Integrating a Systems Approach to Detect Risk of Insider Trading

Rajni Goel
Howard University
School of Business
2600 6th St. NW, Room 438, Washington, DC 20059, USA.

Abstract

Corporations have repeated reported incidents of misuse of material non-public information for illegal insider trading. Though information technologies are being inappropriately used to assist in these activities, creatively using emerging technologies and business process can also aid in preventing and detecting insider trading. This paper first discusses the issues relating to insider trading in the business environment. Next, policy and preventive measures are discussed, along with a novel model which defines a notion of Insider Information Risk value, and presents a framework for using the Systems Development Life Cycle (SDLC) approach to monitor and deter misuse of private corporate knowledge.

Keywords: Insider Trading, Technology Risk, Monitoring, Systems Development Life Cycle

1. Introduction

Within the walls of corporate America, particularly the financial sector, there is a significant amount of non-public information that is exchanged on a daily basis. For the past few decades, regulatory bodies have tried to ensure that employees at these corporations do not use this non-public information for the purposes of insider trading. Due to the difficulty in proving insider trading, greater emphasis needs to be placed on prevention. While the Securities and Exchange Commission (SEC) and the New York Stock Exchange (NYSE) have tools in place that seek to identify potential insider trading, there needs to be greater collaboration with the actual companies that are regulated. Corporations can definitely do more on their part to dissuade employees from practicing insider trading.

Technically, the term “Insider Trading” refers to officers and high level employees of an organization legally trading the stocks of their company. These trades are reported to the SEC and are open for the public viewing. However, it is common practice today to use “Insider Trading” when referring to illegal insider trading by individuals who have access to material non-public information. Some may argue that insider trading is of little threat to any particular corporation because it is actually insiders who are committing the crime and not the company as a whole. However, since the business environment is extremely competitive, it is hard for one firm to differentiate its product from another. Hence, the relationship with the customer is an important part of business. Being involved in insider trading cases may suggest that individuals who are representing the firm do not have the highest level of integrity and are looking out for their own interests before that of the client.

Since client revenue is at risk, financial institutions need to ensure that there are internal mechanisms in place to assist in preventing insider trading. In too many instances individuals have been using the corporate networks and technologies to communicate about insider trading. Many corporations have relaxed security systems that make it easy for material nonpublic information to travel outside the walls of the corporation.

Our research first discusses the background of insider trading and the existing tools for preventing it, and then we provide a novel approach using information systems to detect incidences of illegal insider trading. With a greater effort on the part of corporations to integrate information technology (IT) to monitor, detect and prevent misuse, and by partnering with the SEC, more assurance can be provided to the integrity of the financial markets. Furthermore, the paper break down the tasks and steps in setting up the information system for insider trading detection from a systems development life cycle approach (requirements analysis, development and design, installation, test and evaluation) as well as the need to address network configuration, routing design, network security evaluation, and policy and procedures development as well as security awareness and training.

2. Background

According to the SEC, illegal insider trading refers "*generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, nonpublic information about the security*" **(**www.sec.gov**).** The laws regarding illegal insider trading are covered by two acts. The Securities Exchange Act of 1934, commonly referred to as "34 Act" or "Exchange Act," covers illegal insider trading pertaining to transactions in the secondary market. Based on the power granted to the SEC under "34 Act," the SEC issued Rule 10b-5 which prohibits fraud or deceit when purchasing or selling securities. The second law that monitors insider trading is the Securities Exchange Act of 1933, which governs buying and selling during the initial issuing of securities.

Although insider trading has existed for decades, it really came to national prominence in the 1980's. At the time, there was a series of high profile cases that eventually caused the fall of Drexel Burnham Lambert, one of the largest investment banks in the world. In 1986, the SEC discovered 313 securities violations, of which, 34 were alleged insider trading (Kowalski, 2000**)**. One may think that the high profile prosecutions would have lowered the number of cases, but this has not been the case. In the last fiscal year, the FBI prosecuted 46 Insider Trading cases. During the earlier part of this decade the focus was on companies such as Enron and ImClone. During the emergence of the Internet and email, which coincided with general prosperity on Wall Street, violators of insider trading laws were using corporate facilities to communicate material non-public information. With stronger internal controls and collaboration with the SEC, some of these controls could have been prevented.

3. Enterprise Solutions

The first step for the corporation in creating a stronger information security system is having documented policies in place. By documenting information security requirements, employees have a source that they may reference if unsure about any of their potential actions. Such a document should also include the ramifications and penalties of any violations in the company's security policy, which would assist in discouraging insider trading.

