Fraud: Advanced Concepts for Auditors and Fraud Examiners

The Institute of Internal Auditors
Austin Texas Chapter
December 2, 2014

John@JohnHallSpeaker.com
(970) 926-0355
John J. Hall, CPA

John Hall is the founder and President of Hall Consulting, Inc. and the author of the award-winning book “Do What You Can! Simple Steps–Extraordinary Results”. He is also the developer and author of The Anti-Fraud Toolkit – a self-paced system for leading a Anti-Fraud Campaign in any size organization.

Through live and recorded programs, performance coaching, and business consulting engagements, John helps program participants and client team members:

- Improve organizational and personal performance
- Enhance the effectiveness of business processes and individual behavior
- Improve interpersonal and communications skills
- Identify and improve areas of exposure to business risk, wrongdoing, and fraud

Speaking, training, coaching and consulting areas include:

- Personal and work group effectiveness, team building and motivation
- Communication and interpersonal behavior skills enhancement, including:
  - Establishing rapport and trust
  - Interviewing and listening
  - Speaking and presenting
  - Selling ideas and influencing others to take action
  - Audit and management leadership
  - Collaboration and consulting skills for professionals
- Fraud prevention, early detection and incident response

In January 2014, John published The Anti-Fraud Toolkit – a self-guided system for business fraud prevention and prompt detection. In 9 learning modules and 5 hours of video-recorded lectures, users can strengthen anti-fraud defenses and learn exactly ‘how-to’ reduce losses, find incidents more quickly, and handle them efficiently. The Anti-Fraud Toolkit uses the action steps John developed over 20 years in his client consulting and training engagements.

In total, Mr. Hall has 35 years of experience as a professional speaker, consultant, corporate executive, and business owner. In addition to operating his own businesses since 1990, he has worked in senior leadership positions in large corporations and international public accounting firms. John is a Certified Board Advisor, and a member of the National Speakers Association, the American Institute of CPAs, and the Institute of Internal Auditors.

Meet John at www.JohnHallSpeaker.com

Email John at John@JohnHallSpeaker.com
LET’S GET STARTED

1. Brainstorming fraud risks is based on the “Three C’s of Fraud”:
   - Commission
   - Conversion
   - Concealment

   Follow the seminar leader’s verbal instructions, and outline a scheme leading to the theft of $10,000 from your organization that takes the Three C’s into account.

2. Assume that your organization's fraud losses are 1 percent of your annual revenue. List the five areas of fraud risk that account for most of this loss.
   1.
   2.
   3.
   4.
   5.

3. What is the number one fraud problem at your organization today?

4. What is the single most important action your organization leaders could take right now to cut fraud losses in half in one year?

5. I’m at this seminar because I want to be Better! able to:
SEMINAR FOUNDATION

1. Here’s what’s going to happen:
   a. Using fraud cases (including your cases) as a basis, explore current, emerging and continuing challenges from wrongdoing, misconduct and fraud. Build on the difference between a ‘war story’ and a ‘lesson learned’
   b. From the lessons learned from these cases, develop action plans for us all to use on the job
   c. Use brainstorming – individually, in small groups, all of us together
   d. Emphasize bright spots – where does it already work
   e. Discuss how to improve bottom line results through fraud risk management

2. Fraud exposure areas:
   a. Misappropriation (tangible and intangible assets)
   b. Manipulated results reporting (financial and other measures)
   c. Corruption (or shadow deals)

3. The “Three C’s” and Root Cause Analysis will be stressed throughout the seminar

4. The distinction between macro, micro and systemic fraud is a key concept for us

5. Auditors and fraud examiners are:
   a) Paid to be professional doubters.
   b) Expected to find hidden issues (including fraud) on our assignments.

6. Controls do not prevent fraud. Controls make a fraudster change their method.
   a) Organizations must tweak the path – make wanted behaviors a little easier and wrong behaviors a little bit harder.

7. This program is about you. The answers to your fraud challenges are here in this room. My role is to help you bring them to the surface. **Your role is to convert the solutions we discuss to action on the job.**
   a. You are anti-fraud experts – You must lead, teach and be visible.
   b. The destination must be clear – “Some is not a number; soon is not a time”
   c. We will use the concepts of “Solutions-Focused Therapy”
SYSTEMIC FRAUD - THEFT

PURCHASING CARDS

1. Maintenance department administrative assistant
   - $35,000 tool purchase and immediate resale – Home Depot Los Angeles
2. Dallas Independent School District
   - Dallas Morning News July 2, 2006
   - “Secretary charges $383,788, has no receipts”
   - “Former DISD Employee Pleads Guilty to Federal Charge”

INVENTORY

1. The problem with ‘shrink’
2. Ship electrical generator – Perth Amboy
3. Physical verification matters
4. Value verification matters

USED ASSETS AND SCRAP

1. Disposition of equipment, vehicles, real estate, and other long-term assets
2. The problem with ‘scrap’ and ‘obsolete’ assets
3. Street light poles
CASE EXAMPLE: P-CARD

THE HOME DEPOT 0654
7015 E. TELEGRAPH RD., COMMERCE, CA 90040
STOREMgr.GREG HUNDO (323)727-9800

SALE 0654 00022 95228 03/14/06 51 JC4320 01:50 PM

015082777320 WELD-PACK200 459.00
074162262000 SOFTSCAP 7.5 2 8.17
037004328292 DHM 38 3.49
037008860862 BOUNCE BD 3.99
SUBTOTAL 470.32
SALES TAX 38.80
TOTAL 509.12

AUTH CODE 539593/821858 7A

THE HOME DEPOT 0654
7015 E. TELEGRAPH RD., COMMERCE, CA 90040
STOREMgr.GREG HUNDO (323)727-9800

SALE 0654 00022 07785 02/28/06 51 JM412M 01:06 PM

020877495358 2 GAL VAC 99.00
039752500774 71/4MOWER 159.90
02175972946 365 CLEANER 2.88
020877317056 PAR.BROOM 29.97
020877491578 18V 100 K 525.00
SUBTOTAL 815.85
SALES TAX 75.89
TOTAL 891.74

AUTH CODE 513492/222046 7A

NOW HIRING SPRING SEASON ASSOCIATES
PT/FT APPLY TODAY IN-STORE OR ONLINE
_AT: STORECAREERS.HOMEDEPOT.COM/HELP
******************************************************

ENTER FOR A CHANCE TO WIN A $5,000 HOME DEPOT GIFT CARD!

