

Tackling the Insider Threat

Dawn Cappelli from Carnegie Mellon's CERT provides insight on Motives, Means and Mitigation Strategies

Upasana Gupta

November 6, 2008

Insider threat is a growing criminal activity, and given economic conditions there is a high risk of this fraud occurring -- especially in the event of banks merging, being acquired and employees being laid off. Consider:

- [Societe Generale: Lessons Learned on the Insider Threat](#)
- [Countrywide Insider Case Bigger than Initially Revealed](#)
- [Bank of New York Mellon Investigated for Lost Data Tape](#)
- [The Ameritrade Fallout](#)



These high-profile cases illustrate financial institutions that have become victims of insider theft and fraud in recent times.

What steps can financial institutions take to safeguard themselves from the insider threat? To fully understand the insider mindset and mitigation strategy, we interviewed Dawn Cappelli, a Senior Member of the Technical Staff in CERT at Carnegie Mellon University's Software Engineering Institute (SEI). She has over 25 years experience in software engineering, including programming, technical project management, information security, and research. She is technical lead of CERT's insider threat research program.

Insider crimes basically fall into three major categories:

- **Insider IT Sabotage**- includes deletion of relevant company data, bringing down systems and networks at the company. Key employees include database and system administrators
- **Theft for Business Advantage**- includes stealing business trade secrets, business strategies, proprietary company information, intellectual property. Key employees include- software engineers and programmers
- **Theft or Modification for Financial Gain**- includes stealing personal customer information such as social security numbers, bank account information, modifying credit history or changing name on a check etc. Key employees include- help desk, customer support basically non technical support staff members.

"The motive/ means and the factors which play in to commit these crimes in each of the three categories are very different and can be identified as the following," Cappelli says.

In case of IT sabotage almost always "revenge" is the key motive. Usually the employee is upset about negative work-related issues and wants to take revenge by disrupting the company's systems and network. These work-related issues can range from the employee being denied a promotion, to not getting along with his/her supervisor, or having issues with low salary or total compensation package. This can include any negative work issue that results in irrational behavior and makes the employee disgruntled. These employees usually attack after being terminated. They prepare well in advance when they can clearly see the end coming. They create unknown access paths and backdoor accounts as well as plant logic bombs and download password crackers and crack passwords of other employee accounts etc. All actions directed toward the institution's destruction.

When it comes to theft for business advantage- These crimes are not motivated by money but more often done to acquire and have a competitive edge in a new job. In few cases employees go and work for a competitor and take information with them. Also, theft takes place to start a new business or share confidential business plans and strategy with a foreign government. The employee attitude here is "This is mine; I created it, therefore why shouldn't I take it with me?" Usually these criminal activities (around 95%) commence from the time the employees are resigning. About 68% of thefts in this category take place three weeks after the employee has resigned from the company.

With theft for financial gain, the motive here is always money. These thefts take place usually among employees who are working in help desk and customer support areas where they typically do not have a clear career path and have access to sensitive information. They are current employees of the institution, who do not want to get caught and use common methods to commit the crime like downloading and taking print out of sensitive information home, writing passwords and bank account information etc.

Within banking the most prevalent threat is theft for financial gain, followed by IT sabotage and theft for business advantage, Cappelli says. This analysis is based on CERT crime data ranging from 1996-2007.

One of the interesting factors that have led to the increase in theft for financial gain is also the fact that half of the crimes conducted were employees recruited by outsiders, meaning individuals tied with under ground crime organizations. These individuals have had a major role in placing these employees at various institutions and as a result have used them as puppets to commit the crimes and get access to confidential information. "Companies need to be very cautious while hiring employees and need to beware of employees associated with organized crime groups for money," says Cappelli. Extensive background checks are strongly recommended to ensure that employees do not hold any criminal record and have a sound credit history. Attention needs to be paid to these details while hiring new employees.

What steps, actions and mitigation strategies should financial institutions take to safeguard against insider threat?

- **Pool Your Efforts** -- The first step an organization needs in addressing insider threat is implementing and following best practices in terms of people, process and technology. Usually, when an insider threat happens, management blames it on IT, but fails to understand that insider crime is not just a technical issue. Instead, this is a complex problem that encompasses the entire organization and requires a combined and integrated effort from all. Managers from Legal/ HR/ Audit/ Business/Finance/ IT in an organization need to realize how this works and how they may be vulnerable, as well as how they need to proactively work together to prevent this from happening.
- **Look for Signs** -- Institutions can be proactive and look for signs and patterns for insider threat and prevent it from actually taking place. For example: a few signs of a disgruntled employee are irrational behavior, sudden drop in work performance, etc. Management need to take these signs seriously and deal with the employee problem in time to avoid insider attacks from taking place.
- **Apply the Right Technology** -- Good logging and monitoring practices coupled with sound configuration management and access controls are significant in mitigating insider threats. 68% of theft for information takes place within and after three weeks of the employee leaving his/her job. Again, disgruntled employees create unknown access paths, log on and access unauthorized files and information after being terminated. This is the reason that companies need to proactively log and monitor to ensure insider attacks can be mitigated. Implementing data leakage tools, conducting enterprise wide risk assessments, strengthening internal controls and effective audit functions can all lead to preventing the insider attack from happening.
- **Training** -- Cappelli recommends that institutions stress security awareness training, emphasizing system log protection, password protection etc. And visit the insider threat webpage on the CERT, which contains extensive information and research on insider attack and fraud, including a case library listing around 300 insider threat cases. CERT also provides effective training to organizations on awareness and mitigation strategies.