Research Challenges for Fighting Insider Threat in the Financial Services Industry

Dan Schutzer
Executive Director Financial Services Technology Consortium

1 Introduction

Although the problem of insider threat has always been of great concern in the Financial Services sector, its significance has increased in recent years. This increased concern can be attributed to three key factors:

Consolidation and Globalization: Consolidation and Globalization trends have led to larger institutions comprised of a significantly larger and more diverse workforce to manage, and greater employee turnover: the largest institutions can have hundreds of thousands of employees, not counting site contractors and outsourcers.

Rise of the Extended Enterprise: The dramatic advances in computer and communications technology, and the wide use of electronic commerce has made it possible and desirable to extend the traditional corporate boundaries, making its resources and information more accessible to outsourcers, third-party processors, vendor and customer partners.

Increased value of information: With the growth of electronic commerce, organized crime has found a more efficient and less risky way to commit acts of crime, including identity theft related fraud. It is now easier to recruit accomplices to commit crime more efficiently, and at a safe distance, often hiding from the law in foreign countries where it is more difficult to be caught and prosecuted. This has increased the value of information and the price people are willing to pay for it, including making it easier to collect and sell it without fear of being caught and brought to justice. This has increased the temptations for employees to turn bad and commit theft of sensitive personal information.

The first two factors have resulted in fewer employees remaining loyal to their company, and more likely to become disgruntled. It also makes it harder for the company to track and monitor suspicious activities. The last factor makes the motivation to commit insider crime stronger by making the theft of information both more rewarding and less risky. The third factor contributes to the growth of insider theft by increasing the motivation and making it harder to detect and protect against.
The challenge for research is to compensate for these negative trends by applying technology smartly and innovatively to assist in reducing the motivation of employees to commit or aid and abet insider theft. This can be accomplished by applying technology that can both reduce the motivation for employees to turn bad, improving employee morale, and increasing the risk and penalty of getting caught, while raising the bar of succeeding, by introducing more effective identity theft prevention measures.

In order to identify the most pressing research challenges needed to combat Insider Theft, it is helpful to discuss the overall problem and review the current approaches, shortcomings and gaps in the fight against Insider Theft. The following list is not meant to be exhaustive, but rather to stimulate the researcher into thinking about some of the key needs, problems and challenges in developing solutions to help fight Insider Theft.

An organization’s defenses against Insider Theft can be organized along the following three categories:

1. Screening and selecting employees and other individuals who are granted access to sensitive company information and resources.
2. Controlling access to data and resources, and protecting data and resources against unauthorized access.
3. Monitoring and detecting attempts, patterns and incidents of Insider Theft, and acting in an effective and timely manner to prevent or mitigate loss.

The effectiveness with which these three types of defenses are used today, and corresponding research needs is discussed below.

### 2 Employee Screening And Selection

Studies have been shown that approximately 1/3 of all convicted insiders had prior arrests. This illustrates two current shortcomings:

1. the failure of background checks to detect known criminals, and
2. the ability to better screen the 2/3 of the convicted insiders who would have been hired even if more effective background checks had caught all the previously known criminals.

The first problem, inadequate background checks, could be improved through better information sharing amongst Financial Institutions. Although this is starting to take place, within the constraints imposed by legislature designed to prevent discrimination or violation of an individual’s privacy rights. However, as this information-sharing improves, we are likely to see more effective evasive measures being used, such as falsifying social security numbers, names, and addresses. This reinforces the need for developing more sophisticated and robust means of identifying an individual, even one that is taking evasive actions not to be identified.