Your Opinion Counts! We would like to hear about your shopping experience. Enter to win a $5,000 Home Depot Gift Card by completing a brief survey about your store visit at:


You will need the following to enter on-line:

User ID: 191399 190767
Password: 6164 190745

Entries must be entered by 04/13/06. See complete rules on website. No purchase necessary.

(Para de cada enunciado que no se encuentra en español en la página del Internet.)
YOUR CASES AND LESSONS LEARNED

MISAPPROPRIATION

RESULTS REPORTING

FINANCIAL RESULTS:

OTHER RESULTS:

SHADOW DEALS

INTERNAL CONTROL LESSONS FROM YOUR CASES:

In the end:

• Does it make sense?
• Is it all documented?
• Everyone who approved:
  
  DID THEY KNOW HOW (Situational Competence)?
  ARE THEY ACCOUNTABLE FOR ACTUAL RESULTS?

• Given all the information you have, would it pass the headline test?
FRAUD RISK MANAGEMENT:
OPPORTUNITIES FOR AUDITORS AND FRAUD EXAMINERS

1. FRAUD DETERRENCE AND PREVENTION
   a) Anti-fraud internal control infrastructure
   b) Acceptable and unacceptable behavior is defined and communicated
   c) Leaders at all levels set a great example – every day
   d) Policy on Suspected Misconduct
   e) Reporting of suspected violations is required
   f) Losses are identified, quantified and tracked
   g) Comprehensive fraud exposure analysis
   h) Meaningful fraud skills training for employees
   i) Auditors and employees look actively for fraud
   j) Fraud response is in place and ready to go

2. EARLY FRAUD DETECTION
   a) Detection-based audit steps
   b) Detection-based internal controls and behaviors
   c) Clear statement of detection responsibilities and accountability
   d) Effective hotlines
   e) Other tip sources
   f) Monitoring for red flags and other fraud indicators
   g) Special focus on third party relationships

3. EFFECTIVE FRAUD HANDLING
   a) Employees know what happens when the alarm sounds
   b) Investigation
   c) Loss recovery
   d) Control weaknesses are fixed
   e) Coordination with law enforcement and prosecutors
   f) Publicity issues
   g) Human resources issues
   h) Employee morale issues

Organizations (and their fraud risk teams)
must be prepared to address fraud risks at all three levels.
ANTI-FRAUD ENVIRONMENT

HUMAN SUPPORT

Soft Controls
Competence
Interest
Time

ENVIRONMENTAL SUPPORT

Infrastructure
Hard Controls

CONSIDERATIONS:

Internal control design and implementation
Industry practices
Regulation and compliance
Competition
Governmental concerns
Geography
Ownership
Beliefs

The power of CONTEXT:

a new idea is no match for existing culture
10 REASONS ANTI-FRAUD CONTROLS BREAK DOWN:
HOW MANY DOES THE UNIVERSITY HAVE TODAY?

_____ 1. Blind trust

_____ 2. Willful blindness
• Ignoring control implications of policies, procedures and reports
• Ignoring behavioral indicators of problems

_____ 3. Situational incompetence

_____ 4. Not having information needed to assure transactions are proper

_____ 5. Not questioning the strange, odd and curious

_____ 6. The process mentality

_____ 7. Not enough time to do the control procedures

_____ 8. Not enforcing documentation requirements

_____ 9. Acceptance of the situation
• Fear
• Positional immunity
• Conflict avoidance

_____ 10. Those in charge intentionally ignore or override procedures
HOW IS FRAUD FOUND?

Managers and others with review and control responsibilities

Best position to know; best position to notice

Internal auditors and fraud examiners

Time constrained
Other priorities
Wrongful acts and transactions are intentionally hidden from us
Sampling

External auditors

Will probably miss immaterial cases
Standards (and engagement contract) limit responsibility
Minimal fraud training for most

Other third parties

Students and others directly served by the University
Industry sources
Suppliers, contractors and bidders (including bid losers)
Former employees, suppliers, contractors
Joint venture partners
The public
Anonymous tips
Law enforcement

The thief

Yields to pressure from maintaining the fraud
Gets sloppy or arrogant
Bargain for relief
Foul up

By luck or by accident

Detection barriers

a) We don’t know what can go wrong and what it looks like
b) We are too trusting of employees, executives and managers
c) We accept explanations for symptoms of fraud without verifying the facts
d) We don’t ask enough questions – especially follow up questions
e) ‘Form over substance’ audit and examination work
AUDIT / INVESTIGATION FLOW DIAGRAM

- Tip
- Audit
- Exception
- Pattern
- Review Of Records
- Interviews
- Interrogation
- Law Enforcement
- Insurance Company
- Control Weakness
- Case File
- Bonding Claim
- Audit Report
FRAUD DISCOVERY FOR AUDITORS, FRAUD EXAMINERS AND MANAGERS

I. THINK LIKE A THIEF

Look at identified weaknesses and other opportunities from the perspective of how they could be exploited. Documentation should include specific fraud risks identified and a clear bridge to specific project steps, controls and behaviors targeted at detection of related fraud incidents.

II. USE DISCOVERY TECHNIQUES AGGRESSIVELY

a) Discovery or attribute testing.

These tests have as their purpose surfacing the visible signs of wrongdoing. Such testing can be directed at either electronic or manual records. The use of electronic data analysis tools makes the efficient search of large populations possible.

b) Interviews.