Having a document in isolation does not provide much benefit to the organization. The corporation needs to ensure that it has provided employees with adequate training pertaining to appropriate uses of the company's non-public information. By implementing mandatory bi-annual online certification programs, corporations can ensure that their employees are knowledgeable of the laws pertaining to the company's information security. These online programs should also be complemented with annual presentation sessions from the information security group, which would include any recent updates to the company's security policy or practices. After providing employees with the necessary education and references, corporations need to employ barriers to the employee's access. These barriers will allow for easier monitoring of corporate communication and reduce the risk of sensitive information leaving the confines of the organization.

Today, majority of the content is being delivered through web-based applications (Reconnex, 2005). Corporate sector employees typically have started to utilize web-based services such as those offered by Yahoo and restrictions on the size of information that can be sent over the network and as such, employees Google. Moreover, larger corporations have banned access to web based accounts and message boards. We interviewed twenty individuals who work with large investment firms and all twenty stated their companies' implemented firewalls that prevented them from accessing web-based accounts. This practice must become a required standard throughout the corporate sector.

4. Deterrence Technology Solutions

4.1 Insider Trading Threat Identification

Although corporations have security surrounding web-based mail, security surrounding downloadable devices appears to be absent. From our corporate experience and interviews with individuals, monitoring of the information that is downloaded from corporate networks appears to be neglected. Only two of the twenty individuals interviewed responded that their corporations had technology monitoring USB devices. This is an egregious problem when considering the sensitive data that can be removed from the corporate network. This should not be the case because off-the-shelf software such as USB-Monitor is available for purchase**.** By implementing readily available software, companies can reduce their potential loss exposure from insider scandals. Another area that corporations are ignoring is instant messaging technology. In recent years corporations have been incorporating social networking tools into their organizations.

Employees are starting to substitute e-mail communication with instant messaging to achieve more dynamic written communication. Though instant messaging occurs through the corporate network, corporations are not checking instant messaging logs. Last year a Fortune 500 company discovered insider trading taking place in an AOL instant message conversation. (Reconnex, 2005)**.** Similar to the USB situation, companies must implement rigid policy mandates integrating readily available software to monitor instant messaging logs. Though these preventative measures are necessary to encourage the proper use of material non-public information, they will not be sufficient is stopping all persons from participating in illegal insider trading because the ultimate non-preventable motivation of greed. Having identified currently available preventative measures, we develop identification and monitoring system that corporations should implement to *deter* inside trading.

The first step of the insider trading threat identification process is determining the *access paths* of employees. The *access path* refers to the information availability that may accompany a particular level of clearance or approval. An access path is defined in terms of financial securities that are associated with them. By having a comprehensive list of individuals and their access paths, the corporation can ensure that it has the opportunity to accurately identify the material nonpublic information that the individual has access to. This identification system will be the backbone of the insider trading detection system. The importance of this information lies in its ability to provide collaboration between the corporation and the regulatory body.

Once employees and their access paths have been identified, the employees are defined and clustered by their "*Insider Information Risk,***"** value;this will determine the level of threat an individual poses to being involved in insider trading**.** The *Insider Information Risk* value is determined by a dual criterion; it is dependent on the combination of an employee's Area of Risk based on the person's access paths, and their level of Technical Skill based on ability to work with Information Systems and Technology. Although employers may already monitor their employees based on the access path, the tendency is to ignore the technical competence of that particular employee in determining the level of monitoring. For example, the employee's technical capacity should be based on the individual's academic background, work experience, and certifications received. The Area Risk is also important because it takes into account the amount of material nonpublic information that the person would have access to. The various weighting that would go into such a calculation will be subject to the different environments and processes that may be unique to a particular organization.

With these two factors, we created a matrix (Figure 1.**)** that would be the basis of monitoring and the collaborative effort with the Security Exchange Commission (SEC), New York Stock Exchange (NYSE) or other regulatory bodies.

Figure 1:Risk Identification Matrix

Area Risk / Tech Skill	LOW	MEDIUM	HIGH
LOW	🟩	🟩	🟩
MEDIUM	🟨	🟨	🟥
HIGH	🟥	🟥	🟥

Based on an employee's position in the matrix, the individual would be categorized as red, yellow or green. An employee in the red category would be the most risky (high *Insider Information Risk* value) and the person in green would be the least risky (low *Insider Information Risk* value). Monitoring of the employees corporate communications through e-mail and instant message would be based on their position in the risk matrix. The employees in the green zone, who are seen as low risk, would be monitored annually. Employees at the medium risk level (yellow) would be monitored quarterly, while those in the red zone would be monitored on a weekly basis. The monitoring would consist of queries that would filter the communication channel for buzz words, such as "tip", insider etc.

In addition to being monitored weekly, the names of the employees from the red risk zone should be submitted to the regulatory body for the industry. This will assist the regulatory body in their efforts to identify and investigate insider trading, at the same time helping to maintain the integrity of the corporation involved.

