FORENSIC AUDIT

Forensic Accounting:

Forensic Accounting provides an accounting analysis that is suitable to the court which will form the basis for discussion, debate and ultimately dispute resolution. Forensic Accounting encompasses both Litigation Support and Investigative Accounting. The *integration of accounting, auditing and investigative skills yields the specialty known as forensic accounting*. With the growing complexities of the business environment and the growing number of business related investigations, forensic accounting professionals are increasingly asked to assist in the investigation of financial and business related issues.

It uses accounting and auditing skills to provide an analysis of financial records in conjunction with dispute resolutions, as well as fraud and theft investigation. It analyses, interprets, summarizes and presents complex financial and business related issues in a manner which is both understandable and properly supported.

A forensic accountant is often involved in the following:

- Investigation and analysis of financial evidence;
- Development of computerized applications to assist in the analysis and presentation of financial evidence;
- Communication of their findings in the form of reports, exhibits and collections of documents; and
- Assistance in legal proceedings, including testifying in court as an expert witness and preparing visual aids to support trial evidence.

Forensic Audit Meaning :

a) A forensic audit is an examination and evaluation of Individual's or a company's financial information for use as evidence in court. A forensic audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims. In addition, a forensic audit may be conducted to determine negligence, misuse of powers or even to determine undue benefits given to any other company or individual.

b) Forensic audit is also conducted on behalf of the banks and financial institutions, insolvency professional agency, SEBI or Management of the company.

c) It is the process used to examine an individual's or company's financial information for use as evidence in court. It helps detect diversion of funds, willful defaults and window dressing of financial statements.

d) A forensic audit is therefore an independent and comprehensive process of reviewing a person's or the company financial statements to determine if they are accurate and whether or not any financial benefit has been attained by way of presenting an unrealistic picture or any illegal activity.

Major difference between Financial Audit Vs Forensic Audit

• Objective of financial auditing is to express opinion as to 'true & fair' presentation. Forensic Audit determines correctness of the accounts or whether any fraud has actually taken place.

• Techniques used in the financial auditing are more of 'Substantive' and 'compliance' procedures. The techniques used in the forensic auditing are analysis of past trend and substantive or 'in depth' checking of selected transactions.

• Normally all transactions for the particular accounting period are covered under the financial audits. Forensic audits don't face any such limitations. Forensic auditors may be appointed to examine the accounts from the beginning.

• For ascertaining the accuracy of the current assets and the liabilities financial auditor relies on the management certificate or representation of management. Forensic auditors are required to carry out the independent verification of suspected or selected items.

• Whenever the financial auditor has adverse findings, then the auditor expresses the qualified opinion, with/without quantification

Section 447 of Companies Act 2013 defines Fraud and related terms as below:

i. 'Fraud' in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;

ii. 'Wrongful gain' means the gain by unlawful means of property to which the person gaining is not legally entitled;

iii. 'Wrongful loss' means the loss by unlawful means of property to which the person losing is legally entitled.

Indian Penal Code, 1860

- Section 168 of the IPC – Public servant unlawfully engaging in trade: “Whoever, being a public servant, and being legally bound as such public servant not to engage in trade, engages in trade, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.”
- Section 171 B – Bribery, read with Section 7 of the PC Act “Whoever commits the offence of bribery shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both. Provided that bribery by treating shall be punished with fine only” as per Section 171E.
- Section 403 – Dishonest Misappropriation of property
- Section 405 – Criminal Breach of Trust: “Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both” according to Section 406.
- Section 417 – Cheating
- Section 463 – Forgery “Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine or with both” Penalties under Prevention of Money Laundering Act, 2002.
- Section 4 – Punishment for money-laundering. –

Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine which may extend to five lakh rupees :

FORENSIC AUDIT PROCEDURES

- Data Analysis
- Analytical Procedures
- Inspection
- Observation
- External Confirmation
- Recalculation
- Re-Performance
- Inquiry
- Interviews

