Fraud in the digital arena.

The never-changing face of fraud

- BITCOIN SCANDAL
- Burned By Bitcoin Scandal, Japan Is Introducing Controls
- Domains in disguise - FRAUD MAGAZINE
- Roving signature stamp: Poor internal controls cost transit entity $250,000
- SWIFT acknowledges cyber fraud incidents
- Probe into Standard Bank R300m fraud at ‘advanced’ stage
Fraud: Occupational Fraud

Occupational fraud is the most practical categorization related to Internal Audit, and is intentional misuse of financially-related employment matters for personal gain.

• Differs from other crimes outside the work environment (example is “romance scams”), that do not result in gain (ex. denial of service), or that are not financially related (ex. stealing another’s possession to “spy”).

Fraud: Occupational Fraud

How Occupational Fraud is commonly Committed

**Asset Misappropriation** (~91.5% of all cases)

- Fraudulent invoicing
- Payroll fraud
- Skimming revenues
- Cybercrime

**Corruption**

- Accepting or paying a bribe - AVON, GOODYEAR
- Engaging in a business transaction where there is an undisclosed conflict of interest

**Fraudulent Statements**

- Booking fictitious sales
- Recording expenses in the wrong period
- Management override of control
- Fraudulent financial reporting
Fraud: Types of Economic Crime (SA)

Figure 3: Types of economic crimes experienced in the past 24 months

- Asset misappropriation: 42%
- Procurement fraud: 33%
- Bribery & corruption: 21%
- Human resources fraud: 4%
- Financial statement fraud: 20%
- Cybercrime: 20%
- Money laundering: 14%
- Tax fraud: 12%
- Illegal insider trading: 10%
- Market fraud involving price fixing: 8%
- IP infringement, including data theft: 7%
- Mortgage fraud: 3%
- Espionage: 3%
- Others: 20%

Fraud: ACFE Report to the Nations

- Typical entity loses 5% of annual revenue to fraud.
- Global fraud loss estimated at more than $3.5 trillion.
- Loss median of $140k and 25% over $1M.
- Median of 18 months before detection.
Fraud in context: PwC Global Economic Crime Survey

• 69% of South African respondents indicated that they had experienced economic crime, which is nine percentage points higher than in 2011.
• The percentage of South African respondents reporting fraud has increased from the previous survey (2011) for the first time since the inception of the survey.
• There has been an alarming shift in the perpetrator profile in South Africa. Senior management is now the main perpetrator of economic crimes committed by insiders. Bribery & corruption has been the fastest growing economic crime category in South Africa since 2011.
• Globally, the construction, energy and mining sectors experience the most bribery.
• South African organisations suffer significantly more procurement fraud, human resources fraud, bribery and financial statement fraud than organisations globally.

Fraud: Impact of legislation in South Africa

• Organizations liable for offence and failing to have controls in place
• Losses incurred in terms of fraud by senior management are not tax deductible and result in a higher tax bill as they will form part of gross income (Income Tax Act)
• Demanding anti-fraud and rigorous risk assessment processes and programs with a focus on prevention and timely detection and emphasis on monitoring (KING IV)
• NOCLAR
• Increased management responsibility towards fraud risk through continuous monitoring (ISA 240, KING IV)
• All Independent auditors required to evaluate sufficiency in fraud controls (ISA 240 for external auditors and APA where negligence in terms of duties results in auditor’s liability, IIA ,ACFE)
Fraud: Traditional View

Traditional views have resulted in a fragmented (not integrated/holistic) risk framework and reactive approach to fraud.

- Fraud risk and controls considered as separate, secondary objectives of internal audit and internal control
- Fraud not perceived to be an internal control failure
- Fraud training and awareness not really necessary
- Information and Communication disparaged
- Fraud risk monitoring not perceived as a positive cost-benefit allocation of resources

Fraud: Current View

The current view adopted by most organisations aims to manage fraud risk holistically and proactively.

- Fraud risk and controls are considered an important objective of internal control activities
- Fraud is perceived to be a result of potential internal control failures
- Fraud training and awareness of fraud scenarios are a necessary management tool.
- Information and Communication is aggregated, concise, and timely and included as one of the components of internal control with specific focus on ITGCs
- Fraud risk monitoring perceived as positive cost/benefit (protects revenue and/or recoups losses).
Rationalisation

Motivation

Opportunity

- Financial Pressure
- Personal growth not matching expectations
- Poor debt management (NCA)
- Instant gratification culture
- Market uncertainty (nest egging)

- "I worked the hardest this year but received my lowest increase/bonus to date"
- "The increases don't match actual inflation, I have less money"
- "I should have been promoted"
- "I am not stealing, I'm borrowing the money and I'll pay it back"

Fraud Triangle

Who is the typical fraudster??
Charles Ponzi

(March 3, 1882 – January 18, 1949) was an Italian swindler, who is considered one of the greatest swindlers in American history. His aliases include Charles Ponei, Charles P. Bianchi, Carl and Carlo. The term "Ponzi scheme" is a widely known description of any scam that pays early investors returns from the investments of later investors. He promised clients a 50% profit within 45 days, or 100% profit within 90 days, by buying discounted postal reply coupons in other countries and redeeming them at face value in the United States as a form of arbitrage. Ponzi was probably inspired by the scheme of William F. Miller, a Brooklyn bookkeeper who in 1899 used the same scheme to take in $1 million.