Targeted interviewing techniques can be an efficient method for surfacing hidden information. They are used to get the “human” information not available in records. In situations where the signs of fraud might not be in the records, the interview may be the only method available to surface needed information.

c) Monitoring for fraud indicators.

Examples include:

• Internal information used by management to find problems in operations
• Reconciliations, closing entries, adjustments, override transactions and other available information showing a deviation from normal results
• Recurring software-based inquiries

III. DETERMINE THE CAUSE OF ALL FRAUD INDICATORS SURFACED

All indicators surfaced should be investigated as to their cause. Follow up on fraud indicators, symptoms and red flags may lead to the discovery of wrongdoing. It also may surface other important non-fraud issues. Either result justifies following all observed indicators through to the determination of their Root Cause.
MONITORING IDEAS

1. Standard reconciliations
2. Top performance
3. Poor performance
4. Timing differences
5. Suspense accounts and clearing accounts
6. Complaints
7. Overtime by employee
8. Top travelers and earners
9. Consulting and other third party services billings
10. Adjustments and overrides:
    · Prices
    · Receivable accounts
    · Cash accounts
    · Inventory
11. Closing entries
12. Failures
13. Common names or addresses for refunds or credits
14. Goods purchased in excess of needs / slow turnover
15. Duplicate payments
16. Regular meetings with key executives
OTHER METHODS OF DISCOVERY

1. Auditors and examiners use confirmations for many purposes. Examples of confirmations aimed at fraud detection include:
   - Change of address, mailed to prior address
   - Payments, using a copy of both the front and back of the check
   - Receivables already written off
   - Late payments
   - Refunds and credits

   List other confirmation ideas aimed at surfacing fraud indicators:

   __________________________________________________________
   __________________________________________________________
   __________________________________________________________

2. Some fraud cases surface as a result of tips from informants. What can we do to encourage concerned employees to come forward? What about vendors, customers and other third parties?

   __________________________________________________________
   __________________________________________________________
   __________________________________________________________

ACTION IDEAS – MONITORING AND OTHER WAYS TO DETECT FRAUD
MISAPPROPRIATION OF ASSETS

CASH

1. Theft of cash from point of sale terminals, cash registers and similar devices

2. Diversion of payments received on account

3. Fraudulent disbursements, including schemes in accounts payable, contractor billings, loans, investments and many others

4. Payroll and benefits, including abuse in overtime, benefits, tuition and charitable contribution programs and other schemes

5. Petty cash

6. Travel, entertainment and other out of pocket cost reimbursement

Theft of cash on hand

For reasons that are obvious, organizations with large amounts of cash are very susceptible to theft. The actual theft of the cash -- the *commission* of the fraud -- is relatively simple. Similarly, there is no *conversion* step necessary. These schemes become complicated to the thief during the *concealment* stage.

Cash shortages should be detected in the same day they occur if even basic reconciliation controls are in place and operating. In a similar manner, effective month end bank reconciliation procedures may demonstrate the existence of wrongdoing.

Common schemes involving the theft of cash on hand and the attempt to cover the theft in the records include the following:

1. *Skimming* – Cash is “skimmed” before it enters the accounting system. For example, the employee accepts cash but never prepares a receipt, or prepares a receipt for less than the amount taken.

2. *Substituting personal checks for cash* – The employee takes money from the cash register and substitutes a personal check. In that way, the cash drawer is always “in balance,” but the employee never submits the check for deposit into the organization’s bank account. They employee gets the free use of the cash.

3. *Fictitious refunds or discounts* – Employees record a refund and remove cash as if a refund had occurred. But no merchandise was returned or discount given.
ACCOUNTS RECEIVABLE DIVERSION

Most misappropriation related to accounts receivable involves diversion of payments received from customers and others. Schemes to commit fraud and convert the proceeds are fairly simple to perform:

1. Cash payments are simply removed
2. Non-cash payments on account are diverted
   - An employee opens a bank account in a name similar to the entity being defrauded. Customer payments are then deposited into this account and removed when they clear.
   - Customers are advised of an incorrect account for wire transfer payments

What varies is how the fraud is concealed. Common techniques include the following:

- **Lapping** – The payment from Customer A is diverted to the employee. To keep Customer A from complaining, payment from Customer B is applied to Customer A. Customer C’s payment is applied to Customer B’s account, and so on.

- **Posting bogus credits to the account** – To conceal the fraud, the employee posts credit memos or other noncash reductions (for example, a bogus sales return or write-off) to the customer account from which the funds were diverted.

- **Altering internal copies of invoices** – The company’s copy of the sales invoice is altered to report an amount lower than was actually billed to or collected from the customer. The “excess” payment is diverted.

Other schemes involving receivables include:

- **Diversion of payments on written off accounts** – many organizations do not monitor activity on accounts that have been written off. This creates the opportunity to divert the funds that were not expected.

- **Freshening and kickback** – the fraudster makes arrangements with past due customers to help “manage” their accounts. Adjustments are made to make the account appear to be current (for example, by canceling older invoices and rebilling the transactions with current dates). This effectively gives the customer unlimited time to pay the bills and avoid late fees and interest charges. The employee receives a kickback or other incentive from the customers.
INVENTORY THEFT

Theft of inventory for personal use. More likely to occur when items are small in size but have a relatively high value to the employee or other consumer. For example, in general a notebook computer has more “value” to the thief than does the computer chip that drives that computer.

