ASA

Annie Searle & Associates LLC

Research Note

Navigating the Distinctive Challenge of Insider Crime

By Andrew H. R. Hansen

Keywords: Insider crime, employee theft, fraud, IT sabotage, the Fraud Triangle, CERT

Abstract: Organizations are increasingly falling victim to cases of insider crime. The types of crimes being committed are numerous and diverse and are most commonly perpetrated by employees who have been involved in a negative work-related experience. Although the motives for the crimes differ, pressure, rationalization and motivation are elements that are generally present. Organizations should take the time to learn and identify suspicious behaviors. Effective communication channels and structured reporting processes can help organizations properly resolve employee concerns, avoid legal missteps and damaging consequences.

Introduction

Information security has often been referred to as a journey, not a destination. It's understandable that those committed to this journey often get focused on the hardware and software, malware and spyware, the network and firewall. With so much energy spent defending against threats perpetrated by those outside the organization, flying quietly under the radar is a threat easy to underestimate: employees inside the organization. Due to the fact that employees have legitimate access to information systems, networks and data warehouses, employees pose a risk to organizational security that should be taken seriously. This article will discuss major categories of employee crime, help employers identify suspicious behaviors and understand perpetrator motives, as well as recommend actions organizations should take to prepare for and respond to this inescapable vulnerability.

Types of Insider Crime

Unfortunately for information security professionals and their employers, types of insider crime are only limited by the imagination of the perpetrators. In an effort to narrow the scope to common criminal behaviors, we will focus on three major categories of insider crime defined by researchers at the Community Emergency Response Teams

(CERT) and the Software Engineering Institute and CyLab at Carnegie Mellon University: fraud, theft of information, and IT sabotage[1].

Fraud

Depending on the context, fraud can be defined in multiple ways. But reaching across the majority of characterizations is the simple, succinct, defining attribute: deception. Fraud is deception[2]. In a comprehensive report published by the Association of Certified Fraud Examiners (ACFE) in 2010, researchers compiled data from 1,843 cases of occupational fraud that occurred between January 2008 and December 2009[3]. For the purposes of their study, fraud was parsed into three general categories:

1) Corruption – Included behaviors like conflicts of interest (purchasing schemes, sales schemes, etc.), bribery (invoice kickbacks, bid rigging), illegal gratuities, and economic extortion[4]

2) Asset Misappropriation – Included behaviors like larceny, skimming, fraudulent disbursements (billing schemes, payroll schemes, check tampering, ghost employee, commission schemes, workers compensation, forged endorsement, etc.)[5]

3) Fraudulent Statements – Included behaviors like Asset/Revenue overstatements, timing differences, fictitious revenues, concealed liabilities and expenses, improper disclosures, improper asset valuation etc.[6]

The resulting statistics from this study seen in Figure One,[7] indicate that government organizations and both public and private companies, are all experiencing increases in the frequency of fraud relative to 2008 figures.[8]