4.2 Market Activity Relativity

Furthermore, to identify the individual's insider trading, the measure needs to be the relative strength of the news item that resulted in a significant market movement. Hence, incorporating monitoring relative to market activity further enhances the model. The significant movement level should be measured based on the percentage change in the security price in the session after the news is made public. Those stocks that exhibited minimal movement would be ignored, while those that exhibited strong positive or negative price change would be further analyzed. The securities in which the employee has no position will be ignored, while the ones in which a balance exists will be measured. The beginning and end of the relative change is measured from the week prior to current trading price. The delta should be calculated for the person's position; this delta is the change in the person's amount of stock owned. The proportional and absolute change in the person's position may be sufficient in indicating whether or not an anomaly exists.

In addition, the *gamma* should be calculated; the *gamma* is the change in the delta, or the change in the change. This calculation is particularly useful in the case of serial traders. A high delta may not tell the full story for some traders that actively trade a position. If a particular person increases their shareholdings from zero to ten and then by increments of five thereafter, the delta may cause a false positive scenario. The initial delta would be high and so would the second and third delta. However these changes were small when compare to the initial delta. Hence, the gamma would capture the changes in the person's rate of change in a particular security.

4.3 System Development Approach

Prince (2005) discusses three layers for Internet Security for financial systems :(i) the bare minimum; (ii) detecting and preventing intrusion; and (iii) turning the tables on the phishers. Every one of these layers is vital, yet any one of these layers is unlikely to provide sufficient protection by itself. Thus, information security and trading monitoring needs must be addressed from different fronts. Focusing on the one front while ignoring other aspects of security cannot serve the purpose as weaknesses on other fronts makes it vulnerable as it is. It becomes therefore imperative that technology oriented security aspects, as the monitoring technologies discussed above, must be addressed with priority and in a detailed manner at the beginning and throughout the systems development cycle (SDLC); initiate the objective to integrate an IT monitor tool from the requirements phase of any system on which information can be exchanged.

According to Gary McGraw (as quoted by Frye, 2006), securing applications doesn't require completely changing the software development life cycle, but rather 6 "touchpoints" in SDLC for software security. This could include code review, architectural risk analysis, penetration testing, risk-based security testing, use case development, abuse case development, and security operations- covering firewalls, environment, patching, intrusion detection, and monitoring in vigilance and feedback loops. Keeping this in view, the organization lacking resources can start with these touch points in their detection of insider trading information systems initiatives.

4.3.1 Phasing monitoring security into SDLC

Injecting security into conventional SDLC has been a movement in the computer science domain, however, phasing-in security into SDLC is a newer phenomenon for developing applications, especially for monitoring insider trading needs, and yet to be addressed. The phasing security into SDLC, as Gunnar Peterson (2006) discusses, can be approached with top down, testing and validation, and start in the middle approach. Any of the approaches for a deterrence system in an insider-trading environment is acceptable (constraint by the organization's policies and budget).

The top down approach takes into account functional and non-functional requirements, the Use Cases that can be derived from the Information Security policy, and meetings with security stakeholders. Each organization would need a plan the monitoring at the policy phase. The testing and validation approach targets the tail end of the development lifecycle with trading monitoring security systems use penetration testing, white and black box approaches etc. to validate the sufficiency of the system and to meet the security goals.

The start in the middle approach focuses on code review and testing during the development phase using peer review and automated source code analysis. The use of Source Code Analysis Tool and the advantages of being involved early enough to find and fix security bugs with developer understandable language is the main attraction. However, design errors are too late to be resolved here and clear-cut security policy is mandatory. Gunnar suggests 'Training in the SDLC' as a fourth way that may be combined with any of the above.

4.3.2 Requirements / Initiation phase

This phase establishes the overall direction and priorities for business change for the enterprise; it is important at this phase to define the information security goals for insider trading and strategy for deterring insider trading from a information security perspective. During this phase, the requirements are to be expressed in terms of Security Categorization (i.e., low, moderate, or high) and also in terms of its potential impact on organizations or individuals should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability). Preliminary Risk Assessment –as an initial description of the basic security needs of the system is, therefore, important to predict the threat environment in which the system will operate.

4.3.3 Analysis & Design Phase

The monitoring systems stakeholders would establish the concept/vision, requirements, and design for a particular business area or target system. In addition to functional design, to give the user and the developer a clear assessment of the risk, threat modeling or developing abuse cases needs to be performed to include the right controls in the evolving solution for three essential considerations:

1. To know the potential abusers who can compromise the system
2. To know the techniques that might be used
3. To assess the impact

Furthermore, input data types, security use cases and security architecture are to be conceived using experience analysts by understanding the threat landscape. The software processes planned needs to be embedded with security by training people for good security practices.

