Design elements and pictures/content shortened based on copy right-reasons.

Forensic Accounting.
The What, Why and How
Fraud Detection and Prevention

Ulrike Hugl

Nov 16-17_2017

DEEPSEC

DEEPSEC

 ulrike.hugl@uibk.ac.at

1

Background of forensic accounting

- *FA or Forensic Auditing, Forensic Investigation*
- *The Big Five accounting firms + other consulting firms: special departments / services*
- *Teams with diverse skills: accountants, auditors, compliance officers, psychologists, criminologists, lawyers, experts in business intelligence, maths, etc.*
- *Vocational training: Certified Fraud Examiner (CFE) of ACFE ---including code of professional Ethics of ACFE*

2

What is forensic accounting?

*"**Forensic Accountants combine their accounting knowledge with investigative skills**, using this unique combination in litigation support and investigative accounting settings. **Forensic Accountants may be employed by public accounting firms' forensic accounting divisions**, by **firms** specializing in risk consulting and forensic accounting services, or by **lawyers, law enforcement agencies, insurance companies, government organizations, or financial institutions**. Due to society's heightened awareness and growing intolerance of fraudulent activity, **demand for forensic accountants is rapidly increasing**." (ACFE.com)*

"FA includes the use of accounting auditing and investigative skills to assist in legal matters." (Okoye & Gbegi, 2013)

3

Strategic Dimension of FA

- *FA refers to a strategic approach _ gathering and monitoring financial + non-financial information, studied and analyzed for fraud-prevention reasons*
- *standard accountants focuse on balancing books and maintaining records*
- *FAs intensively investigate financial activity for evidence of misconduct*

Source: http://www.oxfordhomestudy.com/forensic-accounting

4

Potential Cases

Money laundering
Insurance claims
Employee fraud investigations (insider threat)
GAAP violations
GAAS violations
Telemarketing fraud
Check kiting
Contract and procurement fraud
Asset misappropriation
Securities fraud
Financial statement fraud
Bankruptcy fraud
Credit card fraud
Embezzlement

Source: http://www.acfe.com/forensic-accountant.aspx

5

External & Internal Role

"Forensic accountants inhabit a cloak and dagger corner of the accounting world. Their job: respond at a moment's notice when a client spots trouble – anything from procurement fraud to a top executive cooking the books to industrial espionage."

– Justin Pope, Associated Press

"You have an external auditor – that's like a guard dog. Maybe a bulldog…" "An internal auditor is a seeing eye dog. A forensic accountant is a bloodhound."

–Dr. Larry Crumbly, editor – "Journal of Forensic Accounting"

(Source: Forensic CPA Society _ fcpas.org)

6

Performance portfolio

Covers exposure / clarification of criminal behavior as well as prevention:
Criminal investigation *(clarification of e.g. corruption, etc.)*
Loss evaluation *(measure of damages)*
Asset tracing *(detection/securing of assets)*
IT-Forensics *(Forensic Data Analysis, Digital Evidence Recovery, Cyber Forensic Investigations, etc.)*
Forensic profiling (e.g. using data mining profiling)
Business intelligence *(background information about persons, projects, dealings, power system, regions/states, etc.)*
Crisis management *(consulting/support in crisis situations in the field of economic crime)*
Litigation support / Dispute Service *(support from lawyers due to preparation/execution of law-suit) or*
Fraud Risk-Management, Fraud Assessment, Fraud-Risk Review *(prevention, analysis of internal corporate control system > detection/elimination of internal lacks > monitoring the internal control system)*

Source: Bitzer et al., 2017, Forensic Accounting, in: Tax Fraud & Forensic Accounting, Springer.

7

Forensic investigation structure

Potential steps:

- *Obtain evidence*
- *Performs analysis on evidence obtained*
- *Report - draw findings*
- *Testify to findings*
- *Assist in prevention of fraud*

Investigations are typically conducted as though litigation will follow (though it may not) > conservation of evidence!

>> Investigation open or hidden

Source: Grant Thornton / Federation of Credit and Financial Professionals; Fundamentals of Forensic Accounting, March 21, 2017, https://www.youtube.com/watch?v=5IoHJfAqc5c

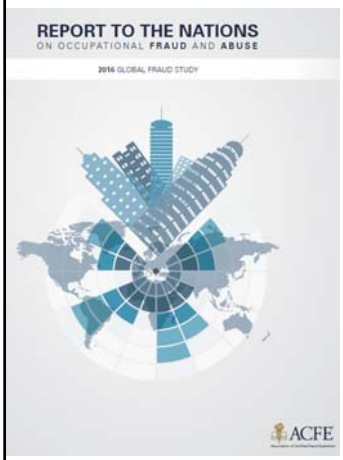
8

Digital forensics investigation

(shortened based on copy right-reasons)

9

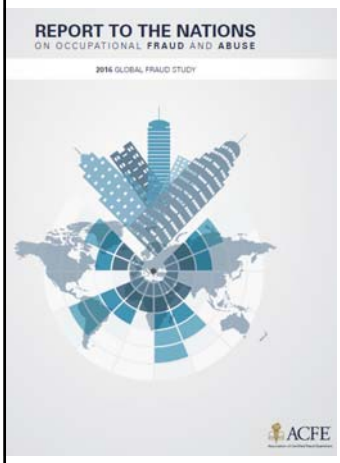
The current Fraud situation?



