

Taxonomy of Inside Threats

How Systems-based Fraud, Errors & Misuse Inflict Enterprise Losses

After fortifying their networks' perimeters against the external threats from mysterious computer hackers, enterprises are now focusing their attention on eliminating the recognized inside threats of systems-based fraud, misuse, and errors.

Every organization faces the risk of technically capable, application-facing employees and insiders who exercise their knowledge of system rules and procedures to "game" systems to commit fraud. Even ethical employees can violate application policies to work around inefficiencies within a system but unwittingly reveal opportunities for damaging errors, misuse, and abuse.

"Though little discussed, the 'inside threat' causes the greatest real losses in corporations and governments today. Detecting inappropriate application activity committed by authorized users represents the 'next frontier' in information security."

– **Matthew Kovar, Yankee Group**

This white paper outlines specific threats of systems-based fraud, misuse, and errors in an effort to educate CFOs, audit executives, and information security professionals about the inside risks and threats that their organizations must defend themselves against.

Fraud

The reliance upon automated financial systems and the IT revolution that links business processes across multiple data systems only increase this risk created by "White Collar Hackers." Fraud and white collar hacks collectively drain 6 percent of an organization's annual revenue, according to reports from the Association of Certified Fraud Examiners (ACFE). In 2002, these losses totaled over \$600 billion. The PricewaterhouseCoopers Economic Crime Survey pegged the average loss per company at greater than \$2 million. Ernst & Young has called this "a bigger loss problem than viruses and worms combined."

An ACFE study found that the average scheme lasted 18 months before it was detected. More than half of the detected schemes accounted for losses greater than \$100,000; nearly one in six caused losses greater than \$1 million.

Fraudulent schemes typically target the billing and payroll processes because, quite simply, that's where the money is. Other forms of fraud include check tampering and "skimming" – or diverting a percentage of payments for personal gain.

Billing Schemes

Billing processes – and specifically a financial system's accounts payable module – are at the greatest risk for potential fraud losses. Internal controls, such as segregation of duties, provide some defenses, but fraudulent billing schemes remain a huge problem for many organizations.

Ghost Vendors. A common scheme is to create ghost – or false – vendors within the billing system. An accounts payable clerk who routinely adds valid vendors into the system can insert a ghost vendor into the financial system and process checks that are payable to the insider.

Personal Purchases. Employees are often tempted to buy personal items from their employer's standard vendors. Purchase orders from approved vendors that fall under typical enterprise budgets – computers for example – are often approved with little oversight, which allows insiders to make personal purchases through the enterprise billing system.

Accomplice Vendor. While not as common as insiders who work alone, employees can corroborate with vendors to commit fraud. With an authorized vendor producing official purchase orders and receiving payments at a normal address, internal controls are not likely to catch fraud schemes that include an accomplice vendor.

Quid Pro Quo & Barter Schemes. Businesses are often at risk of insiders trading valuable goods or services for personal gain. These schemes fraudulently deplete inventory with no benefit for the enterprise.

Returns & Voids. Insiders often dupe their employers out of cash with product returns and voids. After expensing an approved purchase, employees may return the purchased item for a refund and keep the cash from the purchase.

Corruption & Price Inflation. Insiders can orchestrate schemes where the enterprise purchases inferior goods at

higher than market prices. In exchange for the business, the vendor pays the employee a kickback. This scheme can also be played out with a shell company as a vendor where an enterprise purchases goods from the shell company, which is actually run by the insider.

P-Card Abuse. Many enterprises avoid employee expense re-imbursements through P-cards or purchase cards. However, P-cards provide insiders with a direct method of draining enterprise cash if their purchases appear as valid business transactions.

Payroll Schemes

After billing, payroll is the second most frequent target for fraud. Ghost employees, improper wages, and fake commissions often fall through the cracks for large enterprises with thousands of employees.

Ghost Employees. Similar to ghost vendors, ghost employees can be entered into a payroll system to produce an ongoing scheme that drains enterprise cash with monthly checks paid to non-existent employees.

False Commission. Commission-based employees can boost their compensation by falsifying sales orders for improper commission checks.

Worker's Comp Schemes. Much like ghost employees, false worker's compensation claims can be entered into a payroll system to drain enterprise cash with monthly checks mailed to the insider who orchestrates the scheme.

Falsified Wages. With automated payroll systems, insiders can boost their monthly wages if they can access the payroll system and fraudulently increase the amount of their paychecks.