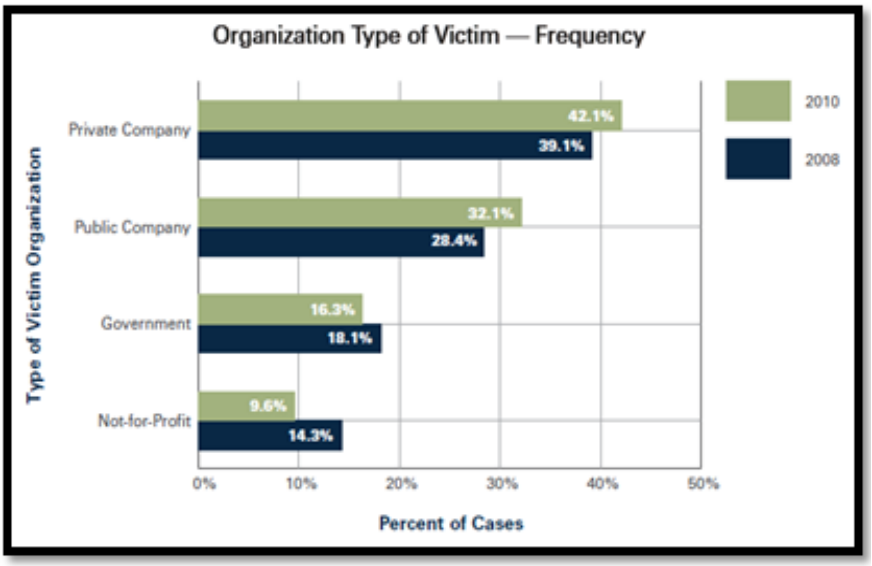

Figure One –Organizational Type and Frequency

Not only is the rate of fraudulent incidents the highest amongst private and public companies, these organizations were also "victim to the costliest schemes… the median loss for the cases of these businesses was $231,000 and $200,000, respectively." [9] Losses experienced by government agencies and not-for-profit organizations were about half as much at $100,000 and $90,000 each.[10] Also worth noting, small businesses – defined as those with less than 100 employees – "suffered the greatest percentage of the frauds… accounting for more than 30% of the victim organizations."[11]

Theft of Information

Defined simply as "stealing confidential or proprietary information from the organization,"[12] theft of information can result in "loss of intellectual property, compromised customer privacy, loss of company reputation, and exposure to regulatory violations."[13] In a recent case of information fraud, an employee of a major bank sold private customer data to criminals. These transactions resulted in losses of $10 million dollars to the bank, and eroded trust between the bank and its customers.[14]

Research conducted by the Poneman Institute in 2009, "surveyed 945 adult-aged participants located in the US who were laid-off, fired or changed jobs in the last 12 months."[15] The study found that more than 59 percent[16] of those surveyed claimed that they kept company data after leaving their employer, despite the fact that 79 percent[17] acknowledge knowing "they do not have permission to do so."[18] The most prominent type of confidential, sensitive or proprietary information kept by the exiting employee was email lists, as 53 percent felt "the information might be useful to them in the future,"[19] followed by non-financial business information, customer information including contact lists, employee records, and financial information.[20]

IT Sabotage

IT sabotage is "acting with intention to harm a specific individual, the organization, or the organization's data, systems, and/or daily business operations."[21] In a study conducted by researchers with the United States Secret Service and CERT, of the insiders that had committed IT sabotage, "eighty-six percent of the insiders held technical positions."[22] Because employees are so familiar with the data and systems they work with on a regular basis, they often know the precise way to inflict the most severe damage to the organization. The study reported that financial losses associated with IT sabotage "ranged from a reported low of $500 to a reported high of 'tens of millions of dollars.'"[23]

In addition to financial damages caused to an organization, the following examples from an Insider Threat Study[24] conducted by CERT highlight problems associated with IT sabotage. These problems can include:

- "Severed communication with affected organizations due to shut-down networks, router, servers, or dial-up access
- Blocked sales due to inaccessible sales applications or deleted sales records
- Blocked customer contact due to blocked customer passwords

- Damaged or destroyed critical information assets, such as proprietary software, data, computing systems, and storage media necessary to the organization's ability to work, produce product, or develop new products
- Damaged supervisory integrity, including exposed personal or private communications embarrassing to a supervisor."[25]

Identifying Motives and Signals

For a variety of reasons, employers may feel that they are impervious to insider crime. They might mistakenly believe that their business has too few employees, their watchful eye has everything sufficiently covered, or that relationships have long been established as trusting. Findings from a comprehensive study prepared by the Association of Certified Fraud Examiners (ACFE), point out that "eight-six percent (of perpetrators) had never been charged with or convicted of a prior offense."[26] This detail highlights the need for employers to be aware of common motives of internal crime and understand ways environmental circumstances influence these behaviors.

