CONDUCTING HOTLINE AND FRAUD INVESTIGATIONS

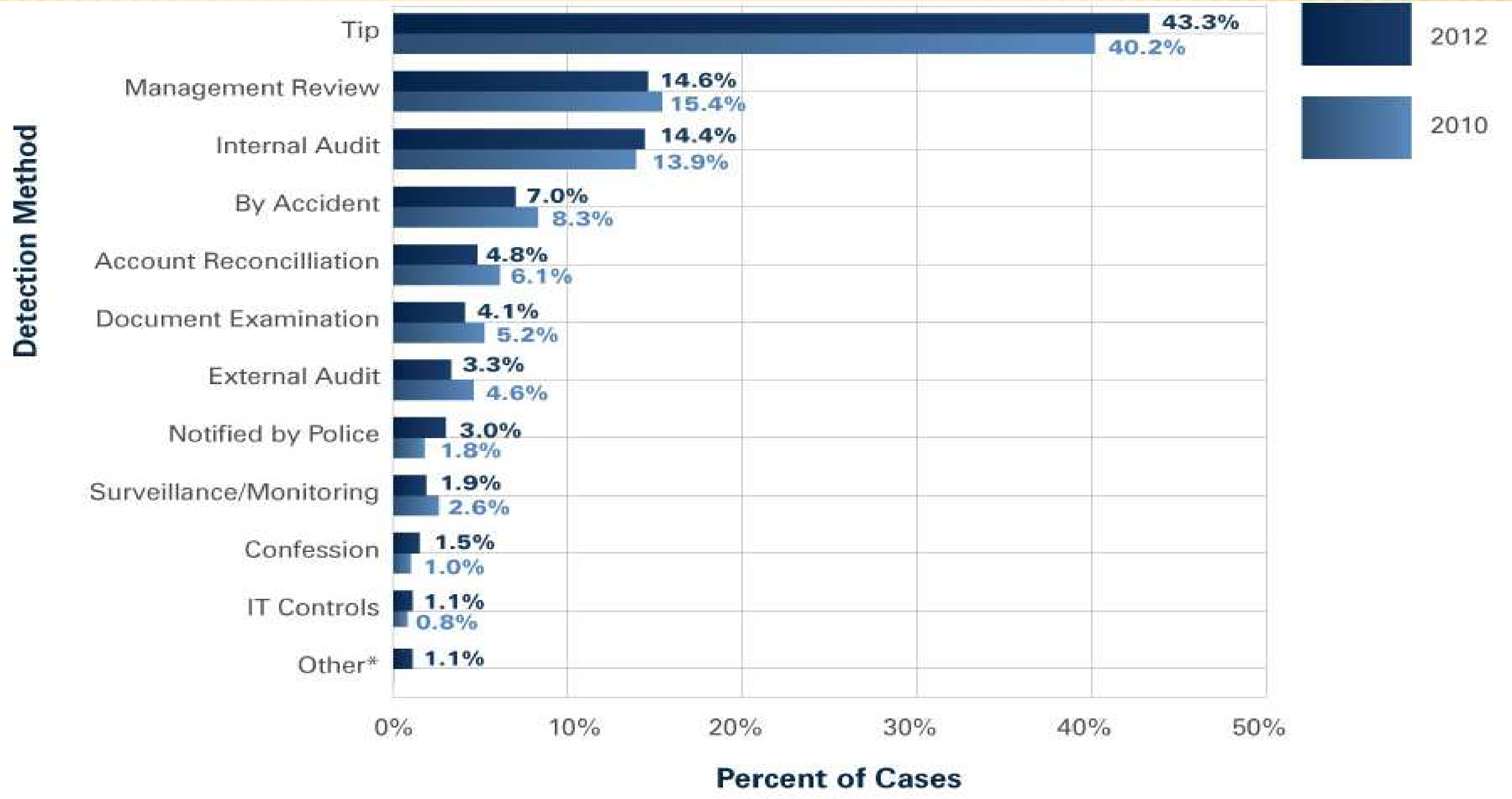
INTRODUCTION

Most organizations worldwide are vulnerable to fraud and misconduct in the workplace. By establishing a proactive approach and engaging stakeholders to promote an ethical workplace, an organization can significantly limit financial liability and loss, and protect its corporate hard image in the market place. A successful strategic approach undertaken by many organizations is the implementation of an anonymous employee whistle blowing line.