4.3.4 Acquisition / Development Phase

This phase includes the acquisition, modification, construction, and testing of the components of the IT monitoring tool as a business solution. This phase also includes routine planned maintenance of monitoring applications. Programmers need to be oriented towards functionality as well as security needs with respect to security practices implemented in the requirements and design phases.

4.3.5 Implementation

This phase includes the integration, testing, piloting, and acceptance of a release. In this phase, the integration team brings together individual work packages of solution components developed or acquired separately during the Development phase. Security Certification is needed here to ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. Bug tracking and validation for security should be attempted sincerely.

4.3.6 Operations / Maintenance

This phase addresses the ongoing operations and support of the monitoring system. It begins after the business processes and system(s) have been installed and have begun performing business functions. It encompasses all of the operations and support processes necessary to deliver the services associated with managing all or part of a computing environment, and includes the scheduled activities, such as planned maintenance, systems backup, and production output, as well as the nonscheduled activities, such as problem resolution and service request delivery, including emergency unplanned maintenance of applications. It also includes the support processes required to keep the system up and running at the contractually specified level.

Implementing security management procedures, monitoring requirements and security upgrades procedures are a must to be undertaken at this stage. Logs, security incident reporting and change control and management are also crucial. From security perspective, Configuration Management and Control is needed to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

For a fully functioning IT insider monitoring system, much more needs to be addressed from a network configuration, routing design, network security evaluation, and an intrusion detection system/intrusion prevention development, policy and procedures development as well as security awareness programs.

4.4 Role of the Regulatory Body

By working with the Security Exchange Commission (SEC) and assisting with the monitoring efforts, corporations will be showing their dedication towards ensuring transparency and integrity of the financial markets. Through a query system, the SEC can run filters to identify possible illegal insider trading. Using the access path list identified by the corporation, the SEC would be able to run individual and financial security specific queries. By collaborating with each other, the regulatory bodies and the corporations will be able to achieve a mutual benefit. The corporations will maintain their reputation and the regulatory body will achieve its goal of ensuring honesty in the financial markets.

5. Conclusion

Since the starting point for an inside trader is from within their organization, security needs to start from the actual corporate entities and from within the technologies used in the corporation. By pursuing a strategy that includes documentation, training, monitoring and collaboration with the regulatory body, a firm should be able to reduce the incentive for an individual to participate in insider trading. No system is full proof and no system will completely eradicate insider trading, but attention to the *Insider Information Risk* value within the companies and monitoring process by the regulatory bodies may result in less people making the decision to engage in illegal trading activities.

References

Donoho, S. (2004) Early Detection of Insider Trading in Option Markets. ACM: Seattle

Efremov, Y. Insider Trading: No longer only for the Rich and Famous. Retrieved from http://www.econ.yale.edu/seminars/apmicro/am04/efremov-040427.pdf

Frye Colleen (2006), "Steps you can take now to begin building in software security" datelined 09 May 2006 interviewing Gary McGraw, author of Software Security: Building Security In, retrieved on 19.05 2006 from http://searchappsecurity.techtarget.com/qna/0,289202,sid92_gci1187360,00.html

Gunnar Peterson (2006) January 10, 2006 in Risk Management, SDLC, Security, Security Architecture, Software Architecture, Use Cases |Permalink retrieved from http://1raindrop.typepad.com/1_raindrop/2006/01/phasing_securit.html

Kowalski, R. (2000) High Profile Cases Can't Slow Insider Trading. The street.com . Retrieved from http://www.thestreet.com/stocks/brokerages/986653.html

Prince Kevin (2005), Added Protection: A Layered Approach to Internet Security, November 2005 retrieved from www.cavionplus.com.

Reconnex. (2005) Stop the Inside Threat. Retrieved fromhttp://www.stoptheinsiderthreat.com/threat.html

Schneier, Bruce. (1998) Security pitfalls in cryptographic design.Information Management & Computer Security. Vol. 6 No. 3, pp. 133–137.

Tenpas, R. (2006). Insider Trading: Another Front in the Battle Against Corporate Fraud. United States Department of Justice. Retrieved from http://judiciary.senate.gov/testimony.cfm?id=2405&wit_id=5776

The United States Securities and Exchanage Commission. Retrieved from http://www.sec.gov/divisions/enforce/insider.htm

Trading Session http://www.investopedia.com

Weidner, D. (2007, March 8) A disgraced trader will find open arms in the financial world. Market Watch. Retrieved from http://www.marketwatch.com/news/story/story.aspx?guid={E2DC9FE2-3AE0-4FF5-A0AF-43F16F76CC2B}&dist=rss