen information, it is paramount and mandatory for information systems to have the ability and capacity to protect their valuable asset. It also estimated around 2005 that a credit card number which is not supported by any other documentation worth an amount of $100 or more, and a credit history reported retails for $90 or more [2].

Previous and recent breaches in information systems that have led to thefts and sabotage of information have shown or revealed that inadequacy in management practices contributed almost 95% of the issue and not technology alone, while technology is the primary cause of the theft of the information in other cases. With each of these thefts or sabotage, there is a third party committing a crime which is considered as an associate , but in each case, risk analysis could have been used to avoid or to help mitigate the theft. It has become a necessity that private and government organizations should examine their business practices and company information security policies to avoid risks associated with information stealing and sabotage. The solution to information stealing or sabotage 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 companies from different continents, America, Africa, Asia and Europe in order to explain and analyzed the short-coming in management practices that have led to the theft and sabotage of information.

A. Aims and Objectives

The aims and objective of this paper is:

1. To identify common forms of information security breaches
2. To promote information rick analysis and evaluation among IT workers
3. To create awareness of information security for valuable data and assets.

II. CASE STUDIES

A Case I: Agro-Allied Bank

In May of 2013, one of the Agro-Allied Bank (AAB), that was noted as one of the Public Liability Company (PLC) that given loans to agriculturist, it said to have lost computer tapes considered to be the hardware of their data that were being sent to the Credit Bureau Department of Central Bank of Nigeria (CBN) via one of the prominent and famous currier service in the country. It is said that the data included names, address, phone numbers, social security numbers and payment history information and data for almost 2.8 million farmers across the nation considered to be the bank customers in agriculture, aquatic and horticultural projects. After this catastrophic event, this Nigerian based company decided that it will start sending its information and valuable data to the Credit Bureau Department of the Central Bank of Nigeria by electronic means using encryption and other secure method. This Agro-Allied Bank (AAB) should have learned its lesson from the outset from similar incidents that happen to one of the mobile telecommunication company (MTC) in Nigeria, the largest nation communication provider that has its headquarters in one of the Africa country who lost a shipment of backup tapes and hard disc that contained personal information of 10,000 employees, numerous figures of credit call cards and new generated mobile phone lines numbers that was being sent to an offshore data storage company in March 2011. But the question remains, why was AAB sent sensitive information unsecured? Why did they not encrypt the data in the first place, and why did they not realized that these tapes could get lost or stolen as evident to what happened with MTC? The answer is because they did not correctly or failed to identify the risk factors. AAB strongly believed that, this famous currier was a secure method for sending this information and that the data would be difficult to retrieve off from the tapes because hardware is needed to read the computer tapes. AAB needed to analyzed and evaluate the risk of data properly in protecting confidential information while in process for transit. Now, AAB has the issue of dealing with the negative public opinion associated with the ugly event as the organization is a public liability company, and the loss of any potential customers/revenue it lose because of it. This issue or situation would have been prevented or avoided if AAB would have properly identified this risk and taken the steps to protect this data and information and probably have a backup system. If the computer tapes were lost to an unauthorized individual or crime organization and the data has been encrypted in the first place, then this story would have never happened.

B Case II: Performance Evaluation Bureau

One of the Performance Evaluation Bureau (PEB) which was noted as a private organization in West Africa, its affiliate its operation with several police department, health department and other organization as inland revenue, university, colleges and banks to assist in crime investigation, loans and education check on their employees, this organization has made more than 3,000 acquisitions since 2009 to 2013 to make it one of the largest collections of personal data in West Africa. PEB release data to clients for background checking on jobs, loan applicants and criminal investigations procedures alongside with the law enforcement agencies. On October 16, 2012, PEB went into announcement to the general public to announced a devastating situation to almost 500,000 people that identity theft have hit their organization and the perpetrator may have gained access to their personal information including their personal data or information, client information social security numbers and credit reports. “Police authorities reports believe it was the work of a crime organizations or group of people who used stolen identity from legitimate business people to setup phony businesses that contradicted with PEB for identity checks, With PEB security incident, there was no indication of firewall hacked, or an identity Impersonation . The security breaches or incident was a deceptive scheme that took advantage of security loop-holes in the business process. The chief information security officer of PEB [3] stated that, “the incident has been misunderstood by their client as hacking and that alone is dragging PEB organization towards its killing point. With such a negative impression by their client that suggested PEB failed to provide efficient and adequate protection". As the management of PEB trying to prove that the incident was a fraud perpetrated by an insider and not harking from outsider seems the organization admitted that, they were victims of fraud, and not at fault. The bottom line is confidential information and data has been stolen, and the individuals who had their information stolen do not care if it was from external hackers or if the company was a victim of fraud from an insider. The truth is, PEB has failed to identify loop-holes in the business process to allow this event to occur. The question now is, what if someone hacked into their system, it would have led to the same result of theft of information and data. PEB organization needs to recognize and identifying risks alongside or in alignment with their business process, is just as essential as securing their information system from an external hacker.