The impact of fraud is costly to organizations, shareholders and consumers alike. According to the Association of Certified Fraud Examiners' (ACFE) 2008 *Report to the Nation on Occupational Fraud & Abuse,* it is estimated that U.S. organizations will lose 7 percent of their annual revenues to fraud. Based on 2008 figures, that translates to $994 billion in fraud losses.

DETECTION OF FRAUD SCHEMES - THE REALITY

Initial Detection of Occupational Frauds



WHISTLE BLOWING AND CORPORATE GOVERNANCE

There is a strong tie between employees reporting misconduct in the workplace and a company’s ethics programmes.

WHISTLE BLOWING AND CORPORATE GOVERNANCE

Employees tend to prefer an anonymous telephone whistle blowing line because they have more confidence that they can remain anonymous. They often fear that electronic communication can be traced back to them. This fear can cause them to either not report their concern, or worse, report it to a source outside of the organization.

INTERNAL VS. INDEPENDENT WHISTLE BLOWING LINES

Some organizations provide an internally managed whistle blowing line as an option for employees who are uncomfortable discussing issues face-to-face. Reports to the whistle blowing line are frequently routed to an employee somewhere in the organization, generally in Human Resources, Legal or the Ethics office.

An internal programme may seem attractive, but there are some serious potential drawbacks.

For instance, if employees realize they are calling an internal number, they may be afraid that their identity could be traced and decide not to submit the report. There are also operational issues, such as the potential for inconsistent handling of sensitive information and callers encountering voicemail. An internal whistle blowing line also leaves the organization vulnerable to charges of covering up issues involving management.

INTERNAL VS. INDEPENDENT WHISTLE BLOWING LINES

In comparison, an independent external process provides greater safeguards of anonymity and avoids even the appearance of impropriety. An external facility is also more attractive to use from home or another location outside the office, as there is less fear of detection. It is also important to evaluate what happens on the back end of the whistle blowing line.

While there are costs associated with an external whistle blowing line, the financial investment is small

compared to the potentially disastrous financial repercussions associated with malfeasance that could go

undiscovered. With the expertise, trained personnel, resources and technology already established to

operate a whistle blowing line and conduct quality assurance, a professional whistle blowing line provider

can usually provide these services for much less than it costs to implement them internally.

WHISTLE BLOWING MUST BE SUPPORTED BY CORPORATE CULTURE

Communicating the purpose of the whistle blowing line should ideally help create and maintain an ethical culture in the workplace. A communications team that includes top management should be involved in developing an ongoing ethics communication campaign.

An ethics communication campaign is essentially an internal marketing campaign that seeks to inspire certain behaviour within an audience, from the top down.

As with any such campaign, the first step is to determine desired behaviours and the key messages that will help motivate these behaviours.