- *A typical organization loses 5% of revenues per year*
- *$ 6.3 billion in total losses*
- *Median loss: $ 150.000 (23%: 1 mill. or more)*
- *Asset misappropriation as most common form of occupational fraud – but also others*
- *Median duration of the frauds: 18 months*
- *In 94,5% the perpetrator took efforts to conceal the fraud (mainly in creating and altering physical documents*
- *The most common detection method: tips in 39% of cases (mainly coming from employees), followed by internal audit (16%) and management review (13%)*
- *Most represented sectors: banking/finance services, government, public admin, manufacturing industries*

10

Red flags?



- *Most occupational fraudsters are first-time offenders.*
- *41% of cases: the victim organizations decided not to refer their fraud cases to law enforcement (fear of bad publicity)*
- *23% of cases resulted in civil suit*
- *Fraud perpetrators tended to display behavioral warning signs >> The most common red flags:*
  - *Living beyond means, financial difficulties, unusually close association with a vendor / customer, excessive control issues, a general „wheeler-dealer" attitude involving unscrupulous behavior, recent divorce or family problems (one of these in about 80% of cases!)*

11

Areas of risk?

RISK MODEL

(shortened based on copy right-reasons)

12

What was the overriding motivation for fraudster?

13

Motivation

- Financial distress
- Disgruntled employee
- Entitlement
- Announcement or fear of layoff
- Revenge
- Work conflict
- Ideology
- Outside influence

Hunting Insider Threats

Forrester's Model For Establishing An Insider Threat Team

by Joseph Blankenship
July 20, 2016

Sample indicators of insider threat

- Poor performance appraisals
- Voicing disagreement with policies
- Disagreements with coworkers
- Financial distress
- Unexplained financial gain
- Odd working hours
- Unusual overseas travel
- Leaving the company

14

Managerial implications

15

The behavioral side of FA

- ***Know your insiders.*** *Managers, coworkers, and HR professionals have insight into insiders …*
  „Some behaviours can't be detected with technology; they have to be done by discussing and understanding the nontechnical indicators."
- ***Understanding business context.*** *Understanding how users use systems and interact with data helps to identify suspicious behavior. For example, you need to understand what systems your sales force uses on a regular basis and what typical download sizes are; in some cases download activities of an employee is what sparks the investigation.*
- *If you have users entering and **exiting high-risk areas**, badging and surveillance logs and other software and issues can be used for **forensic reasons**.*

Source: http://datacoresystems.ro/index.php/2016/09/22/forrester-report-2016-hunting-insider-threats/

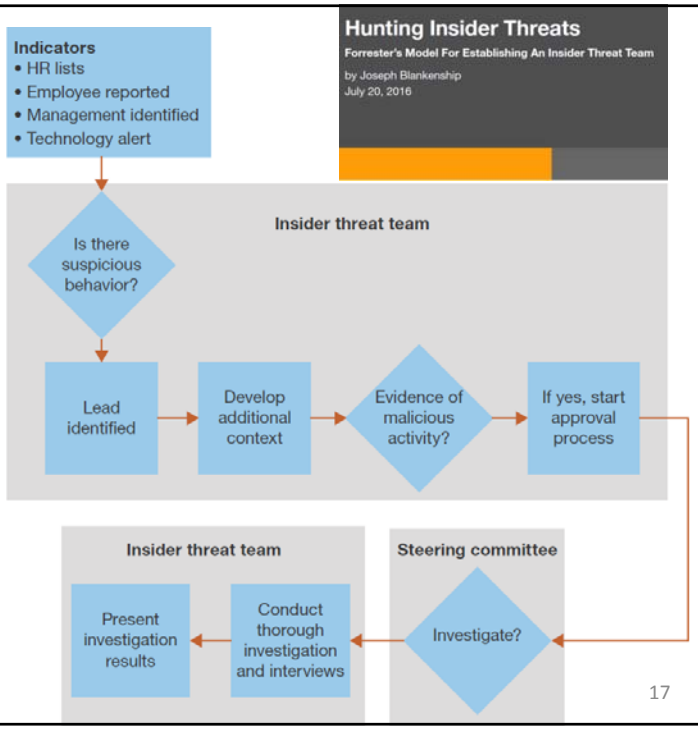
16

Forrester's Threat Program Model

<u>To help with potential litigation:</u>

- *Leverage existing policies and processes when possible (effective policies and controls)*
- *Know your data*
- *Use technology to enable process (technology tools that best fit to a specific case…)*
- ***Treat every investigation as if it will end up in court***

Source: https://www.forrester.com



17

Impact of Anti-Fraud Controls

- Can't create completely fraud-proof
- Can take preventative anti-fraud actions
- Decrease duration of schemes that occur
- Decrease amount of losses

Source: Angela Morelock, forensic accounting/investigation team, bkd.com

18

Thanks for your attention.

ulrike.hugl@uibk.ac.at

19