Developed by Dr. Donald R. Cressey, "The Fraud Triangle"[27] specifies three elements that are generally believed to be found in the majority of fraud cases. Although the model was based upon cases of fraud, the concepts certainly extend to the other types of employee

crimes previously discussed. Illustrated in Figure Two[28], the three elements of the fraud triangle are:

1) Opportunity. For fraud to occur, the employee must believe the crime can be committed and concealed[29]

2) Pressure. In many cases it is financial pressure, job dissatisfaction or fear of losing a job[30]

3) Rationalization. Most often comes in the form of entitlement, or an inflated sense of self-importance and contributions, or a false sense of ownership.[31]

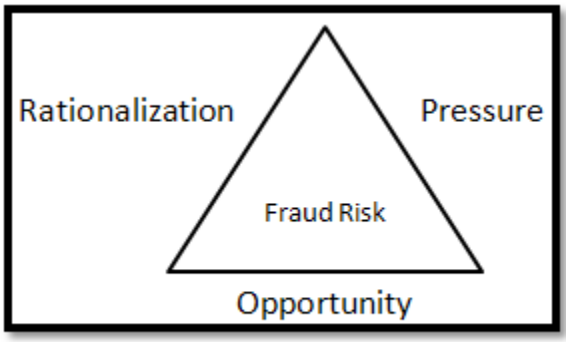

Figure Two – The Fraud Triangle

It is important for employers to recognize that the majority of insider crime is the direct result of a specific event or a series of events[32] – often the employee feels as though they have been mistreated in some way. Employees involved in insider crime almost always engage in some form of abnormal behaviors that comes to the attention of their coworkers.[33] However, abnormal behaviors should not necessarily be interpreted as extreme behaviors. Employers should watch for more basic changes in employee performance. For example, a generally strong performing and reliable employee is suddenly constantly truant or tardy, engages in arguments with coworkers, or the quality of their work diminishes significantly.[34]

Each of these may be warning signs that the employee has been involved in an event that is negatively impacting their feelings towards their work.

Mitigating

Having covered major types of insider crime and identified some of the motives and behaviors associated with them, we are now better prepared to discuss possible mitigating steps employers can take to improve their ability to defend against these troubling actions.

In the study conducted by U. S. Secret Service and the Cert Program mentioned earlier, researchers suggested that "First, managers should recognize the personal predisposition of their employees and understand the impact they can have on insider threat risk. Second, organizations should attempt to manage expectations of employees to minimize unmet expectations."[35] Operating under this framework, employers are then better prepared to take further proactive mitigating steps.

Employers should strive to have clearly established policies in place, and ensure efforts have been made to educate and inform their employees. Conducting thorough pre-employment screenings can also serve as a layer of protection to the organization.[36] Employers should

take the time to confirm that the people they are inviting to become a part of the organization are truly of the caliber they are expecting.

Efforts should also be made to ensure that there are open lines of communication between the different layers of the organization. Managers should not separate themselves from employee concerns, they should be willing to discuss grievances and make a special effort to resolve feelings of injustice or mistreatment.[37] Establishing a formal process for reporting incidents and documenting problematic behavior is also a wise practice.[38]

Lastly, "separation of duties is the most fundamental, effective fraud prevention measure. No single employee should have complete control over an entire transaction."[39] Although financial circumstances may make it difficult at times, implementing a system where multiple employees handle different tasks of the same transaction, can serve as a built in monitoring feature, and end up saving the employer money in the long run.

Like most threats to organizations, there is no panacea when it comes to dealing with insider crime. Employers should consider conducting a high-level audit of their own to brainstorm ways their organization might be vulnerable and prepare ways to mitigate these threats.

Responding to Suspected Insider Crime

Should an employer suspect criminal behavior, they should avoid jumping to conclusions. A thorough investigation should be conducted, being careful not to make accusations until actual evidence is found. [40] If an employee begins acting suspiciously or if credible evidence emerges in the investigation, employers should consider placing the employee on leave until after the investigation concludes.[41] Employers should also take special care to create detailed documentation throughout the entire process.[42]

Following these guidelines will increase the probability that an organization will be sufficiently protected against possible legal complications and improve their ability to press charges if this is deemed the appropriate course of action. Responding to insider crime in a measured and deliberate manner further protects the organization and ensures that a management misstep doesn't come back to cause additional harm to the organization.