After Implementing a hotline what next

FRAUD INVESTIAGTION

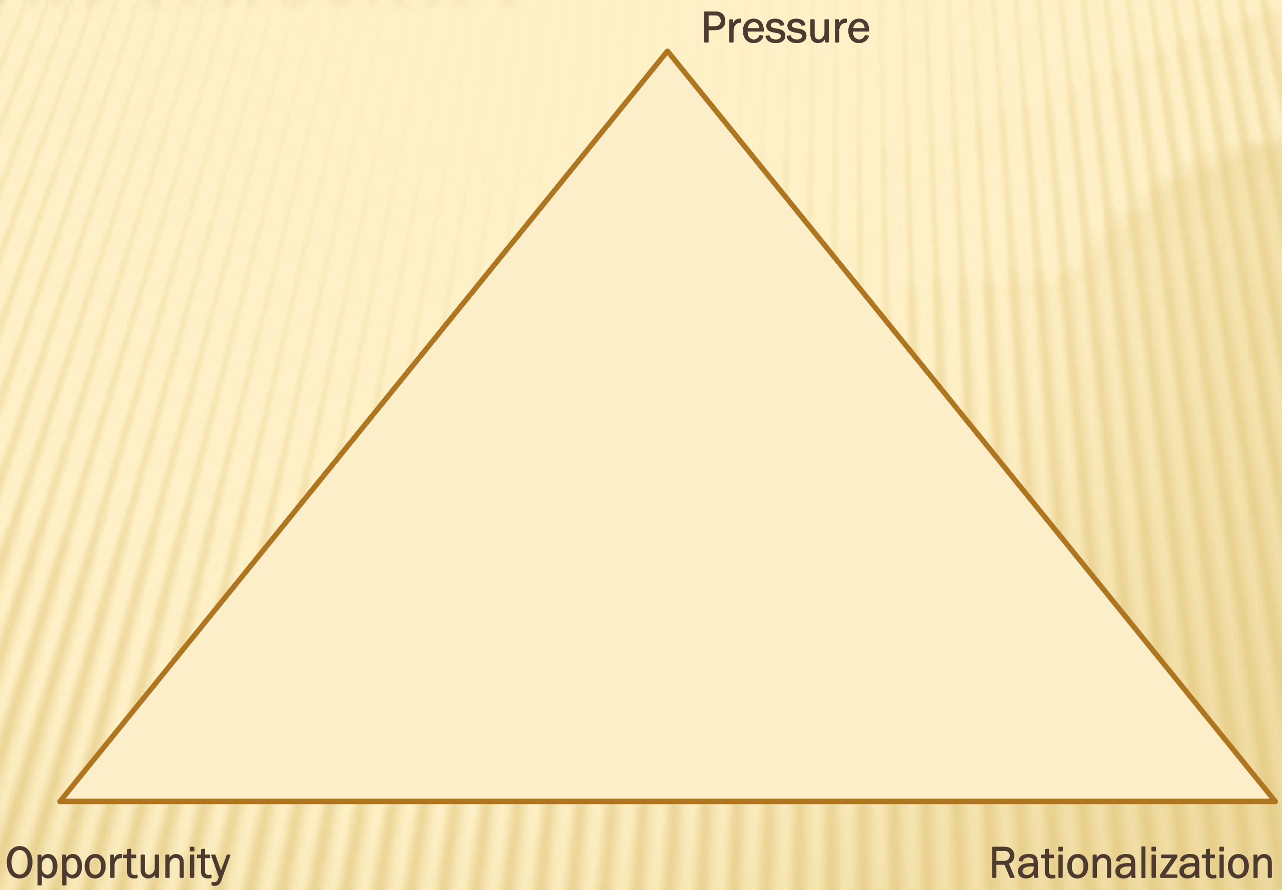
FRAUD

Fraud is generally defined in the law as an intentional misrepresentation of a material existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes other statements misleading.

WHY FRAUD OCCURS

The Fraud Triangle

FRAUD TRIANGLE



Pressure

- Opportunity

Rationalization

The theory of fraud triangle by Dr. Donald R Cressey

FRAUD TRIANGLE - EXPLAINED

Pressure

Pressure is what causes a person to commit fraud. Pressure can include almost anything including medical bills, expensive tastes, addiction problems, etc. Most of the time, pressure comes from a significant financial need/problem.

Often this need/problem is non-sharable in the eyes of the fraudster. That is, the person believes, for whatever reason, that their problem must be solved in secret. However, some frauds are committed simply out of greed alone.