Check Tampering

Outside of the schemes targeted at false or invalid bills and employees, insiders can direct their schemes toward the valid payments to commit fraud.

Altered Payee. Valid, authorized payments are frequent targets for fraud where an insider, such as an accounts payable clerk, alters a payee. For example, just before checks are run, an insider in the accounts payable system changes payee information to write the check so that he will be able to cash it. The insider also alters the vendor's address or bank routing number to deliver the check or route the payment for the insider to receive the funds. The insider then covers his tracks by changing the delivery or routing information back to the original information.

Forged Checks. Procurement systems that process wire transfer payments often produce paper checks made out

for \$00.00 with each wire transfer. Insiders can then alter these zero-value checks and cash them for whatever value they are altered to.

Forged Endorsements. Refund checks to an enterprise are at risk of never entering the financial systems. If intercepted, refund checks can be fraudulently endorsed. In one known instance, a payroll manager intentionally overpaid taxes, which led the government to send refund checks. The payroll manager then endorsed the checks "Pay to the order of" himself and deposited them to his own account before they ever hit the company's books.

Skimming

Skimming is an "off-book" scheme in which cash is removed from the company before it enters the accounting system. The receipt of cash or payment is never reported to the company. The most common skimming schemes are targeted at:

- Unrecorded sales
- Understated sales
- Theft of incoming checks
- Swapping checks for cash
- Refunds.

Misuse

Misuse or unauthorized use of automated financial systems poses another inside threat and must be considered a "business hack" because they violate enterprise policies and open the door for system errors and fraud. For example, authorized insiders can legitimately break enterprise policies in order to bypass inefficient processes. While this flexibility boosts productivity, it also opens the door for fraud and errors by overriding proper approvals and potentially creating duplicate accounts or introducing systems-based errors.

Override of Controls

Segregation of duties and internal controls form a base for corporate governance to prevent fraud. For enterprise financial systems, these policies are carried out through business process rules where, for example, a billing system has rules that do not allow the same person to process a purchase order and validate the receipt of goods. However, these rules are expensive to implement and maintain as policies evolve and individual privileges change with new hires, promotions, transfers, and terminations.

Most organizations have application-facing insiders who know how to circumvent or override these controls when needed. While most instance of control overrides are done with the intent to get business done, the override of controls creates an opportunity to commit fraud by

pushing through a payment to a ghost vendor without going through proper authorization and control checks.

Circumvention of Signing Authority Controls

Most enterprises assign budget and purchase authority to their managers and executives but cap their authorization for purchases of an established dollar figure. For example, the director of information security may have authorization for purchases under \$20,000 but must seek approval from the CIO for expenditures greater than \$20,000. In order to purchase a \$65,000 system without CIO authority, the director of information security divides the purchase order and payments into four separate purchase orders and payments that are each under the \$20,000 cap.

This circumvention of signing authority is common in most organizations. While some enterprises choose to overlook such abuse, this culture of disregard for controls and policies sets a tone for employees who seek to push the boundaries of their authority as it highlights the potential for fraud.

Unauthorized Use of Credentials

Loose password security and careless sharing of authorization credentials can lead to an insider misusing the financial system by the unauthorized use of someone else's credentials. If logged into the system as another, an insider can abuse these privileges by:

- Accessing unauthorized information
- Inappropriately altering information
- Circumventing controls
- Presenting the opportunity for fraud to occur.

Errors

While not directly targeted for personal financial gains, system errors can nonetheless inflict financial losses on enterprises and must be recognized as an inside threat that directly affects the bottom line. While business process errors seem limitless in scope, the greatest threats originate from those errors revolving around outgoing payments.

While payment errors can be damaging enough, some form of errors can create an opportunity for insiders to commit fraud. For example, if an employee sees that an invoice is paid twice or that a single invoice is booked twice, he then recognizes the opportunity to commit fraud by routing the second payment for personal benefit.

Duplicate Payments

For decades, duplicate payments have been recognized as a recurring problem that has spurred an entire industry of recovery audit services. Accepted industry studies have reported duplicate errors as approximately 2 percent

of total payables. To recover the losses from these duplicate payments, enterprises invest in recovery audits and collection services, which typically charge approximately 35 percent of the recovered payments.