Theft of inventory for resale. As theft is for resale, “value” to the thief is not based on their own ability to use the item taken, but is based on the ability to the thief to convert the stolen items to cash or other assets through resale. As such, high quantities of items stolen provide high conversion value and thus higher appeal to the thief. Common schemes include:

1. Receiving personnel removing goods right from the receiving docks before physical custody is perfected.
2. Collusion with delivery personnel to arrange for goods to be dropped at an unauthorized location
3. Records direct that items purchased are to be delivered to a location where the thief can easily take control

Theft of scrap, other used assets and production by-products. In many organizations, controls may be weak over production and inventory scrap disposition as well as the retirement and disposition of used long-lived assets. Creative thieves find ways to sell these items, and divert all or part of the proceeds. Examples include:

1. Setting up but not disclosing ownership of “customer” organizations or brokers who purchase or dispose of these items at a below market “spot price.”
2. Purchasing used vehicles at less than fair value, and then immediately reselling these vehicles to third parties at market value.

Note that losses can be significant, especially where the embezzler has the authority or other ability to inappropriately designate good inventory and other usable assets as scrap.
PURCHASING, ACCOUNTS PAYABLE AND VENDOR FRAUD

The purchasing, contracting and payments functions are particularly vulnerable to fraud. Exposures include:

Payment of invoices to a fictitious or related entity – the embezzler establishes a fake entity or has control over a real entity, and enters transactions into the payments stream through the vendor master file or as a one-time payment vendor. An invoice is produced and processed. Funds are diverted by check or through electronic payment.

Kickback paid by vendors – formal kickbacks or other similar incentives are used to:

1. Allow the vendor to submit fraudulent billing and approving the payment (billing for goods never received or services never performed, billing more than once for the same item, providing low quality items but billing for the higher quality)
2. Allow excess purchase of property or services
3. Facilitate bid rigging
4. Maintain the relationship

Common Indicators – Purchasing and Accounts Payable

Fictitious vendors and related payments schemes -

1. Photocopied invoices, invoices with signs of tampering, or invoices on plain paper when preprinted forms might be expected
2. No phone number on the invoice; no tax ID number on file
3. Address, tax ID number or phone number is the same as an employee, another vendor or a related party
4. Vendor names are a “knockoff” of a well-known business (‘IBN Consulting’)  
5. The amount of invoices falls just below approval threshold levels
6. Invoices numbers from vendors occur in an unbroken consecutive sequence

Kickbacks -

1. Purchasing agent or other high level manager handles all matters related to a vendor even though this level of attention might be outside or below his or her normal duties
2. Vendors who receive an inordinate amount of business for no apparent business reason
3. Prices from a particular vendor are unreasonably high when compared to others, and/or quality of goods or services received from a vendor is low
4. Tips or complaints from other employees or honest vendors
5. Key contracts awarded with no formal bid process
6. Purchase of excess goods
CASE EXAMPLES: FICTITIOUS / MANIPULATED VENDORS

1. Charity Adams + Two = $540,000
2. Data Cable Connection
3. Elevator / Escalator Maintenance
4. The Controller Case

GARY MECHANICAL SERVICES
68 Stamford Ct.
Gary, IN 46402
(800) 555-9876

September 1, 2014

Your Company
Attn: Accounts Payable
200 N. Main St.
Naperville, IL 60791

Invoice For Services Rendered

For work performed on HVAC system
Month of August, as follows:

1. Feasibility analysis, per July 10 quote  $22,600
2. Engineering services with regard to seating of hypolosatic ventilator  33,925
3. Design services for hypolastic ventilator identification system and dry well  37,200

Total Due  $95,725

Due upon receipt
CASE STUDY: THE CONTROLLER

Company Background

• Manufacturing
• $2.5 billion in sales
• Publicly traded
• 8,500 employees
• Over 75 US plants

What Happened

• $3.5 million taken over seven years
• 3 primary parts:
  a) Payments to janitorial company owned by the controller and his wife
  b) Work on two homes and a vacation condo
  c) Gift cards from a national warehouse club retailer
• Month end journal entries were routinely used to move costs
• Plant financial performance deteriorated over the life of the scheme

Who Did It

• 63 year old controller
• Male, married with grandchildren
• Poor health
• Approaching retirement
• Marginal performer
• 25 year employee at time scheme started
• Had ability to initiate, approve and code transactions
• Month-end authority allowed moving costs by journal entry
• Lifestyle issues were well-known

Symptoms, Red Flags and Indicators

• Missing documents
• Unqualified accounting assistant
• Poor plant financial performance
• Cash advances
• Large budget variances
• Journal entries
• Missed closing deadlines
• Known related party
• Dramatic change in lifestyle
• Unusual behavior
FRAUD EXPOSURES IN PROCUREMENT AND CONTRACTING

1. Bid rigging, price fixing, collusion and other Shadow Deals:
   a) European marketing rep
   b) The Crawford Case
   c) Vatican property management

2. Material or skills substitution:
   a) Consulting, legal, and public accounting ‘field promotions’

3. Alternate methods employed:
   a) Shotcrete v. formed and poured
   b) PVC v. copper

4. Excess hours, materials or other measures on T&M contracts:
   a) Data cable installation
   b) Bovis Lend Lease

5. Buyouts on subcontracted work and suppliers:
   a) Disclosed v. undisclosed savings

6. Defective pricing:
   a) Equipment rental
   b) Change order pricing

7. Cost Accounting exposures:
   a) Labor and related burden (The Wisconsin Contractor)
      • Labor rates
      • Payroll taxes
      • Insurance and other charges
      • Methodology and/or application “errors”
   b) Non-reimbursable costs (Hockey and fishing trips)
   c) General conditions
   d) Falsification of records

8. Your examples and lessons learned
DETECTION SUGGESTIONS – PROCUREMENT & CONTRACTING

1. Analyze bids, looking for patterns by vendor or purchasing agent
2. Confirm losing bids and failure to respond to bids and Requests for Quotations
3. Audit vendors – transaction records, T&E, 1099’s
4. Surprise count and inspect at receiving points
5. Match PO, proof of receipt, and invoice
6. Observe inventory held by others
7. Observe highly tempting items
8. For sole source vendors, confirm existence, prove ownership, test prices, find other sources, and analyze usage volumes. Verify sole source justification
9. Reconcile inventory, purchases and usage of items subject to pilferage
10. Audit rental of equipment, including equipment rental used by contractors
11. Verify accuracy of items that must be stored in containers (gases, liquids, other)
12. Audit purchases that do not go through normal purchasing procedures
13. Audit maintenance agreements
14. Audit property management agreements
15. Audit costs on cost-plus agreements to original documentation. Look for creative interpretations of the term “cost” by vendors or contractors
16. Pull D&B reports and enter vendor names into press databases
17. Use computer to look for multiple PO and split bills
18. Confirm delivery locations
19. Verify address and other master file changes by vendor
TECHNOLOGY CONCERNS AND CYBER-FRAUD

