International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 3, April 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

An Insider Threat Model for Prevention of Insider Cyber Crimes in the Organization

Dr. Jigar Patel[1], Dr. Ashok Patel[2]

[1] *Kalol Institute of Management(MCA), Kalol, drjigarvpatel@gmail.com*
[2]*Department of Computer Science,H.N.G. University, Patan, hod_computers@ngu.ac.in*

Abstract— Sometimes the threat of insiders is more serious than the outside criminals because of insider are using organization resources with higher privileges. Inside employee of the organization has sole duty to use the organization data in secure way, but when they start to commit the crimes, it's resulted into huge financial losses to the organization. The organization has to create strong information infrastructure to avoid threats of insiders. This paper is describing the model for how one can reduce the insider threats by security, policies, detection, prosecution and punishment. Paper also discusses few case studies of such insider attack because it is helpful to enhance our security policies to avoid the insider attack in future. The Cyber laws and punishment of inside criminals is also important and not only that the amendment of Cyber laws is most needed exercise for the governments and law makers as technology and nature of Cyber crime changes time by time.

Keywords-Cyber Crime, Cyber Laws, Digital Forensic, Insiders Threat Model

I. INTRODUCTION

To get the sensitive data from the organization is easy by the inside user of the organization due to such users entertaining all the access rights they need [1]. Insider is becoming largest risks nowadays for the critical data and ease of committing crime due to privileges given to them. The position of the insider in the organization is important in the Cyber crime. The dimention of crime committed by managers is higher because managers may have more access rights and it may be easier for them to hide their crimes. While the other employees can perform less Cyber crimes because they don't have the much control over or access to the organization assets, consequently the companies' loss will be less. An alliance between a manager and an employee in committing a crime may be even difficult for detection and stop because their working on different levels of hierarchy may allow them more options to hide or disguise the crime [2].

The insider Cyber criminals can be divided in many categories like espionage, sabotage, theft and personal abuse of the organizational network. A spy is such type of criminals who keeps the watch on the organization activity and confidential information like research and plan [3]. After that this kind of employee can give sensitive data to competitors that may result into big direct or indirect loss to the organization. If insider criminal is in the higher position in the organization than mostly risk is doubled to the organization. Second category of the crime is sabotage, in this saboteur is type of employee who is working in the company but not fully satisfied. Generally people are starting this kind of activity once they missed the promotion or higher salary package or sometimes insider is about to dismiss from the organization.

There are a lots of similarities between espionage and the sabotage. But these two crimes are also different in some sense. They both can be done by a competitor, but the saboteurs are not necessarily employed by the organization. They could act from a distance. The saboteur and the spy should possess a sound knowledge in the IT area so that they would be able to commit the Cyber crime and hide their steps. Both saboteur and spy are secret persons, trying not to be seen. But the saboteur can act to harm the organization with personal motives like revenge for a lay off, or a missed promotion. A saboteur could be a person recently laid off, or an employee who feels neglected by the organization in some way. Saboteurs are probably between 25 years and 40 if employed by the company, so they have enough experience within the organization to learn the weaknesses and to feel offended if not offered a promotion or bonus. If employed by a competitor then their age could vary significantly. According to survey, among 523 respondents, 51% of those who experienced a security incident also experienced an insider attack. The problem with approximating a total number of insider attacks is that, by experience, a large number of these attacks go unreported. In fact, according to the survey, the public may not be aware of the number of incidents because almost three-quarters (72%), on average, of the insider incidents are handled internally without legal action or the involvement of law enforcement[4].

This paper mainly focuses on the types of security risks from such insider and kinds of activity they can do with some statistics of insider crime cases. In second part of the paper the model namely Insider Threat Model is explained which shows what is mean by insider and what kind of security precautions organization can forced to avoid insider crime and even such crime happened then how one can detect the crime and collects the digital evidence against the insiders. In the later part of the paper it is explained how organization can prosecute such kind of cases and what kind of punishment provisions are available in the laws. In the last part of the paper it is discussed how such cases are important to improve the policies and procedure of the organization and also for the improvement of the laws prevailing in the country.