Rather than returning the cash and payment back from a duplicate payment, vendors who receive the duplicate payment often extend a credit to the double-paying buyer who suffers unneeded pressure on its cash flow. However, 10 to 20 percent of duplicate payments are never recovered, which means that the average enterprise suffers an annual cash drain equivalent to 0.1 to 0.2 percent of its total payables.

Overpayments

Similar to duplicate payments, overpayments represent another significant error that inflicts an annual drain on enterprise cash. While studies have not dedicated the resources to report on the extent of these errors, overpayments are accompanied by all of the same costs associated with duplicate payments, such as:

- Recovery audit costs
- The direct hit to cash flow
- Recovered overpayments received in vendor credits.

Early Payments (with or without discounts)

Early payments are a common form of payment errors that impair enterprise cash flow. For predictable budgeting and capital planning purposes, most organizations have a policy on when invoices are to be paid. Some vendors offer discounts for early payments, but these should fall in line with enterprise policies and should only be authorized by appropriate managers.

Missing or Bad Information

Common billing mistakes are made from financial systems that are populated with missing or bad information. Checks that are not properly delivered must be tracked down and sent to the proper address. These payment errors can lead to check tampering fraud if undelivered checks present an opportunity for an insider or outsider who mistakenly receives the check.

Duplicate Information

Large organizations often face a common error where a single vendor or contractor is registered in the financial system more than once. Besides a management headache when consolidating records, duplicate information can lead to greater errors and make it more difficult to detect improper activity or fraud in regard to the vendor or contractor.

Payments to Erroneous Employees & Vendors

Payments to erroneous employees and vendors are more common than one might think. Most of these payments errors are the direct result of human errors in processing

a voucher or expense payment to employees or vendors with similar names.

The Oversight Solution

To meet the market's heightened concerns over inside threats from systems-based fraud, misuse, and errors, Oversight Technologies pioneered the concept and technologies of *Continuous Transaction Incident Monitoring*. Unlike existing perimeter security solutions or access control systems, Oversight identifies events where authorized users perform suspicious transactions within business systems. Oversight systems analyze transactions across multiple business applications in real time to detect, prevent, and deter financial loss from systems-based fraud, misuse, and errors.

The Oversight solution combines advanced data acquisition, data analytics, case management, and evidentiary analysis functionality. Oversight collects data across multiple platforms and performs multi-perspective analysis to identify fraud, misuse, and errors. Oversight then generates high-impact reports, provides integrated case management, and enables evidentiary analysis.

The benefits of continuous transaction incident monitoring are clear. First, this type of transaction monitoring establishes a business environment that deters employees and other insiders from committing business hacks. Continuous transaction incident monitoring provides the benefits of rigorous internal

controls without the overhead. Even if procedural rules are not 100 percent maintained or employees learn to game the system, risk managers are satisfied with a solution that keeps pace with real-time business transactions. Finally, continuous transaction incident monitoring acts as the ultimate layer of security from outsiders who penetrate the network as authorized users.

Multi-System Data Acquisition & Correlation

Oversight based its data acquisition technology on multi-pass and multi-system query technologies. Oversight collects data across multiple platforms to correlate information from ERP systems, legacy mainframe applications, network monitoring solutions, and external data sources as relevant to:

- Accounts Payable
- Accounts Receivable
- General Ledger
- Human Resources & Payroll
- Inventory Management.

Oversight's patent-pending data collection technology processes the incoming data and populates an independent and secure transaction-documentation database, which is then analyzed by Oversight's Collaborative Reasoning Engine.

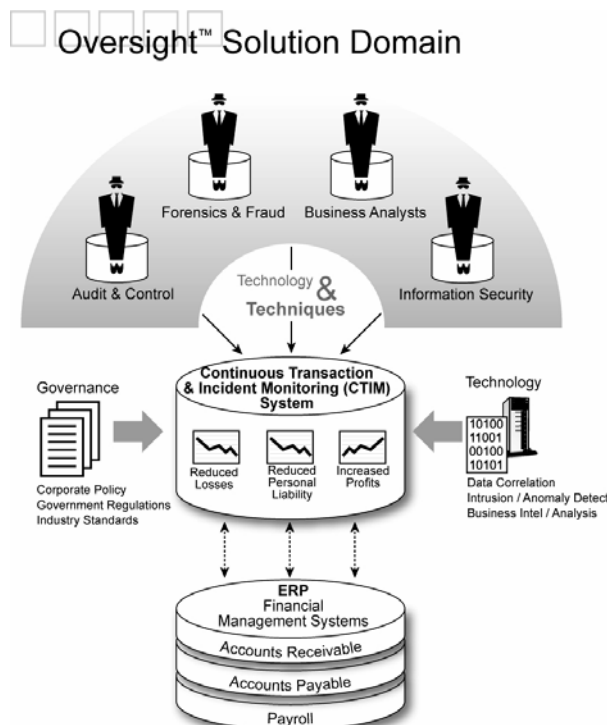
The Oversight Collaborative Reasoning Engine