Conclusion

Taking a moment to step outside all the statistics and recommendations allows the dust to settle on perhaps the most critical factor – the importance of open channels of communication and proper

employee treatment. Hopefully the merit of this statement has been firmly grasped as these ideas have been alluded to throughout this article. The simple reality is that organizations would not exist without people. As previously established, the majority of insider crimes are caused by employees who feel they have been wronged or mistreated. Employers that take special notice and care to foster a responsive environment sensitive to the concerns of their employees will result in a healthier organization, better prepared to avoid the devastating consequences of insider crime.

References:

[1]Dawn M. Cappelli, "Pay Attention! What Are Your Employees Doing?" Software Engineering Institute, Carnegie Mellon University. Slide 11. http://www.cert.org/insider_threat/. 2006.
[2]Mieke Jans, Nadine Lybaert,, and Koen Vanhoof, "A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR^2 Framework," *The International Journal of Digital Accounting Research* 9, (2009) 3.
[3] "Report to the Nations on Occupational Fraud and Abuse," 2010 Global Fraud Study, Association of Certified Fraud Examiners, 4.
[4] "Report to the Nations," 7.
[5] "Report to the Nations," 7.
[6] "Report to the Nations," 7.
[7] "Report to the Nations," 27.
[8] "Report to the Nations," 27.
[9] "Report to the Nations," 27.
[10] "Report to the Nations," 27.
[11] "Report to the Nations," 27.
[12] Cappelli, "Pay Attention!," Slide 11.
[13] "Theft of Information: A Multilayered Prevention Strategy," Cisco, accessed November 7, 2010, http://www.cisco.com/en/US/solutions/ns170/networking_solutions_products_genericcontent0900aecd8051f382.html
[14] David Lazarus, "Bank of America data leak destroys trust," Los Angeles Times, May 24, 2011. Accessed November 7, 2011. http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524
[15] "Data Loss Risks During Downsizing," Poneman Institue, LLC, Sponsored by Symantec Corporation. February 23, 2009, 2.
[16] "Data Loss," Poneman, 3.
[17] "Data Loss," Poneman, 3.
[18] "Data Loss," Poneman, 4.
[19] "Data Loss," Poneman, 8, 10.
[20] "Data Loss, Poneman, 10.
[21] Cappelli, "Pay Attention!," Slide 11.
[22] Andrew P. Moore, Dawn M. Cappelli, Randall F. Trzeciak, "The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures*," *Insider Attack and Cyber Security: Beyond the hacker*, Springer Science + Business Media, LLC., 2008, 4.
[23] Andrew P. Moore, Dawn M. Cappelli, Randall F. Trzeciak, "The 'Big Picture,'" 4.
[24] Michelle Keeney, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall, Stephanie Rogers, National Threat Assessment Center, United States Secret Service, CERT Program, Software Engineering Institute, Carnegie Mellon University, "Insider Threat Study: Computer Systems Sabotage in Critical Infrastructure Sectors," May, 2005, 21.
[25] Keeney, et al. "Insider Threat Study," 21.
[26] "Report to the Nations," 69.
[27] "Employee Fraud and Embezzlement," The Business Owner, 30, 2006, 3.
[28] "Employee Fraud," 3.
[29] "Employee Fraud," 3.
[30] "Employee Fraud," 3.
[31] "Employee Fraud," 3.
[32] "Insider Threat Study: Illicit Cyber Activity in the Government Sector," CERT Software Engineering Institute, Carnegie Mellon, 2008, 14.
[33] "Insider Threat Study," 14.

[34] "Employee Fraud," 7.
[35] "The "Big Picture,'" 14.
[36] "Employee Fraud," 4.
[37] Michelle Keeney, et al, "Insider Threat Study: Computer Systems Sabotage in Critical Infrastructure Sectors," May, 2005, 22.
[38] Michelle Keeney, et al, "Insider Threat Study: Computer Systems Sabotage in Critical Infrastructure Sectors," May, 2005, 23.
[39] "Employee Fraud," 4.
[40] "Employee Fraud," 6.
[41] "Employee Fraud," 6.
[42] "Employee Fraud," 6.