C Case III: YHLI Organization

YHLI was a company that opened in 1984 is one of the leading manufacturing companies with around 2,500 employees in the formal capital of Malaysia (Kuala Lumpur) with over 500 employees in Saber and Sarawak [4]. It is said that, the company has more than 5 locations around Malaysia. As one of the leading manufacturing company in the south-east of Asia, the organization manufactures chemicals such as the industrial chemicals, food chemicals and agro-allied chemical, paints etc. and serves a wide range of industries, such as food chemical, pharmaceutical, biotechnology and many more. In our preliminary findings, the organization shared data that entails personal data that involve medical record with external party such as the Health Department that provides medical services to the organization Oyelami and Ithnin, (2013a) , Insurance firm that insured the legal property and its employees, banks (financial institution) that relate to the employees loans etc and with the stakeholders. The enrichment in terms of multi-cultural and diverse ethics group and to serve as the specific in-depth case study for the investigation on how human factors could influence the management of information security and what factors to be consider when planning and implementing information security for data exchange across the organization. From documents analysis, it was revealed that in December of 2000, YHLI stated that "an hacker has breached its computer system and may have gained access to its customer database". The analysis of the data collected indicate that, there was "no solid evidence" to support or proved that the database with the credit card numbers for its customer has been stolen and also could not give confirmation account that, they were not stolen. The inability on behalf of YHLI management to determine how many of its customers credit cards might have been compromised may indicate that, the company does not have a real-time auditing system in place, It also indicate that YHLI could not specifically declare how many credit-card numbers they have lost. The overall picture revealed that, YHLI security incident was not properly handled and that they did not have a good plan to manage the theft of information, and it also appeared as if they made the plan to handle this situation as it happened. This lack of adequate planning and risk analysis by the management caused the organization business to suffer tremendously. Shortly thereafter this event, YHLI almost went into bankruptcy as at November, 2001, It appears the inability for the organization to successful determine with certainty the extent of information that where stolen caused more damage to the company's reputation than the actual incident itself. If YHLI had a well-developed incident response planning (IRP) in place to handle this security breach and a mature way to handle the media that followed the incident, the organization might have been able to weather the storm and stay focus despite the incident. It was recorded that, customer confidence was lost and YHLI was not able to recover as at 2001 until when the IT department restructured there ERP and IT security policies.

D Case IV: Western Corporation

An ex-employee in AMB, a private western corporation in Montréal, Canada allegedly sabotages enormous data of customers. This private organization working as subsidiary with PNC Bank alleged to have stolen information and data on 676,000 customer accounts that are all Montréal residents in Canada. It was further established and considered as one of the largest information and data security breach in history by the department of the treasury [5] according to him, he stated that "The suspects pulled up the huge account information and data while still working with the firm , then printed out all the screen captures of the information and data and wrote it out by hand" [6] who later added that " the data and information that where stolen was then provided to another company called APP Associates Inc., which had been setup as a front-line for the illegal operation". This APP organization advertised itself as a data locator service in Canada and as a collection agency, but the APP organization was not duly and properly licensed and authorized to perform or carry out such activities by the department of treasury. With this kind of scenario in information and security breach, there was no indication that technology involved, no hackers breached on the information system. This was completely a dubious job from an inside. The question becomes of how this could have been prevented? The answer is that in some cases the theft or sabotage of information cannot be prevented sometimes but the only action the management could do, is to prepare for it when it does happen. Because due to information and data incidents like this, it is becoming a duty and responsibility of management to log out the access or password of every ex-staff and official, retrieve their staff identity card and to have adequate incident response plan (IRP) in place. Initially before information and data security breach occurred. From the risk analysis point of view, an information incident of this nature is difficult to detect and almost impossible to stop before it happens. But when it does occur and the criminals or perpetrator are caught, it becomes a necessity to punish the ones responsible to the full extent of the law to serve as a deterrent to others not to follow or put on same or similar criminal suit.