1. Access – unauthorized transactions
2. Sabotage, including viruses
3. Theft of data, including research
4. Funds movement
5. Fraud by IT contractors, including consultants
6. Misrepresentation in selling of equipment and software
7. The Internet
8. Counterfeiting of securities, checks, currency and other documents
9. Program changes for personal gain
10. Direct file changes
11. Spreadsheet validity
12. Software piracy
13. Theft of computer equipment

DISCUSSION QUESTION

High impact auditors use computerized analysis techniques to look for symptoms of fraud occurrence in large quantities of data. In addition, some set up audit routines to run periodically or be integrated into normal processing. Any activity that satisfies the predetermined criteria will be flagged for audit attention.

If your had unlimited resources and your entire annual salary was dependent on finding one new significant fraud scheme – but you had to use computer data retrieval and analysis techniques to find it – where would you look and how would you design computer-based test to find it?
FRAUD AND TECHNOLOGY RISKS: LARGER PICTURE

“SECURITY EFFORTS FOUND LAX AMID LAX COMPLIANCE”

The best IT security policies are only effective if employees abide by them, and these days that can be a big “if.” More than half (53%) of employees in a recent international survey said they work around their company’s IT security policies to get work done.

Other findings included:

• 64% frequently or sometimes send work documents to their personal e-mail address to work on them from home.

• One in 10 has lost a laptop, smartphone and/or USB flash drive with corporate information on it. For U.S. employees, only 5% reported such a loss.

• 43% have switched jobs internally but still have access to accounts and/or resources that they no longer need.

• 37% have stumbled into an area of their corporate network to which they believe they should not have had access.

• 15% have held a door open for someone at work whom they did not recognize. Among U.S. employees, almost one in three (31%) has let a stranger into the workplace.

The survey by RSA, the security division of EMC Corp., polled more than 400 attendees at industry conferences in the United States, Mexico and Brazil. (Source: EMC Corp., The 2008 Insider Threat Survey, www.emc.com.)

DISCUSSION QUESTION

Assuming the human ‘soft control’ technology risks outlined above exist within your organization, what specific steps could your department take in the next six months to help your leaders and staff reduce this risk?
COOKING THE FINANCIAL BOOKS

1. REVENUE RECOGNITION

*Recording fictitious sales to nonexistent customers and recording phony sales to legitimate customers* – These schemes normally occur near the end of an accounting period and may involve the issuing of some form de facto reversal of the sale soon after the end of the accounting period.

*Recording revenue on transactions that do not meet the revenue recognition criteria* – may include transactions where right of return exists, “bill-and-hold” transactions, accelerated “percentage-of-completion” recognition, and transactions where the earnings process is not complete.

*Recognizing revenue in the wrong period* – most common is recognition of revenue on anticipated future sales. Often involves altering dates on shipping documents or keeping the records open until the shipment has occurred.

2. OVERVALUED ASSETS

Overvaluing assets is a relatively simple way to directly manipulate reported financial results, since overstated assets usually result in understated expenses. Common schemes for reporting overvalued assets include:

a) Inflating the value or quantity of inventory on the balance sheet (PharMor)
b) Capitalization of costs that should have been expensed (WorldCom)
c) Including non-business assets on the balance sheet (boats and exotic cars)
d) Failure to recognize impairment losses on long-lived assets

3. UNDERREPORTED LIABILITIES

a) Recognition of assets without related ‘liability effect’ (Enron)
b) Understating accounts payable by recording purchases in subsequent accounting periods, overstating purchase returns, or falsifying documents that make it appear that liabilities have been paid off
c) Failure to record all debt or other liabilities, or recognize contingent liabilities
d) Underreporting future obligations such as warranty costs

4. HOW AUDITORS WERE FOOLED: LESSONS FROM FAMOUS CASES

a) ZZZZ Best
b) Peregrine Financial Group
COOKING OTHER RESULTS

1. School district cheating
2. Side effects from drugs
3. Family Connections

The Christian Science Monitor - CSMonitor.com

America's biggest teacher and principal cheating scandal unfolds in Atlanta

At least 178 teachers and principals in Atlanta Public Schools cheated to raise student scores on high-stakes standardized tests, according to a report from the Georgia Bureau of Investigation.

In February 2009, Atlanta Superintendent Beverly Hall was named 2009 Superintendent of the Year in San Francisco. Ms. Hall stepped down from her post on June 30, days before the release of a report that documented widespread cheating by teachers and administrators in the 55,000-student Atlanta Public School District.

(Paul Sakuma / AP / File)

By Patrik Jonsson, Staff writer / July 5, 2011 at 5:37 pm EDT

Atlanta

Award-winning gains by Atlanta students were based on widespread cheating by 178 named teachers and principals, said Georgia Gov. Nathan Deal on Tuesday. His office released a report from the Georgia Bureau of Investigation that names 178 teachers and principals – 82 of whom confessed – in what’s likely the biggest cheating scandal in US history.

This appears to be the largest of dozens of major cheating scandals, unearthed across the country. The allegations point an ongoing problem for US education, which has developed an ever-increasing dependence on standardized tests.