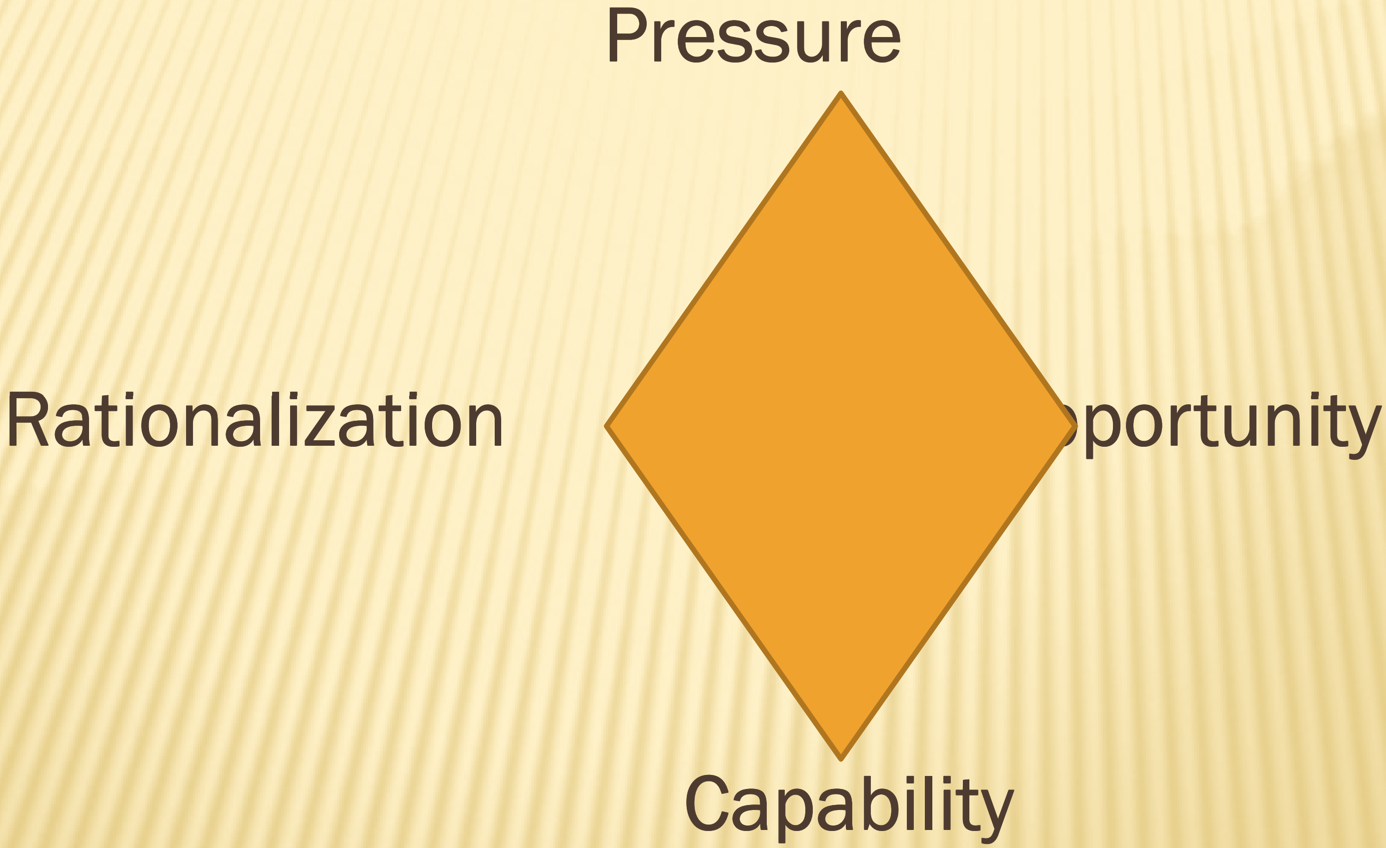
FRAUD TRIANGLE - EXPLAINED

Rationalization

Rationalization is a crucial component in most frauds. Rationalization involves a person reconciling his/her behavior (stealing) with the commonly accepted notions of decency and trust. Some common rationalizations for committing fraud are:

- The person believes committing fraud is justified to save a family member or loved one.
- The person believes they will lose everything – family, home, car, etc if they don't take the money.
- The person believes that no help is available from outside.
- The person labels the theft as "borrowing", and fully intends to pay the stolen money back at some point.
- The person, because of job dissatisfaction (salaries, job environment, treatment by managers, etc), believes that something is owed to him/her.
- The person is unable to understand or does not care about the consequence of their actions or of accepted notions of decency and trust.

THE FRAUD DIAMOND



Developed by David T Wolfe and Dana R Hermanson

THE FRAUD DIAMOND

Capability

Capability refers to the personal traits and ability of persons that enable them to perpetrate fraud, beyond the environmental or situational factors of opportunity, rationalization and pressure.

- A person’s knowledge of the policies, procedures and controls of the business and, in particular, of the weaknesses there in.
- Involvement in and influence over key relationships, either
  - Internal relationships within the business, or
  - External relationships with third parties
- The necessary psychological traits to commit fraud e.g. self confidence, egotism, etc.

- Essentially, you would have to look for warning signs in unusual places…….

THE INSTRUCTION .....

- “The world is a dangerous place to live;
Not because of people who are evil,
But because of the people who don’t
do anything about it” Albert Einstein

Albert Einstein

ON FRAUD AND CORRUPTION LEARN………….

"Those who profit are the ones at the top. They keep the doughnut for themselves and give the hole to the people."

Alexander Ivanovich Lebed
Russian Lieutenant-General and Politician

FRAUD INVESTIGATION

Digital Forensic Investigation

DIGITAL FORENSIC INVESTIGATION

Definition: establishing facts based on digital evidence

Typically refers to investigations of potential or known crime (including fraud).

For today's purposes, the most practical scope of discussion is occupational fraud -intentional misuse of financially related matters of employment for personal gain.