E Case V: European Stock Exchange

One of the stock exchanges (SE) provider in Europe whose primary function is to provide financial and business data for organizations or individual intend to buy shared and dividend in any other organization declared on March of 2012, that the information on 42,000 people had been stolen. These information security breaches occurred at one of the subsidiary companies, XYZ Inc. This company provides data and information to the multistate organization and industries in conjunction with European Stock Exchange (ESE). The European stock exchange, which acquired XYZ, lost several million due to the incident [7]. The organization expressed regret over the incident and they notifying the individuals whose information may have been accessed and the organization promised will provide them with credit-monitoring services. From the view point of risk analysis, in this incident, hackers stole username and passwords of legitimate users to access the confidential information and data. The ESE organization noted that, the company will improve on the user identity and password administration procedures that its customers use and will devote more time and resources to protect user's privacy and reinforcing the essential of privacy. This information security breached is very similar to the incident that happened at YHLI organization and Wachovia incorporation. There are several information security policies that should have been implemented that could have reduced the risk of this information security breach. Since European stock exchange gives third parties access to its confidential information and data, there is a need to educate these organizations on certain information practices to protect information and valuable data. In this regard, information security awareness and training (ISAT) is paramount to all information users. The question now is, where was this education, and was there a lack of information security education due to the possible effect that it could have on business? Also, what was the password policy for its customers? From analysis, the organization has not elaborated on the details of the information security breach, but considering the statement of the CEO of European stock exchange after the incident, it indicate clearly that there was a failure to detect the risk associated with their customer’s password policy that could result in a theft of information. ESE inability to properly assess this risk caused the information security breach. Through security education and ISAT [8] and a secure password administration policy, this event could have been avoided.

III. RESULTS AND DISCUSSION

When analyzing these case studies, an important thing to ponder is the fact that, for every security information and data breaches reported, how many where resolved after the report and how many unsolved? These information security breaches could have been avoided or averted with proper and adequate risk assessment and risk analysis, or at least the probability of information security breach could have been reduced or minimized greatly. For all information security breaches, the prevention or at least the reduction of the probability of the information security breach begins and ends with decisions that management makes. In an organization, when information or data security breach occurs it causes a company to re-evaluate their information security policies that guide their information security and management. With this rash of numerous information and data security incidents that have recently taken place, organization do not need to wait until an information security or data breaches happens they should evaluate or re-evaluate their information security policies and analyze their risks. Companies need to have an ongoing and consistent risk analysis that is continually and consistently developed and re-developed. They need agile and iterative information security policies that are ever changing to meet new or current threats, challenges and new security weaknesses from both business practices and information technology viewpoints. Observing the information and data incidents that happened at agro-allied bank, performance evaluation bureau (PEB), YHIL, AMB Corporation and the European stock exchange (ESE), these companies have technological solutions to protect their data from being stolen or sabotage, but the problem is they failed at weighing equal importance to the information security of the data from a business issue and perspective. This showed or revealed that, there is inability to properly evaluate the risk in the business practices and processes. In several cases, the theft and sabotage of information occurred because of the business practices and management of the company is porous, inadequate and technology was not even involved. Also, companies need to learn from the mistakes of others because history will or may repeat itself if proper lesson or knowledge is not learned. There is an old adage saying that is a wise person learns from their mistakes, but an even wiser person learns from the mistakes of others. Agro-allied bank needed this advice. With Agro-allied bank lost of backup tapes, they should have learned from the mistake that MTC made just years earlier, but they did not. Information security policies and practices need the flexibility to change, and management has a responsibility to make these changes when new threats, challenges or new weakness immerge so that, they could protect their data adequately. Companies, both private and government organizations need to realize the importance and essentials of making information security a business issue as well as a technological one. With the issue that happened with YHLI, they did have security systems in place to protect their information and valuable 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.” YHLI lost 20% of its stock value when their customer data was stolen and they were not ready for the media storm that followed the information security breach which ultimately caused their collapse. By making information security a business issue, as well as a technological one, companies or organization can add operational, organizational and strategic defenses to protect their information and data.