FINANCIAL STATEMENTS FRAUD

- This is also known as *fraudulent financial reporting*, and is a type of fraud that causes a material misstatement in the financial statements. *It can include deliberate falsification of accounting records; omission of transactions– either revenue or expenses, non-disclosure of relevant details from the financial statements, balances or disclosures from the financial statements; or the misapplication of financial reporting standards.* This is often carried out with the intention of presenting the financial statements with a particular bias, for example concealing liabilities in order to improve any analysis of liquidity and gearing. Companies get into this type of fraud to try to show the company's financial performance as better than what it actually is. The goal of presenting fraudulent numbers may be to improve liquidity, ensure top management continue receiving bonuses, or to deal with pressure for market performance.

PROCEDURE FOR FORENSIC AUDIT INVESTIGATION

- The investigation process is similar to regular audit of financial statements. The forensic auditor should take steps for planning, review and a report. If the investigation is to be conducted to unearth the fraud in respect of purchases, then a complete investigation is to be conducted for due diligence of all the suppliers of the company. *This investigation will include verification of the prices at which the goods are supplied by the various suppliers with the prices prevailing in the market from the third party sources.* There may be instances of bogus bills being accounted for into the books of accounts without receiving the goods. The forensic auditor has to collect the evidence to unearth the fraud. He will also access the quantum of losses suffered by the company. The findings are presented to the client or the appointing authority.
- Thus, the procedure for forensic audit will be changed according to the requirement and type of the forensic audit.
- The method for conducting forensic audit are as follows:

SYSTEMS OF FRAUD

- Delayed submission of returns information etc;
- Delayed remittances into Bank;
- Delay or non preparation of Bank reconciliation statements;
- Lifestyle of promoters/ directors and key employees;
- Continued internal control lapses and not following norms of corporate governance.

- INTERNAL INDICATORS

- Delay in finalisation of accounts;
- *Frequent changes in accounting policies*;
- Continuing losses;
- Over drawl of loans and advances;
- *Higher cost per unit of production*
- High amount of losses or wastage shown in books vs. norms;
- High investment in group companies;
- Profit not supported by increased cash availability.

PREPARATION OF REPORT

- The report generally includes various sections describing the nature of assignment, scope, approaches utilized, findings, opinion and limitations. Report is generally submitted to the Appointing Authority.
- The contents of the report may vary depending upon the situation, the nature and the extent of the frauds and irregularities involved. The generalized form of such forensic accounting investigation report is as follows:

PREPARATION OF REPORT…(CONT.)

1. **TITLE OF THE REPORT**
2. **EXECUTIVE SUMMARY**
3. **BACKGROUND OF ENGAGEMENT**
   - 3.1. Origin
   - 3.2. Objectives of Engagement
   - 3.3. Proposed outputs of the Assignments
   - 3.4. Implementation Approaches
4. **ANALYSIS OF THE RISKS INVOLVED**
   - 4.1. Internal Environment Risks
   - 4.2. External Environment Risks
   - 4.3. Political and Legal Scenario
   - 4.4. Risks from Customers, Suppliers and Competitors etc.
   - 4.5 Business Process and Human Resources Management
   - 4.6. Market, Operational and Technological Risks
   - 4.7. Others

PREPARATION OF REPORT…(CONT.)

5.EVIDENCE OF RISK EVENTS

6. ANALYSIS and FINDINGS

7. AUDIT RECOMMENDATIONS

- 7.1. Logical Framework Approach
- 7.2. Preconditions and Risks

8. IMPLEMENTATION OF RECOMMENDATIONS

- 8.1. Budget Considerations
- 8.2. Stakeholders to be Engaged

9. LIST OF ANNEXURES

Financial Auditing Vs Forensic Audit:

The concept of Financial Auditing may be defined as "a concentrated audit of all the transactions of the entity to **find the correctness of such transactions and to report whether or not any financial benefit has been attained by way of presenting an unreal picture**". Forensic auditing aims at legal determination of whether fraud has actually occurred. In the process, it also aims at naming the person(s) involved (with a view to take legal action).