II. BACKGROUND

In a Global State of Information Security Study, employees within the studied organization were considered as a major source of information security breaches. The data show that in 2006 the rate of insider attack was 3 per cent. This rose to 48 per cent in 2007[5]. The trends continue up to 2011 and in the recent survey done by UK's Frauds Prevention Service namely CIFAS[16] of 2012 and 2013, As shown in the table 1 there was an 18% rise in the total number of staff frauds recorded in 2013 when compared with 2012.

Fraud Type	*2012*	*2013*	*% Change*
Account Fraud	***55***	***46***	***-16.4%***
Dishonest action by staff to obtain a benefit by theft or deception	***268***	***254***	***-5.2%***
Employment application fraud (successful)	***34***	***31***	***-8.8%***
Employment application fraud (unsuccessful)	***171***	***293***	***+71.3%***
Unlawful obtaining or disclosure of commercial data	***2***	***4***	***+100.0%***
Unlawful obtaining or disclosure of personal data	***46***	***48***	***+4.3%***

Table 1: Comparison of Insider Attacks of 2012 and 2013

Attempts to obtain employment fraudulently (e.g. by not declaring previous convictions for falsely claiming qualifications) shot up by over 70%, demonstrating that organisations are now increasingly vetting prospective employees properly. While the level of dishonest actions by staff to gain a benefit by theft or deception (e.g. theft of cash from customer accounts) decreased, these frauds still account for 40% of all confirmed insider frauds. Frauds where an organisation's staff stole customer or commercial data continued to rise.

Thomson (2008) interviewed 3596 information technology professionals from the United States, United Kingdom, France and Germany, and found that in 75 per cent of cases, breaches within companies were caused by inside staff [6]. According to Cappelli et al. (2006), the financial loss incurred by insider attack ranges from a few hundred dollars to millions of dollars [7]. A former employee of Cox Cable has been sentenced in the United States for intentionally damaging telecommunications and the company's network. The employee remotely shut down portions of the company's system, resulting in the loss of internet and telephone services, including 911 emergency accesses [8]. Chi Mak admitted that he was sent to the United States in 1978 by China to obtain employment in the defense industry with the goal of stealing U.S. defense secrets, which he did for over 20 years. He passed information on quiet electric propulsion systems for U.S. submarines, and information on stealth ships being developed by the Navy. The Chinese government also tasked Mak to acquire information on other technologies. He recruited family members to encrypt and covertly courier information back to China. In May 2007, Mak was convicted of conspiracy, failing to register as an agent of a foreign government, and other violations. He was later sentenced to over 24 years in prison. Michael Mitchell became disgruntled and was fired from his job due to poor performance. He kept numerous computer files with his employer's trade secrets, then entered into a consulting agreement with a rival Korean company and gave them the stolen trade secrets. In March 2010, he was sentenced to 18 months in prison and was ordered to pay his former employer over $187,000 [9].

III. INSIDER THREAT MODEL

Here in Insider Threat Model it is explained the overall procedure about the insider attacks by misusing the organization resources as well as the protection against such attacks taken by the organization as shown in figure 1. Even the insider crimes happened then we have to collect the evidence against the criminals which must be trusted by the court of laws and criminals are prosecuted and punished under the various Cyber laws. Each steps are explained as below.

3.1 Insider

Here term Insider means the employee working inside the company or organization and using its resources like computers and its networks. Insider is general term which can use for employee in the organization at any level ranging from apprentice or trainee to CEO level or any person work in the top level management.

3.2 Security

Security means all the rules must be applied for the Information and Network security when insiders are using the computer and its network. Firewalls and Intrusion Detection Systems are used for merely securing the outsider attack therefore, to restrict insider threats we need to enforce specific type of security infrastructure to protect the organizations sensitive information. Here we required to enforce general security rules like all the computers have proper password protection as well as all the data pass through network must be in encrypted form when it is sensitive and confidential.