- Differs from other crimes outside the work environment (ex. "romance scams") or that do not result in gain (ex. denial of service) or are not financially related (ex. stealing a password to "spy").

DIGITAL FORENSICS & INTERNAL AUDIT

While roles and responsibilities vary greatly amongst entities, the **overlap between Digital Forensics and Internal Audit is generally:**

- Evidence procedures related to **fraud investigations**
- Identity Theft (**Information Security)**

Several factors challenge Internal Audit's role related to digital forensics:

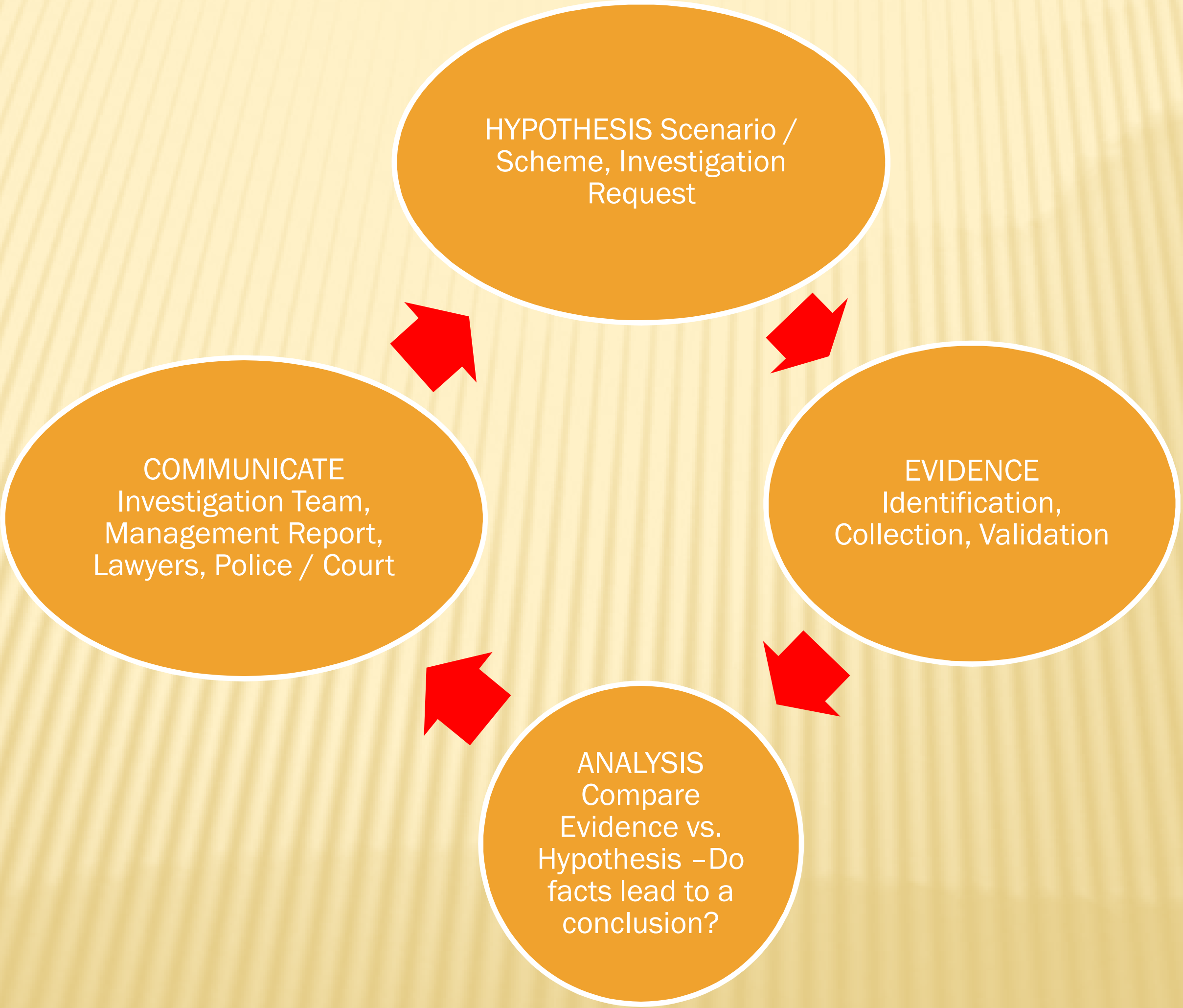
- Trend from street to computer to online to "mobile" crime
- Lack of clear responsibilities related to fraud and forensics
- Senior Management is usually not well-informed on these risks

Internal Auditors should be educated on fraud-related matters:

- 70% of computer-related malicious acts originate within (Gartner 2005)
- 30 –60% of accounts no longer valid in large corporations (IDC)
- "Big Data" & Management's expectations of Internal Audit

Forensic knowledge, tools, and processes should align with entity's risk.