Oversight's patent-pending Collaborative Reasoning Engine (CoRE) powers the system to flag suspicious activities and clearly distinguish real concerns from hundreds of indicators of fraud, misuse and errors. This advanced technology converts thousands of indistinct data sets into meaningful and actionable alerts and reports. The advanced CoRE analytics allow Oversight to move beyond simple, rules-based logic that produces unmanageable false positives while missing subtle linkages that indicate real misconduct. This multi-perspective analysis eliminates the dependence on low-level, procedural rules, and the need for complicated rules maintenance.

Oversight's CoRE conducts multi-perspective analysis based on domain engineering, automated link analysis, behavior, deductive analysis, and standard business intelligence. As an independent system that provides out-of-band monitoring and analysis, Oversight also detects acts of concealment and conversion designed to circumvent standard auditing techniques.

Case Management & Evidentiary Analysis

Oversight supports end-to-end case management and advanced investigative link analysis for high quality cases with irrefutable evidence. The case management system supports the collection and management of all case-specific events, clues, interviews, e-mails, and



reports. This secure work area greatly increases the investigator's ability to quickly and thoroughly resolve multiple cases without sacrificing the legally required integrity of the process.

The advanced evidentiary analysis tools significantly reduce the investigative and forensics analysis workload. Complex link analysis of the case related subjects, systems, and accounts takes a fraction of the time associated with manual research and analysis methods. Finally, Oversight's thorough results increase the recoveries of lost assets.

Security

Oversight systems are designed with security as the essential element of the hardened appliance. The digitally secure and trusted Oversight *Evidence Locker* stores transaction records, the reasoning behind evaluations and activities associated with the investigation process. Other security features include:

- Encryption & authentication of all communication channels
- Out-of-band configuration options to block its visibility on the network
- Hardened operating system
- Support for authenticated queries into business systems.

Return on Investment

Unlike perimeter IT security that guards against potential network attacks, continuous transaction incident monitoring provides a measurable return on investment with tangible results that go straight to the bottom line. As opposed to deflecting external threats, continuous transaction incident monitoring identifies, prevents, and deters real financial loss from system-based fraud, misuse, and errors.

With the Oversight solution, organizations boost their bottom line with by identifying, preventing, and deterring financial loss from systems-based fraud, misuse, and errors. For every loss that is recovered and prevented, Oversight delivers results that go straight to the bottom line.

Benefits

With its real-time transaction monitoring and analysis engine, Oversight identifies fraud, misuse, and errors that directly affect the bottom line. Oversight combines the benefits of a systems auditor, fraud examiner, forensics auditor, and an information security specialist on duty 24x7 to monitor the effectiveness of internal controls.

Detect

With its advanced analysis engine, Oversight identifies systems-based fraud, misuse, and errors in real time. Rather than relying on periodic audits that sample transaction data, Oversight's continuous transaction incident monitoring identifies the problem the moment it occurs and prevents a perpetrator from covering his tracks.

Prevent

By identifying errors, misuse, and abuse in real time, Oversight prevents financial loss by allowing an organization to quickly and decisively respond. In many cases, Oversight alerts allow an enterprise to close a hole before it can be exploited.

Deter

With continuous transaction incident monitoring, Oversight powers enterprises to "trust but verify" its financial transactions. Oversight allows an enterprise's management team to establish "tone at the top" regarding expectations of conduct.

About Oversight Technologies, Inc.

Oversight Systems is the leading provider of independent, automated transaction integrity monitoring solutions. By combining the expertise and experience from security, fraud, audit and enterprise software development professionals, Oversight Systems is redefining how enterprises satisfy Sarbanes-Oxley compliance requirements and enabling corporations to gain substantial returns from their compliance investments. For more information, visit www.oversightsystems.com.

Oversight Systems, Inc.
75 Fifth Street NW
Second Floor
Atlanta, GA 30308
www.oversightsystems.com
phone: 404.920.2039
info@oversightsystems.com