The report on the Atlanta Public Schools, released Tuesday, indicates a
CASE STUDY: FAMILY CONNECTIONS

Background Information

- $3.1 million Austin Texas based non-profit
- Created in 2004 as merger of two non-profits
- Early childhood education and support
- Served 32,000 children and adults
- Parenting classes, mental health counseling for mothers, child care referrals, health education classes
- 30 full-time employees
- 11 member board of directors

Executive Director:

- 51 years old
- 1982 accused of writing fraudulent check to retailer
- 1987 convicted of theft – 4 year sentence, served 4 months
- 1990 while on probation, hired into finance department of nonprofit agency
- Handled billing, invoices and payments
- 1992 filed for bankruptcy
- 1994 promoted to executive director
- 2004 appointed executive director of merged non-profits that became Family Connections

Allegations:

- Theft over $327,000 to private bank accounts from 2004 to 2009 (including $33,000 from Dec 2009 thru Feb 2010)
- In 2004 wrote $80,000 in checks to EAC
- Paid personal car loan from organization funds
- Paid $150,000 of personal mortgage
- Falsified financial audits and filed with government agencies and others
- Kept all financial records on a thumb drive
- $130,000 taken from Texas Association of Child Care Resources – volunteer Treasurer for 10 years
- $8,000 taken from Hyde Park Christian Church

Inflated Results:

- Resource library helped 6,500 families – actual closer to 3,700
- Child care locating services 3,500 families – actual 860
- Parenting classes for 2,300 – actual 1,000
DISCUSSION QUESTIONS

1. The Controller, Peregrine Financial, Atlanta School District and Family Connections cases all involved high-level managers taking advantage of their authority to override controls. What should we do during the planning and performance phases of our projects to take into account the possibility of management override to commit and conceal fraud? Be specific.

2. One difficult fraud exposure involves override by top executives and fraud for the benefit of the organization. Have you encountered any instances of senior manager or executive override to commit fraud? Provide details of what happened and how it was discovered.

Describe challenges faced by the investigative team.

3. Another macro fraud risk involves fraud committed for the benefit of the organization. Examples include a pattern of manipulating high-level financial or operating results, misleading government agencies, misrepresenting the capabilities of products or services sold, and similar events.

Have you encountered any instances of fraud for the benefit of the organization? To the extent you can, provide details of what happened and how it was discovered.

Describe challenges faced by the client engagement team.

4. Most auditors would agree that we should detect material management fraud in the organizations we audit. After all, if the fraud is big enough to be material, it should be big enough to detect. But what about management fraud that does not hit the standard of “materiality”? The one that happens all too frequently – and is “material” to the manager’s compensation.

Should external auditors be responsible for detection of such “immaterial” financial or other results reporting fraud?
EXAMPLE INDICATORS OF FRAUD

1. Conflicting or missing evidential matter, including:
   a. Missing or inadequate documentation
   b. Unavailability of other than photocopied documents when documents in original form are expected to exist
   c. Significant unexplained items on reconciliations
   d. Inconsistent, vague, or implausible responses from inquiries or procedures
   e. Discrepancies between the entity’s records and the records of third parties
   f. Missing assets, including inventory

2. Discrepancies in the accounting records, including:
   a. Transactions not recorded in a complete or timely manner or improperly recorded as to amount, accounting period, classification or entity policy
   b. Unsupported or unauthorized balances or transactions
   c. Last-minute adjustments by the entity that significantly affect financial results

3. Disbursements:
   a. Photocopied invoices or invoices that have been altered
   b. Invoice numbers that occur in an unbroken consecutive sequence
   c. Invoices with the same address and/or phone number as employees
   d. Amounts of invoices fall just below the threshold for review
   e. Multiple companies have the same address and phone number
   f. Missing checks or checks out of sequence
   g. Large, unexplained reconciling items
   h. Unusual endorsements on checks
   i. Bank statement pages that have been cut, altered, and then photocopied
   j. Disbursements are unsupported by invoices or other documentation
   k. Checks presented for payment which were not issued

4. Complaints from:
   a. Customers
   b. Vendors
   c. Competitors
   d. The public
   e. Bid losers
   f. Former employees
   g. Former suppliers
Example Indicators of Fraud
(continued)

5. Revenue recognition and income management:
   a. Credit adjustments to receivables after the end of the accounting period
   b. Cancellations of orders after the end of an accounting period
   c. Unusual entries to the accounts receivable sub-ledger or sales journal
   d. A lack of cash flow from operating activities when income from operating activities has been reported
   e. Sales to customers in the last month before the end of an accounting period at terms more favorable than previous months
   f. Sales with affiliates and related parties
   g. Pre-dated and post-dated transactions
   h. Journal entries made directly to the sales or revenue account
   i. Cookie jars
   j. Big bath charges

6. Kickbacks:
   a. Employee handles all matters related to a vendor even though it might be outside or below his or her normal duties
   b. Vendors with an inordinate business volume for no apparent reason
   c. Vendor representatives make frequent, unexplained visits
   d. Prices from a vendor are unreasonably high when compared to others
   e. Quality of goods or services received from a vendor is low
   f. Tips or complaints from other employees or honest vendors
   g. Key contracts awarded with no formal bid process
   h. Purchase of excess goods

7. Anything physically impossible:
   a. Overtime
   b. Quantities stored / used
   c. Credits in accounts where no sale or in excess of transaction amounts

8. Other indicators:
   a. Duplicates, variances, overrides, adjustments
   b. Ghosts and other unauthorized personnel on the payroll
   c. Cash shortages and cash overages
   d. No proceeds from accounts sent out for collection
   e. No proceeds from the disposition of assets
OBJECTIVES OF INVESTIGATIONS

1. Discover the truth (and the deception)
2. Protect innocent parties
3. Document the facts
4. Provide a foundation for removal of wrongdoers
5. Support action by the authorities
6. Support recovery of losses
7. Protect the organization
8. Protect the auditors / investigators
9. Identify and correct any weakness exploited

BARRIERS TO EFFECTIVE INVESTIGATIONS

1. Failure to recognize fraud as fraud
2. Management commitment and doubt
3. Some attorneys
4. Some human resources leaders
5. Fear of litigation (both legitimate and anecdotal)
6. Labor relations
7. Suspect knows of other fraud (especially fraud for the organization)
8. Suspect is a top performer
9. Suspect is politically protected
10. Fear of violence
11. Uncertainty or conflict over responsibility for investigation
INVESTIGATION MANAGEMENT

1. Investigation is not for everyone. There are inherent risks, and things can go wrong despite best efforts. The auditor or examiner may be lied to, attacked as to qualifications and professionalism, and subject to intense scrutiny.