FORENSIC ACCOUNTING

- Forensic accounting is the specialty area of the **accountancy profession** which describes engagements that result from actual or anticipated **disputes or litigation**.

- *Forensic accounting uses* ***accounting, auditing, and investigative skills*** to conduct investigations into theft and fraud. This includes tracing **money laundering** and identity **theft activities as well as tax evasion.**

TECHNIQUES OF FORENSIC ACCOUNTING

- **Interview Techniques**

It is important that forensic accountants properly structure the interview process because the results of the interview may be used in court and adjudication processes. Because the outcome of the interview may enter a legal process it is important that the interview process be coordinated with an attorney from the auditing organization. The auditors must work within the rules of the interview process but there are areas that they should try to control to make the interview process work (Golden and Dyer 2006). Some of the key factors are listed below:

Document Review Strategies

- Document reviews are a key part of the evidence for an audit (Miller and Marston 2006). Forensic accounting requires special care in dealing with documents because the audit may involve special adjudication and court proceedings where the rules of evidence may be used to exclude documents from the evidence if they are not properly acquired and maintained. Three basic questions apply to the documents being reviewed in a forensic accounting investigation:
- 1. How do you **handle confidential information**?
- 2. How do you **preserve the information** in the documents so it can be used in an adjudication or court situation?
- 3. Who **maintains the records** from the audit?

Computer Assisted Auditing Tools (CAATs):

CAATs are computer programs that the auditor use as part of the audit procedures to process data of audit significance contained in a client's information systems, without depending on him.

CAAT helps auditors to perform various auditing procedures such as: (a) Testing details of transactions and balances,

(b) identifying inconsistencies or significant fluctuations,

(c) Testing general as well as application control of

computer systems.

(d) Sampling programs to extract data for audit testing, and

(e) Redoing calculations performed by accounting systems.

Data mining techniques:

It is a set of computer-assisted techniques designed to automatically mine large volumes of data for new, hidden or unexpected information or patterns.

Data mining techniques are categorized in three ways:
Discovery, Predictive modelling and Deviation and Link analysis.

It discovers the usual knowledge or patterns in data, without a predefined idea or hypothesis about what the pattern may be, i.e. without any prior knowledge of fraud. It explains various affinities, association, trends and variations in the form of conditional logic. In predictive modelling, patterns discovered
from the database are used to predict the outcome and to guess data for new value items

Ratio Analysis:

Another useful fraud detection technique is the calculation of **data analysis ratios** for key numeric fields. Like financial ratios that give indications of the financial health

of a company, data analysis ratios report on the fraud health by identifying possible symptoms of fraud.

Three commonly employed ratios are—

1. the ratio of the highest value to the lowest value **(max/min);**

2. the ratio of the highest value to the second highest value **(max/max2);** and

3. the ratio of the **current year to the previous Year Ratio** analysis may help a forensic accountant estimate expenses.

NEED OF FORENSIC AUDIT

- Criminal Investigation
- Shareholders and Partnership Disputes
- Business Interruption's
- Business/Employee Fraud Investigations
- Business Economic losses

SKILLS &APPLICATION FOR FORENSIC AUDIT

Skills

- Knowledge of entity's business and legal environment.
- Awareness of computer assisted audit procedures.
- Innovative approach and skeptic of routine audit practices.

Application

Forensic Accounting and Audit may be applied in the following areas besides fraud detection:

(a) Conducting due-diligence (especially for segment wise profitability analysis)

(b) Business valuation

(c) Management auditing

(d) Assessing loss before settling insurance claims.

FRAUD

- **Dictionary Meaning** of fraud is "deceit, impersonation with intent to deceive, criminal deception done with the intention of gaining an advantage."