IV. CONCULSIONS

As more identity thefts occur, companies or organization that makes their money or income from storing this information are going to become liable or responsible for their actions. The YHLI organization scandal has been a wakeup call for how vulnerable consumers and stakeholders are to identity theft due to lack of information security standards for the largely unregulated information. There should be a bill that will ensure that information brokers are held accountable for enforcing tough security practices to prevent unauthorized person from gaining access to sensitive customer, consumer, personal and operational data. And this bill will give consumers and customers the rights to examine the information maintained about them and to correct any errors they may find within it.

Companies neither private nor government, need to find out the importance of protecting their information and valuable data from both technology and business practice weaknesses. Companies view the protection of their data from a technology issue, but fail to realize the importance that management plays essential roles in protecting their systems with the creation of information policies and understanding the risks that confront or may confront their information systems. From a consumer and customer standpoint, if a company is making or makes profit from someone’s personal information and data, and they failed to protect those data, should they not be given some sort of reputation? Companies who own and manage consumer information, and individuals have little or no power over their information that is controlled by these organizations. As identity theft continues to rise daily and companies failed at protecting those data, proper legislation should be passed and implemented that will force companies to comply with regulatory standards that may force companies to give this reputation to individuals who have their identity stolen or misused.

Today, there are only laws to protect data in certain industries. This includes the Health Insurance Portability and Accountability [9] for healthcare and the Gramm-Leach-Bliley [10] for financial services and data protection [11], which deals with information and data sharing. With consumer groups and union voicing out their opinions regarding the theft of information from companies and organizations, the US Congress and other state legislators are getting prepared to pass broader data privacy protection to protect consumers.

V. RECOMMENDATIONS

There are steps that companies and organizations need to take to protect themselves from the theft of information. First, companies need to be fully prepared when a security breach occurs because a risk to an asset can never be a zero percent. Secondly, organizations need to establish adequate information policies and risk assessments that will protect their data from both technology risks and business practices well before a security breach occurs. This can be achieved by (1) Companies should have the organizational structure that will enable and allows management to fully understand the business processes and technology that is liable to expose their information systems to threats and information breaches and sabotage. (2) Companies must develop the ability to change and adapt to new threats that may oppose their information and data both within and it transit. It is impossible sometimes to prevent all security breaches that may lead to a theft of information and data, but companies should ensure to have adequate policies and practices in place to better protect their data. Companies will also need not weighing technology risk only to their information and data, but also to understand business and management issues to that associated to it. The gravity of information stolen is no longer relevant, whether it was a external hacker or an insider that committed the crime; companies need to protect their information from all threats and minimize their risks from all aspects and ramifications.

REFERENCES

[1] N. Easen, “Cyber-crime is right under your nose”. (2004), pg12

[2] M. Crawford “Criminals grasps the metrics of information” (2005) value. Retrieved 20/06/2005

[3] A. Desmond, “West Africa security reports”, (2012). pg 5-8

[4] J.O. Oyelami and, N. Ithini, (2013a). “Enhancing the Conventional Information Security Management Maturity Model (ISM^3) in Resolving Human Factors in Organization Information Sharing”.(2013).International Journal of Computer Science and Information security 11(8):1-8

[5] D. Weiss, “Scope of Bank Data Theft Grows to 676,000 Customers” (2009).pg.10-12.

[6] J. Peterson., “The Insider threat. Bulleting on data security and theft” (2010) Pg. 4-5

[7] A. white, “European stock exchange news bulletin” (2012) vol. 11, pg 4.

[8] J.O Oyelami and N.Ithinh, (2013b) “People Are the Answer to Security”: Establishing Successful Information Security Awareness Training (ISAT) Program in Organization. International” Journal of Computer Science and Information security 11(8):1-8

[9]United State Congress. Health insurance portability and accountability act of 1996 (HIPAA).

[10] Gramm-Leach-Bliley Act of (1999) for financial services.

[11] Data Protection Act (1998). Part VI (Miscellaneous and General), Section 55, Office of Public Sector Information, accessed 14 September 2007 Directorate Access to Information and Privacy, (2009).

AUTHORS PROFILE

Oyelami Julius Olusegun Is Currently is a postgraduate research student at the department of information system, faculty of computing, University Technology Malaysia (UTM), and a member of information assurance and security research group (IASRG-UTM), His research interest are in information security management, social networking, information systems, Information sharing and knowledge management System. He is a member, Association for Computing Machinery (ACM) Association for Information Systems (AIS), British Computer Society (BCS) of the Chartered and the Institute of Information Technology Professional New Zealand. He has recently extended his research interest into security in cloud computing.