2. Don’t investigate without a policy. Make sure of your authority and the limits of that authority. Ask: “What will the organization do if I’m sued?” And get a solid answer – preferably in writing. The auditor or examiner is not a deep pocket. But a tactical suit may be aimed at discrediting the individual who performed the work – and thereby weakening the conclusions in the eyes of others.

3. Do not do anything that is unauthorized or illegal.

4. There should be clear policy on when to report to law enforcement or other governmental authorities.

5. Each fraud incident is unique. Although there are many similarities in fraud cases, there is nothing completely identical from one investigation to another. The actual scope, methodology and strategy in each investigation will vary. However, there are efficiency opportunities from building lists of helpful investigative practices.

   a) Develop a *Fraud Investigation Checklist*. It should include typical steps to be performed and sources of information.

   b) Consider developing an *Investigative Resource Guide*. Keep track of the types of information needed during an investigation and the sources used to find it. Use the Guide as a tool on investigations and keep it current.

6. Case Reports for Executive Management:

   a) Speak to intent: Was it an error or on purpose
   b) Who did it? Who else was involved?
   c) Extent of the loss
   d) Recovery potential or status
   e) How it was done and the internal control implications

7. Reports for law enforcement and insurance companies:

   a) Sequence of events
   b) Relevant company policies and procedures
   c) Copies of documents
   d) Reference review by counsel
   e) Exclude internal control implications?
INVESTIGATIVE TECHNIQUES

1. Interviews
   a) Listening is the key
   b) Gather background information
   c) Information needs to be confirmed
   d) Scripted questions v. free flow discussion
   e) High attention

2. Transaction / document analysis
   a) Patterns
   b) Information flow
   c) Alterations, erasures, phony signatures
   d) Expert analysis
   e) Low attention

3. Informants
   a) Look for motivation
   b) Some are involved
   c) Most resist active involvement in the investigation

4. Observation
   a) Limited for internal audit (loading dock, etc.)

5. Public records and database search
   a) Background information
   b) May lead to other sources and expand scope & depth
   c) Related party transactions
   d) Hidden assets

6. Undercover operations
   a) Limited for internal audit
   b) Pretext call
   c) Sting
TRAVEL EXPENSES INTERVIEW

You have been asked by your supervisor to interview a mid-level manager about certain apparent discrepancies in that manager’s expense reports over the past three months. This manager is a 25-year employee. They routinely travel throughout the US, Canada and Europe as part of their responsibilities.

The request occurred because a reviewer in the Travel Accounting area noticed what they described as “unusual activity over several months, including both charges and credits, on the employee’s company credit card.”

You were asked to interview the manager to gain additional information merely because you happened to be in the second week of a three-week audit at the same location where the subject manager has their office. Copies of the related expense reports and support were emailed to you this morning, and your quick review leads you to believe that the questions are legitimate. For example, you notice that explanations for dinners routinely indicate only “business dinner” as the purpose of a meal, entertainment expenses while traveling appear to be excessive, and cash expenditures for taxis, meals and other cash items seem high for the locations visited.

DISCUSSION QUESTIONS

1. List two things that you should consider as you plan this interview.
   a) 
   b) 

2. List two things that could go wrong during this interview.
   a) 
   b)
FRAUD BASED INTERVIEWS

Most people we interview believe telling the truth is the morally right thing to do.

We have all learned the lying successfully allows us to avoid punishment.

INTERVIEW PREPARATION:

1. Background information
2. Time Lines, Flowcharts and Relationship Charts
3. Use a script?
4. Creating a record of the interview
5. Include a witness?
6. Reluctance on the part of the interviewee
   - Time demands
   - Fear or disapproval
   - Etiquette
   - Memory
   - Repression
7. Denial of access to records
   - My boss told me not to let anyone see this
   - Privacy laws won’t allow access
   - Overhead costs are trade secrets
   - The contract is lump sum. You have no authority to see our costs
   - I need to see your authority in writing
8. Written confirmation
9. Location and room arrangements
10. Remember: people lie, embellish, bend and shade the truth
SIGNS OF POSSIBLE DECEPTION

1. Establish a Baseline or “Behavioral Norm” – both Physical and Verbal
2. Ask background questions that result in truthful responses
3. Probe short and long term memory
4. Ask questions that require creative responses
5. Look for behaviors that do not make sense with the words spoken
6. Look for gross body movements, and analyze in relation to what was just said

NONVERBAL

Nonverbal behavior will either support and enhance the credibility of an answer, or suggest discomfort and possible deception – indicating the need for follow-up questions.