- **The Institute of Turkish History** explains the word Fraud as "a deceptive trick, scam, game, artifice, cabal which is committed to cheat, mislead someone" and "contributing something unless to something in order to gain advantage"

- **Fraud** involves deliberate misrepresentation of facts and/ or significant information to obtain undue or illegal financial advantage.

EXAMPLES OF FRAUD

Examples of frauds that employees commit to benefit themselves are given as follows

- Embezzlement of the money during its collection but before it is recorded in accounts
- Stealing the cheques of business
- Tampering the bank records and taking monetary advantage
- Gaining advantage through forgery of documents
- Making payments which should not be made or previously made
- Creating fictitious debts and having payments done in favour of oneself
- Giving discount improperly or without authority
- Inventory and scrap theft

- Creating fictitious expenses and obtaining disbursements
- Creating ghost employees and embezzling their wages/salaries
- Accepting bribes from the customers and suppliers of the business with various reasons
- Using credit cards of the business for personal objectives
- Benefiting from overstated personal expenditures
- Manipulating the overtime periods and obtaining extra payment
- Benefiting from padded travel expenses
- Selling business assets under the market value

ELEMENTS OF FRAUD

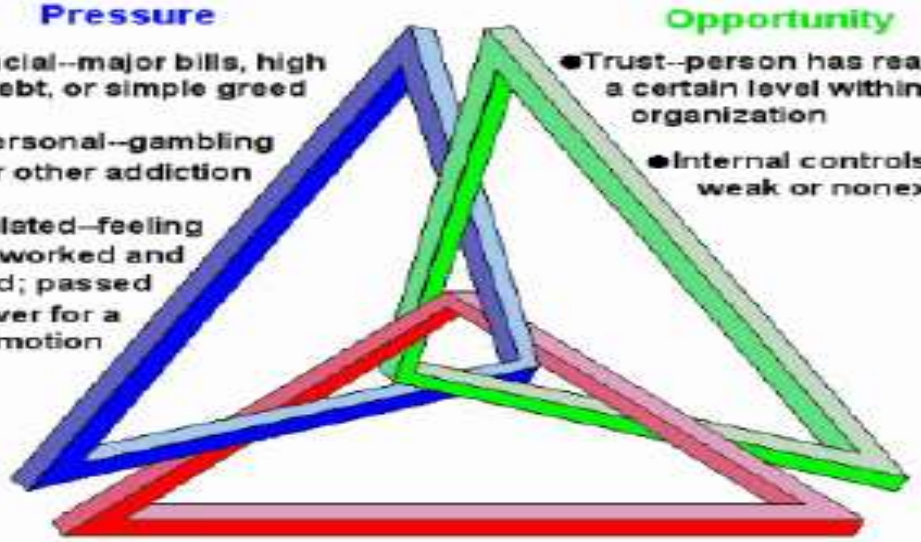
- There must be at least two parties to fraud namely, the perpetrator and the party who was or could have been harmed by fraud, otherwise known as the victim;
- A material omission or false representation must be made knowingly by the perpetrator;
- There must be an intent by the perpetrator that the false representation be acted upon by the victim;
- The victim must have the legal right to reply on the representation;
- There must be either actual injury or a risk of injury to the victim as a result of reliance;
- - Fraud involves the betrayal of trust.

REASONS WHY EMPLOYEES COMMIT FRAUD

When business frauds are analysed, it is ascertained that three components come together when committing the white-collar crime. These are pressure, opportunity, and justification that constitute the **"fraud triangle."** Components of the fraud triangle are similar to the fuel, spark, and oxygen which together cause fire. When the three come together, inevitably fire breaks out.