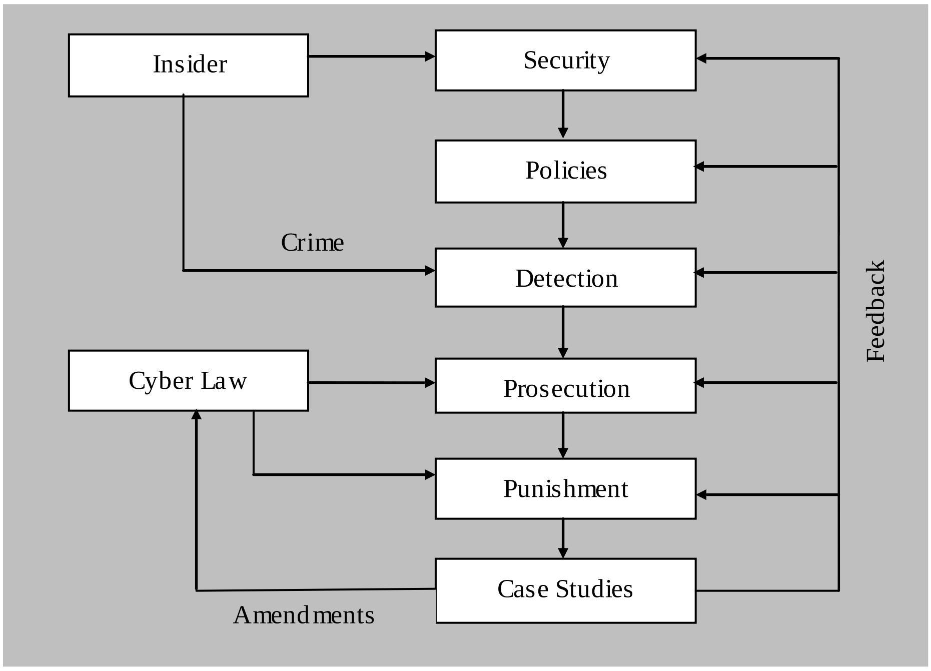

Figure 1. Insider Threat Model

3.3 Policies

It is very important to make the policies related to all resource and information access by the insiders. We can make the Email and Internet use policies according to the employee requirement. A review of this practice shows that adoption of acceptable Internet use policies alone to combat unproductive use of the computer is ineffective [10]. For that we can block certain sites inside the organization premises using filters as well as we should monitor employees which may be very expensive[11] Internet use and any case of violation of policies employee can be punished according to the rules and regulations. In addition of that organization has to draft the policies for what kind of other electronics media is allowed in the premises like mobile phones, pen drive, CD or DVD etc. because such things might be use for secrete data theft which is resulted into huge direct or indirect losses to the organization.

3.4 Detection

The crime in the computer field is in digital form unlike the conventional crime like murder, theft etc. where you can have some physical evidences available to prove the crime. Therefore, detection of such digital crime is very important stage in the entire process. For detection and collection of evidence against insiders we have to use the all the processes of digital forensic.

3.5 Prosecution

Here prosecution means any insider detected in such criminal activity in the organization will be heard for any reason behind such activity by higher authority. Organization can make the jury to handle such insider abuse which contains the member from all departments which have a knowledge and understanding of such crimes committed by the insiders. Here in the prosecution jury can analyze the evidence collected by digital forensics against the suspected insider and the declarations and arguments given by them. If the case is bigger and insider is leaving the job meanwhile the case may be prosecuted in the court of laws. Here in the court case prosecution is happened in the conventional way by using the Cyber and other related laws prevailing in the country.