- Change in pattern of eye contact
- Increased breathing rate, perspiration, or swallowing
- Change in coloring or facial tone
- Posture becomes closed, stiff or otherwise defensive
- Movement away from the interviewer
- Reluctance to physically handle documents or other evidence presented
- Passive reaction to direct accusation
- Grooming Gestures and Physical Adjustments
  - Rubbing or wringing of hands
  - Picking at fingers, hands or nails
  - Touching the nose, ears, mouth or hair
  - Adjusting or cleaning glasses
  - Picking lint from clothing and similar gestures
  - Change in patterns of movement of feet
Possible Signs of Deception
(continued)

VERBAL

• Denial confined only to **specific** aspects of the issue
• Delayed, evasive, or vague answers
• Qualifies answers
• Uses reinforcements in answers
• Answers given in fragmented or incomplete sentences
• Mixture of unusually poor and exact memory
• Answers consistently lack detail
• Answers start with repeating the question
• Answers start with a request that the question be repeated
• Mental blocks exhibited: “The liar has to remember the lie.”
• Throat clearing or coughing
• Mumbling
• Swearing, oaths, or various religious statements
• Inappropriate laughter
• Passive or weak denial

*Does the subject’s response provide a definitive answer to your question?*

*If not, follow up!*
ROSLYN UNION FREE SCHOOL DISTRICT

Background Information

a. Five square miles
b. 5 schools (1 pre-school, 2 elementary, 1 middle, 1 high school)
c. 3,300 students
d. Class size – 20 to 25
e. Graduation Rate 95%
f. 610 employees
g. 325 Teachers and administrators
h. Budget -- $69.4 million ($21,000 per student)
i. Initial fraud estimate -- $11 million ($3,300 per student)
j. 1996 to 2004

Weaknesses from Roslyn:

a. Insufficient policies and procedures
b. Management override of existing controls
c. Ineffective budget to actual variance analysis
d. Inadequate stewardship, oversight and review
e. IT not locked down
f. Ineffective Internal Audit
g. No segregation of transaction:
   ▪ Initiation
   ▪ Approval
   ▪ Recording

Indicators from Roslyn:

a. Cash advance activity
b. “Hand Drawn Warrants”
c. Unusual payments (geography and type)
d. Budget variances
e. Budget transfers
f. Change of payee in payments system after checks issued
g. Gaps in check sequence
h. Unreasonable payroll
i. Tips
j. Unusual behavior
FRAUD PREVENTION BLUEPRINT

1. Anti-Fraud Internal Control Infrastructure

Fraud exposures are identified and specific control procedures are developed, implemented and maintained to both prevent these events from happening and to detect them should they occur.

2. Acceptable and Unacceptable Behavior is Defined and Communicated

Employees, vendors, contractors and others all need to know what is allowed in daily behavior. And just as important, what is considered misconduct. Employees and managers must know the rules for reporting financial and other results. Vendors, contractors and other third parties must know your restrictions on gifts and entertainment and penalties for violations. Make your “Code of Conduct” part of any agreements with third parties.

3. Leaders at All Levels Set a Great Example – Every Day

For years the phrase “tone at the top” has been used to focus on the statements, business practices and personal behavior of executives and other senior management members. But a ‘leader’ includes anyone we look to for an indication of proper behavior. That includes everyone from first level supervisors in the field right up to the Board. Require outstanding personal example. And counsel all who don’t act properly.

4. Issue a Policy on Suspected Misconduct

All organizations face the risk of wrongdoing and fraud. To effectively manage those risks, everyone should know what their responsibilities are in this important area. An effective “Policy on Suspected Misconduct” is the perfect place to document these responsibilities. Employees and managers will have a one-stop source explaining their role in deterrence, early detection and effective incident response.

5. Require Reporting of Suspected Violations by Others

Codes of Conduct and other behavior policies should require reporting. Periodic sign off is a good way to track awareness and minimize “I didn’t know” situations. Make the reporting of violations mandatory. Add a sign-off where managers and employees acknowledge that they are not aware of violations by others.
6. Identify, Quantify and Track Losses

Few organizations have taken the time to develop a complete list of their existing fraud loss areas. Begin by listing areas where losses have occurred in the past. Then research these areas and assign ranges of probable current loss levels. Normally this list will total no less than one percent of revenue.

7. Comprehensive Fraud Exposure Analysis

Position by position, department by department, ask the question “What could go wrong?” Create a robust inventory of fraud risks. Use this list to provide training for new employees and supervisors. Develop offsetting prevention and early detection procedures for each risk identified. Publicize the effort and the results. Create awareness in honest employees, and fear in those tempted to commit wrongdoing.

8. Fraud Skills Training

Sponsor or conduct fraud awareness and skills training programs addressing what employees and auditors need to know to prevent, detect and handle fraud. Most employees have never been taught the skills needed to be effective in this area. This skills gap allows fraud to occur and go undetected.

9. Auditors and Employees Look For Fraud

Auditors and employees look for fraud symptoms in information they see each day. Managers and employees are aware of and monitor for fraud indicators in documents they handle and approve, in operations and exception reports, and in behavior. Auditors brainstorm fraud risks on every project, link fraud risks to specific audit procedures, and carry out fraud detection steps during their testing and interviews.

10. Fraud Response in Place

Identify the skills and relationships that will be needed when fraud is detected, and assemble the team in advance. Craft the message you want to deliver to employees, customers, the press and others. Know who will be authorized to investigate, handle requests for information, and interface with any outside parties.
SUGGESTED BEST PRACTICES

1. Brainstorm fraud risks – Think like a thief.

2. Teach organization employees what they need to know to be more effective.

3. Where appropriate look for fraud indicators. Conduct discovery based tests.

4. When gathering information and in interviews, utilize a “Show me how you...” rather than a “Do you...” approach.

5. When in doubt, doubt.

6. Refer or resolve all suspicions.

7. Read:
   a) Switch, by Chip Heath and Dan Heath
   b) Influence, by Robert Cialdini
   c) Nudge, by Richard Thaler and Cass Sunstein

8. Sponsor a Major Fraud Initiative (based on The Anti-Fraud Toolkit)
   ✓ Chief executive commitment
     • Timely detection of wrongdoing
     • Effective response to suspected wrongdoing
     • Practical prevention
     • Avoiding problems in the first place
   ✓ Organizational assessment of the environment
   ✓ Development of a tailored fraud awareness program for executives, managers and supervisors
   ✓ Presentation of concepts to chief executive
   ✓ Executive overview presentation, with kickoff by chief executive
   ✓ Presentation of program to managers and supervisors in groups of 25 to 30
   ✓ Ongoing reinforcement
   ✓ Tracking and publication of participant results