The Fraud Triangle

All three components must be present at the same time for someone to commit fraud



Pressure

- Financial--major bills, high level of debt, or simple greed
- Personal--gambling or other addiction
- Work-related--feeling overworked and underpaid; passed over for a promotion

Opportunity

- Trust--person has reached a certain level within the organization
- Internal controls--either weak or nonexistent

Rationalization

- Justification--"I'm only borrowing the money. I'll give it back when my financial situation improves."
- Lack of ethics--"Management isn't honest, so why should I be?"

PREVENTING FINANCIAL FRAUD THROUGH 'FORENSIC ACCOUNTING'

The term Forensic Accounting encompasses a wide range of activities including:

- *1)**The Expert Witness*** – preparation of formal Reports for filing in Court and giving evidence as an Expert
- 2) ***Litigation Consultancy*** – working with lawyers and their clients engaged in litigation and assisting with evidence, strategy and case preparation.
- 3) ***Fraud Detection*** – assisting clients in detecting financial fraud by employees and others and tracing misappropriated funds.
- 4) ***Computer Forensics*** – assisting in electronic data recovery and enforcement of IP rights etc.

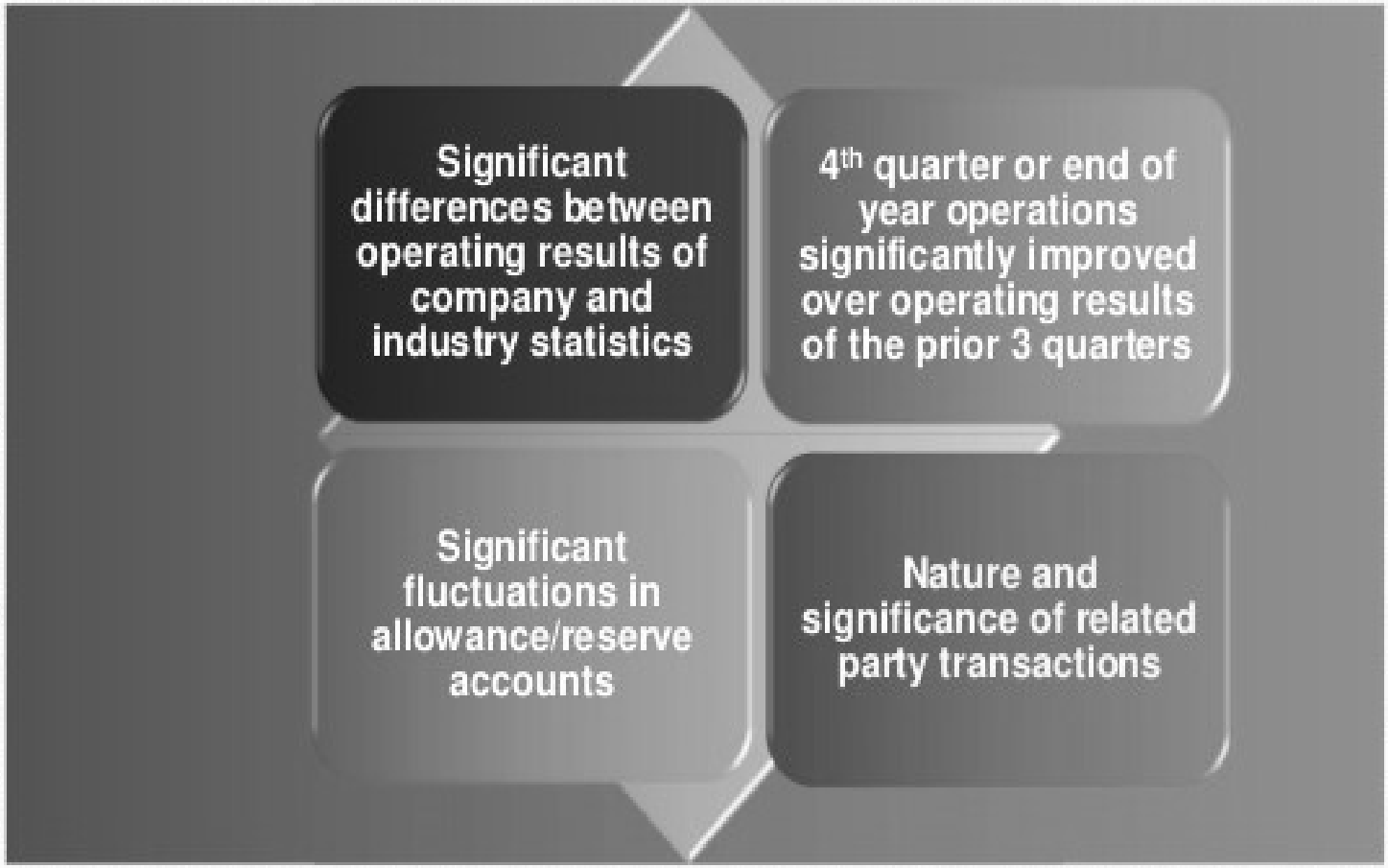
ROLE OF FORENSIC ACCOUNTANTS

Forensic Accountancy involves a financial detective (Forensic Accountant) with a suspicious mind, a financial bloodhound, someone with a 'sixth sense' that enables reconstruction of past accounting transactions and an individual who looks beyond the numbers.

ESSENTIALS OF FORENSIC AUDIT

- The basic requirement is to ask questions, ask questions even if the person is tom, dick or harry. One does not know from which corner the untied loose thread reveals itself. The implications of not asking questions both in normal audit and forensic audit have far reaching consequences.
- It's often observed that auditors hesitate to ask questions as they feel that it may hurt the other. This feeling creeps in because the auditor may be having less confidence in himself. He may have a periphery feeling that something is wrong, but does not have the courage to question it either because it embarrasses another person or that it may land him into legal trouble. One must understand that not questioning, which ultimately leads to a scandal, may be more disastrous than the gravity of asking a question.