INVESTIGATION PROCESS



HYPOTHESIS Scenario / Scheme, Investigation Request

EVIDENCE Identification, Collection, Validation

ANALYSIS Compare Evidence vs. Hypothesis –Do facts lead to a conclusion?

COMMUNICATE Investigation Team, Management Report, Lawyers, Police / Court

DIGITAL FORENSIC INVESTIGATION TECHNIQUES-INVESTIGATION PROCESS

- The investigative process is iterative.
- Digital forensic techniques can assist in each phase.
- A successful investigation depends on evidence that clearly links from hypothesis to communicated conclusion.

HYPOTHESIS & EVIDENCE IDENTIFICATION

Evidence to be collected and associated techniques depend on how well the hypothesis is initially formed.

Targeting: Known issue & source

- + "Bull's-eye" approach emphasizing facts, evidence preservation, and clear results
- + Consider the cost / benefit

Sourcing: Known issue and unknown source

- + Brainstorm and profile considering facts, schemes, flags, and controls
- + Follow the "cash" and audit trails

Exploring: Determining whether any issue exists Analyze risks top-down and bottom-up, be adventurous and discrete

- ✖ Use CAATs to assess risks across populations

If litigation is a possibility, start documenting evidence chain and custody.

Consult with internal & external experts if your task is greater than your means.

EVIDENCE COLLECTION -HARDWARE

Acquiring data from hardware may require different methods depending on data state and the many possible storage forms.

- Computer Media: drives, RAM, CDs, DVDs, flash drives
- Mobile devices: phones, PDAs, iPods, GPS
- Network Infrastructure: printers, servers, O/S, AD, databases, and logs
- “Cloud”: Apple iCloud & MobileMe, Amazon S3, Google Cloud Storage

Analyze the state of hardware and data before interacting, and never power down hardware before collecting temporarily stored data.

- Ideally hardware should be collected “in-state” and transported to secured, “pristine” environment for analysis.

Acquired hardware requires validation for completeness and accuracy similar to data validation.

EVIDENCE COLLECTION -DATA

- Create a visual diagram to identify, track, and communicate data analysis
- Be sure the source is authoritative / appropriate.
- Validate any data collected or transferred for completeness and accuracy.
- Metadata can serve as audit trail, though may need to be validated / corroborated.
- Deleted data predominantly is not really deleted, though specialized tools may be necessary.

EVIDENCE COLLECTION –BEYOND TECHNOLOGY

- Digital evidence is only one piece of a bigger puzzle, and evidence in total must corroborate.
  - Never forget about the human element. People commit fraud using technology, not technology using people.
- Interviewing, body language, and writing (handwriting, emails, letters, etc.) analysis are there own disciplines for a reason. Expertise should be analyzed and sought out before approaching these topics.
- “Bullseye” –make every effort not to approach the suspected fraudster until sufficient evidence proves the assumption (know when to hold ‘em).

ANALYSIS -BASICS

Basic analysis techniques

- Understand the data context (do your homework)…
  - "Aggregate"–financials, # of employees / locations, hard drive size, # of files / records, etc.
  - Statistical analysis –stratification, classification
- Look for anomalies… mining, regression analysis, gaps, duplicates, Benford's, time period comparisons, unusual transaction attributes, etc.
- Consider lookups / cross-references (especially for shell schemes)
- Carefully consider whether population or sampling analysis is appropriate

- Continuously asses how analysis relates to known facts, profile, etc.
- Conduct analysis with thought of how results may be communicated.
- Analysis should be recorded with the same rigor as evidence collection.