3.6 Punishment

After the detection and prosecution it is also important to punish such employees according to damage made by them to the organization. Earlier incidence happened in the various organizations about the misuse of the company resources at work. Edward Jones, one of the leading brokerage firms fired 19 employees for such misuse of the Internet and worn more than 40 employees for sending jokes and other messages not related to business by Email [12]. In other case Xerox terminated 40 workers for misusing Internet in working time for surfing pornographic and shopping sites on the Internet [13]. Dow Chemical fired 50 employees and suspended another 200 without pay after an Email investigation uncovered hard-core pornography and violent subject matter [14]. Merck dismissed multiple contractors for inappropriate Internet use [15].

3.7 Case studies

In this Insider Threat Model it is crucial to review and analyze different cases happened around the globe because due to that all organizations can learn the lesson and changing their policies when it is require. Other important benefit of study of such cases is different countries around the globe can draft some amendments in their laws to prevent such kind of cases in the future. Therefore, the feedback get by such cases will helpful to improve all stages of the Insider Threat Models like punishment and prosecution enhancement as well as changes of detection and security methods from such cases happened in the Cyber world.

IV. CONCLUSION

Generally, insider crime promulgate by either over ambiguous or unsatisfied employees in the organizations. Ultimately they are breaking the trust that the organization has put on them and misusing the information and resources. An Insider Threat Model can helpful to understand the overall process of insider crime and not only that it is also useful to combating such insider threats by understanding and implementing each stages of this model. To decrease such kind of insider abuse organization has to improve its policies as well as the security and monitoring system on the employees.

REFERENCES

[1] Marc Lee, Cyber crimes: preparing to fight insider threats, Computer Fraud & Security, June 2012,pp 14-15.

[2] Nick Nykodym, Robert Taylor, Julia Vilela, Criminal profiling and insider cyber crime, Computer Law & Security Report (2005) 21, pp. 408-414.

[3] Barnes & Nobles Books. New Universal Unabridged Dictionary, 1996;

[4] Permalink, Interesting Insider Threat Statistics, http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=60, Jan-2014.

[5] Price Waterhouse Coopers. Global state of information security study., http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/pwc-gisswp-112007.pdf, 2007.

[6] Thomson, I., Insiders, not hackers responsible for corporate data loss, IT News, 10 October, 2008.

[7] Cappelli DM, Moore AP, Shimeall TJ, Trzeciak. Common sense guide to prevention and detection of insider threats, version 2. 1, technical report. Carnegie Mellon University/CyLab and the Internet Security Alliance, http://www.cylab.cmu.edu /education/faculty/cappelli.html, January 2012.

[8] Haugsted L., Former cox employee gets jail time for computer hacking. Multichannelnews, http://www.multichannel.com/article/CA6522132.html, November 2008.

[9] The Insider Threat: Two Cases, http://www.fbi.gov/news/stories/2012/november/ teaching- industry-how-to-protect-trade-secrets-and-national-security/the-insider-threat-two-cases.

[10] Johnson, J. J., & Ugray, Z. Employee Internet abuse: Policy versus reality. Issues in Information Systems, 8(2), 214–219, 2007.

[11] Mirchandani, D., & Motwani, J. Reducing Internet abuse in the workplace, SAM Advanced Management Journal, 683, 4–48, 2003.

[12] Newsbytes, Edward Jones fires 19 workers for Email abuse. Newsbytes, May 7, 1999. Available from: http://www.exn.ca/Stories/1999/05/07/04.asp, Accessed January 2009.

[13] Adschiew, B. A web workers. NBC Nightly News, June , 2000.

[14] Collins, L. A.. A dow chemical fires 50 over e-mail. Associated Press. Available from: http://news.excite.com/news/ap/000727/18/dow-chemical-e-mail. Accessed on January 2009.

[15] DiSabatino, J. A. , E-mail probe triggers firings. Computerworld, 34(28), 1–2., 2000.

[16] CIFAS Report, Rise in insider frauds leaves organisations vulnerable warns CIFAS, Available on http://www.cifas.org.uk/insiderfraudtrends_janfourteen, March, 2014.