Bernie Ebbers

Bernard John "Bernie" Ebbers (born August 27, 1941, Edmonton, Alberta) is a Canadian-born businessman. He co-founded the telecommunications company WorldCom and is a former chief executive officer of that company.

In 2005, he was convicted of fraud and conspiracy as a result of WorldCom's false financial reporting, and subsequent loss of US$100-billion to investors. The WorldCom scandal was, until the Madoff schemes came to light in 2008, the largest accounting scandal in United States history. He is currently serving a 25-year prison term at Oakdale Federal Correctional Complex in Louisiana. Portfolio.com and CNBC named Ebbers as the fifth-worst CEO in American history; Time Magazine named him the tenth most corrupt CEO of all time.
Walt Pavlo

As a senior manager at MCI, and with a meritorious employment history, Mr. Pavlo was responsible for the billing and collection of nearly $1 billion in monthly revenue for MCI’s carrier finance division. Beginning in March of 1996, Mr. Pavlo, one member of his staff and a business associate outside of MCI began to perpetrate a fraud involving a few of MCI’s own customers. When the scheme was completed, there had been seven customers of MCI defrauded over a six-month period resulting in $6 million in payments to the Cayman Islands.

In January 2001, in cooperation with the Federal Government, Mr. Pavlo pled guilty to wire fraud and money laundering and entered federal prison shortly thereafter. His story highlights the corrupt dealings involving the manipulation of financial records within a large corporation. His case appeared as a cover story in the June 10, 2002 issue of Forbes Magazine, just weeks before WorldCom divulged that it had over $7 billion in accounting irregularities.

(Source: Walt Pavlo executive bio provided by himself)
Age of Fraudster

- Older than 55 years: 13% (2007), 10% (2011)
- 46 to 55 years old: 31% (2007), 35% (2011)
- 36 to 45 years old: 39% (2007), 41% (2011)
- 26 to 35 years old: 14% (2007), 12% (2011)
- 18 to 25 years old: 3% (2007), 2% (2011)

Rank within the organisation

- Board member: 11% (2007), 18% (2011)
- Senior Management: 26% (2007), 29% (2011)
- Management: 14% (2007), 18% (2011)
- Staff: 35% (2007), 40% (2011)
Where the fraudster works

- Back Office: 2007: 5%, 2011: 5%
- Board Level: 2007: 1%, 2011: 7%
- CEO: 2007: 11%, 2011: 26%
- Finance: 2007: 26%, 2011: 30%
- Legal: 2007: 0%, 2011: 0%
- Procurement: 2007: 0%, 2011: 8%
- Research & Development: 2007: 1%, 2011: 3%

Time at the company

- More than 10 years: 2007: 22%, 2011: 38%
- 6 to 10 years: 2007: 27%, 2011: 29%
- 3 to 5 years: 2007: 29%, 2011: 36%
- 1 to 2 years: 2007: 9%, 2011: 10%
- Less than 1 year: 2007: 4%, 2011: 10%
"WORK EXPANDS SO AS TO FILL THE TIME AVAILABLE FOR ITS COMPLETION"

PARKINSON'S LAW
Fraud Awareness

TRAINING- TONE AT THE TOP

BIG DATA – BATMAN

DATA ANALYTICS – SUPERMAN

AUDITOR- OPTIMUS PRIME – professional judgement

AUDITOR- PROFESSOR X – hidden insights

Fraud Awareness - Tone at the top

PROMOTING ANTI-FRAUD POLICY

The link between corporate culture and fraud - FRAUD MAGAZINE
Fraud Awareness

Toshiba

Consumer electronics and engineering company Toshiba announced in July that its CEO would step down in the aftermath of an investigation into the company’s profit inflation scheme. Toshiba overstated operating profits by $1.9 billion (225 billion yen) over seven years going back to 2008. The September announcement of the scheme represents an even bigger correction than the $1.2 billion adjustment reported in July. (See Toshiba says it inflated profits by nearly $2bn over seven years, by Kana Inagaki, Financial Times, September 7, Toshiba just lost its CEO to a huge accounting scandal, by Geoffrey Smith, Fortune, July 21 and Toshiba Inflated Earnings by $1.2 Billion, a Panel of Experts Says, by Jonathan Soble, July 20, The New York Times.)