TECHNIQUES ANALYSIS INTERMEDIATE

Designing and executing analysis from the view of the hypothesized fraud scheme / red flags can effectively identify and analyze data. As examples:

Asset Misappropriation Schemes

- Segregation of duties in bank statement receipt and reconciliation
- Rotating duties or mandating vacation for key employees
- Examining all types of transactions just under required review/approval level, and classifying them by employee, vendor, and/or customer
- Reconciling inventory and confirming receivables regularly

TECHNIQUES ANALYSIS INTERMEDIATE

Billing -Shell Vendor Schemes

- Sorting payments by vendor, amount, and invoice number for anomalies to investigate
- Examining charges in largest expense accounts
- Verifying service-only vendors' invoices
- Using CAATs to cross-reference employees' addresses with vendors' addresses

Payroll -Ghost Employee Schemes

- Reconcile employees / SSNs in payroll file with those in human resource (HR) database.
- Rotate duties of handling printed checks or require vacation timed with payroll
- Data mining payroll data for post office box , physical address matches that of another employee (i.e., a "duplicate"), direct deposit account number that matches that of another employee, missing phone number or a phone number that matches either another employee or a work phone, compare dates of paychecks compared to termination dates, employees who have no deductions from paychecks

ANALYSIS ADVANCED

- Establish the fraud scenarios for ongoing/continuous monitoring
  - Build and document understanding around related systems and data
  - Ensure adequate understanding of underlying business, processes and controls
- Document flow and mapping of system architecture, applications, interfaces and data structures
- Build inventory of procedures given scenarios and systems understanding
  - Tools like ACL can retain procedures through logs ors cripts
- Integrate results by communicating to related Internal Audit and other risk management functions

COMMUNICATE

- Evidence has to corroborate each other (fit with the profile, scheme, initial facts, etc.) or be explained as to why it does not corroborate.

- Differentiate facts and opinions, and be transparent with any assumptions.

- Demonstrate how evidence and analysis clearly lead to results.

- Play “devil’s advocate”… If the case goes to trial, anything can be questioned and possibly sway the outcome.

DATA ANALYSIS & SEARCH TOOLS

Wikipedia Listing of Tools: http://en.wikipedia.org/wiki/List_of_digital_forensics_tools

Investigation Processes

- EnCase-data acquisition, analysis / workflow, preservation, & reporting:
  - http://www.guidancesoftware.com/forensic.html
- Symantec & Norton Ghost -disk imaging:
  - http://www.symantec.com/themes/theme.jsp?themeid=ghost
- Paraben–Mobile Forensics:
  - http://www.paraben.com/

Investigation and Data Analysis Platforms

- Sleuth Kit -system / file data acquisition and analysis tool with various O/S and data file interoperability and user-defined C language scripting
  - http://www.sleuthkit.org/index.php
- Picalo-system / file analysis tool with various O/S and data file interoperability, open source (Python*) script community, no record size limit
  - http://www.picalo.org/

DATA ANALYSIS & SEARCH TOOLS

Data Analysis

- ACL -http://www.acl.com/products/
  - Desktop -"traditional" data analysis tool with various file interoperability, built-in analysis functions, and custom-language scripting / automation abilities
  - Exchange -data feeds, functions with custom parameters, documentation acquisition and storage, Microsoft Office integration, and data exception identification and workflow
  - Acerno-Excel Add-In for results analysis

- IDEA -http://www.caseware.com/products/idea: Data analysis tool with various file interoperability, built-in functions, and custom-language scripting / automation
- Active Data/ Active Audit-Excel Add-Ins for data analysis similar to IDEA and ACL

- Search Websites
  - Craigslist / EBay search: http://www.searchtempest.com/
  - Person or Company profiling: http://www.zoominfo.com/
  - Address or Phone search: http://www.zabasearch.com/
  - Social Media search: http://www.kurrently.com/
  - Blog Search: http://technorati.com/

REFERENCES &RESOURCES

- ACFE 2012 Report To The Nation (RTTN) -http://www.acfe.com/rttn.aspx
- PwC 2011 Global Economic Crime Survey (GECS) - http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml.
- Internet Crime Complaint Center (IC3) 2011 Internet Crime Report - http://www.ic3.gov/media/2012/120511.aspx
- PwC 2004 –The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks.
- Mitigating Business Risk –Example of Anti Fraud Framework from the Australian Standard on Fraud and Corruption Control, AS 8001-2003
- Grant Thornton –Managing fraud risk: The audit committee perspective
- Forensic Firms Forensic Strategic http://www.forensicstrategic.com/
- Forensic CPAs -http://www.forensic-cpas.net/index.html
- Financial Forensic & Valuation Group - http://www.ffvgroup.com/index.html

Open Discussion

Questions

reubenborogitahi@gmail.com