

Digital Forensics, Forensic Audit Interviews, Fraud Risk Assessment Tools & scorecards (Unit 8 – Module 1)

DFA

March 21, 2022

Arijit Chakraborty

- ◆ **Digital Forensic**
- ◆ *“Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law).”*
- ◆ **Digital Evidence =**
- ◆ any information, data of probative value stored in binary form, transmitted , received by an electronic devices.

Digital Forensics- Audit steps

Evidence Handling

1. Document **condition of evidence**.

- Photograph (screen, computer front & back, area around computer) and/or make sketch of computer connections & surrounding area.
- Determine if computer is in stand-by mode & follow procedures as if it was powered on.

2. Document **external component** connections.

Safety Advisories , Best practices (Guidance)

- **Forensic & Cyber / IS Auditors** - engaged in public practice or employed by insurance companies, banks, police forces, EOW, ACB, government agencies
- **Minimum Safety SOP** =external threats / risks

Personal Hazards, safety & protection issues : Cyber Auditor

- ◆ Risk of personal / physical threat to forensic auditor/ team
- ◆ Report of forensic auditor = **presentation as evidence.**
- ◆ Investigation = lead to legal (criminal) proceedings against suspect,
- ◆ Members of Forensic audit team = involved in resultant court case.
- ◆ Forensic audit team members = called to court to describe evidence & explain how suspect was identified.
- ◆ If chargesheet filed against accused found valid, penal consequences on accused , hence substantial chance that suspect /accused **may try and prevent the forensic auditor from achieving his intended audit result.**
- ◆ **Attempts to prevent forensic auditor** such that he is unable to expose illegal or unethical acts of suspect before Court of law.
- ◆ Forensic audit evidences **may also be tampered or damaged.**
- ◆ Forensic auditor face direct personal threats endangering his safety & security. = **personal safety risk to forensic auditor.**

Safety Checklist of Forensic Auditor

- Cyber & Forensic auditor - develop Safeguards in professional engagement comprising:
 - firm-wide safeguards &
 - engagement-specific safeguards.
- Include appropriate Safety Checklist .
- Significance of personal **risk / threat to be evaluated**, monitored & safeguards applied when necessary.

Insurance Coverage

- ◆ Forensic audit firm =
- ◆ securing adequate insurance cover &
- ◆ Professional indemnity Insurance

NSE Co-location scam

- Former MD and CEO Chitra Ramakrishna revealed to have been taking guidance from an unknown 'Himalayan yogi' to run NSE, have been sharing confidential information with him,
- Email ID of the 'yogi', rigyajursama@outlook.com.
- CBI quizzed Former NSE MD Mr Narain in co-location case – Feb 18-19, 2022
- **CBI investigation** = 2018 case : then NSE brass accused of providing a bunch of high frequency traders unfair access to speed up algorithmic trading.

- **Co-location=** There are dedicated spaces in the exchange building, right next to exchange servers, where high-frequency and algo traders can place their systems or programs
- With co-location facilities being extremely close to stock exchange servers, traders have advantage over other traders due to the improvement in latency (time taken for order execution).
- Co-location = mainly used only by institutional investors and brokers for their proprietary trader. Retail investors have negligible presence here.

High Frequency Trading (HFT) scam.

- High frequency trading (HFT) = type of algo trading characterised by high speeds. The algo is rapidly shooting buy and sell orders at a speed **that cannot be matched** by humans
- Dec 2009, NSE started offering its colocation members tick by tick (TBT) data on the price feed.
- Concept = watch ball-by-ball coverage of a cricket match, instead of only getting to know the score at the end of each over.
- Eg : stock is quoting at Rs 100. A regular broker can see the best buy and best sell orders from Rs 100 to Rs 98. In other words, he is getting a snapshot. Colocation broker was able to see every pending order, & granularly. Say, a regular broker can see cumulative buy orders for 10,000 shares at a certain price. The colocation broker could view every individual bid. He could see that there is a single bid for 5,000 shares, 10 bids for 100 shares, 20 bids for 200 shares, three bids for 250 shares and so on.
- Knowledge of the depth of the order book can be misused to manipulate prices, as it is clear at what price points the maximum buyers and sellers are.

- **Evidence # 1.** Geotagged images with location = 13 metres from Chennai residence of Anand Subramanian- former Group Operating Officer of NSE,
- **Evidence # 2.** : hotel booking by “Himalayan Yogi” for which payments were made by Subramanian, email attachments of “Yogi” modified by Subramanian minutes before they were sent,
- **Evidence # 3:** similarity of phrases used in communications by “Yogi” and Subramanian. - Skype conversation (Fuzzy Matching technique)