An 82-page summary of the investigation’s findings stated that there “existed a corporate culture at Toshiba where it was impossible to go against the boss’ will.” And make no mistake about it. The investigation concluded that the earnings inflation was intentional, not something that could be attributed to accounting errors. The report described “a systematic involvement including by top management, with the goal of intentionally inflating the appearance of net profits.”

Fraud Awareness

Start with the “Fraud Tree” of schemes

General focus of the regulators (relationship for Auditors and Investigation)

Fraud tree

General focus of auditors

Fraudulent statements

Conflicts of interest

Deliberation and presentation

Inability to complete work

Fraudulent statements

Asset misappropriation

General focus of internal auditors

Cash

Theft of items

Financial statements

Petty cash

Period fraud

T&E fraud

Thrift of data

Source: EY
Fraud Awareness - The curious case of Galen March - Morgan Stanley

He was presumably downloading data from an account on which he was working, when he realised that he was able to change the filters on the system. Perhaps he did this at work and waited until he was at home to login again from his personal computer. After this discovery, he took actions that would have raised the following flags in an alert system.

1. Logged in from a personal computer: by itself, a low risk - yellow.
2. After logging in, selected a Branch ID which he was not assigned to: immediate red flag.
3. Fiddled with the financial advisory numbers until he found the correct one: orange, could happen, but presumably not more than once during a session.
4. Downloaded the data onto his personal machine - immediate red flag, presumably no one should download anything from the client management system unless it is on a Morgan Stanley machine.
5. Presumably repeated steps 2, 3 and 4 several times until he logged out for the night: a layered alert showing increasing counts of suspicious actions.

Ultimately, Marsh undertook these actions thousands and thousands of times during the course of his employment. That’sterrifying to security teams, understandably so. Had Morgan Stanley been monitoring for these items, using a centralised platform for the analysis of login data and client management system activity (including where the downloads were going), a security analyst could have received an alert showing the layering of these threat events - producing a very high-risk score.

Audit professionals must be able to:

• Make decisions with incomplete information.
• Determine needed information and where to find it.
• Synthesize collected information to solve problems and make decisions.
• Be comfortable if there isn’t one "right" answer and defend his or her assumptions and choices.
The tendency to want to immediately solve a problem by making a quick judgment results in underinvestment in steps 1 and 2 in the judgment process (see exhibit 1). Often, the solution is to select the first seemingly workable alternative without sufficient consideration of the problem to be solved and the objectives to be achieved. As a result of the rush-to-solve trap, decision makers sometimes end up solving the wrong problem, or they might settle for a suboptimal outcome.

**Judgment Triggers**

Every judgment or decision has an initiating force that triggers a decision and that trigger can lead the decision maker to skip the early steps in the judgment process. Triggers often come in the form of an alternative masquerading as a problem definition, and we thus move forward without a complete understanding of the problem or objectives and without a complete consideration of other alternatives.

**Overconfidence**

The pervasive tendency to be overconfident can lead to suboptimal behavior in every step of a good judgment process. Overconfidence can lead to underinvesting in defining the problem and identifying fundamental objectives, the consideration of too few alternatives, or truncating or skipping an information search, all of which can lead to a suboptimal conclusion.

**Fraud Awareness**

**Confirmation**

The confirmation tendency and related potential judgment bias primarily affects steps 3 and 4 of the judgment process. Our tendency is to seek and overweight confirming information in the information gathering and evaluation steps and to favor conclusions that are consistent with our initial beliefs or preferences.

**Anchoring**

The anchoring tendency and related potential judgment bias primarily affects step 3 of the judgment process. In gathering and evaluating information, it is human nature to anchor on an initial value and adjust insufficiently away from that value in making our final assessments.

**Availability**

The availability tendency limits alternatives considered or information gathered to those alternatives or information that readily come to mind. The availability tendency can have particular influence on steps 2 and 3 of the judgment process.
Fraud Awareness: global company response

- Compliance and legal are often teaming with internal audit to look beyond anti-corruption policies and training and into tests of books and records

- Integrating new analytics specifically targeting corruption – these aren’t your typical rules-based, process control tests

- Integrating “Big Data” concepts including:
  - Text mining (unstructured data)
  - Statistical analyses and anomaly detection
  - Visual analytics and interactive dashboards
  - 100% data sampling, not just random sampling
  - Analytics used to assess high fraud/corruption risk areas

References

- Fraud Magazine Website- Multiple articles
- EY presentations
- BDO Presentations
- KPMG Report on Fraud
DISCLAIMER
This Presentation, case studies and/or opinions expressed are those of the presenter and do not constitute official views of W.consulting. No party may rely upon the opinions expressed during this presentation for any purpose whatsoever. W consulting, its directors, employees and agents shall not be liable to anyone in respect of any reliance placed on information received from or views expressed during this seminar.
Should you wish to obtain an official view on a specific issue or structure, please contact W.consulting and we will be happy to assist you once the specific facts and circumstances of your query have been fully understood.