- Forensic audit requires being proactive in fulfilling its objective. Skilful enquiry regardless of the person's position in the organisation and being obsessed with it, with all other methods of verification, will go a long way in establishing strong and intimidating processes for the auditor.

More Red Flags



Types of Internal Frauds.

Asset misappropriation

Theft of cash

- Stealing from petty cash.
- Taking money from the till.
- Skimming of cash before recording revenues or receivables (understating sales or receivables).
- Stealing incoming cash or cheques through an account set up to look like a bonafide payee.

False payment requests

- Employee creating false payment instruction with forged signatures and submitting it for processing.
- False email payment request together with hard copy printout with forged approval signature.
- Taking advantage of the lack of time which typically occurs during book closing to get false invoices approved and paid.

Cheque fraud

- Theft of company cheques.
- Duplicating or counterfeiting of company cheques.
- Tampering with company cheques (payee/amount).
- Depositing a cheque into a third party account without authority.
- Cheque kiting (a fraud scheme using two deposit accounts to withdraw money illegally from the bank).
- Paying a cheque to the company knowing that insufficient funds are in the account to cover it.

Areas of Risk

Billing schemes

•Over-billing customers.
•Recording of false credits, rebates or refunds to customers.
•Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund).
•Using fictitious suppliers or shell companies for false billing.

Misuse of accounts

•Wire transfer fraud (fraudulent transfers into bank accounts).
•Unrecorded sales or receivables.
•Employee account fraud (where an employee is also a customer and the employee makes unauthorised adjustments to their accounts).
•Writing false credit note to customers with details of an employee's personal bank account or of an account of a company controlled by the employee.
•Stealing passwords to payment systems and inputting series of payments to own account

Inventory and fixed assets

- Theft of inventory.
- False write offs and other debits to inventory.
- False sales of inventory.
- Theft of fixed assets, including computers and other IT related assets.
- Theft or abuse of proprietary or confidential information (customer information, intellectual property, pricing schedules, business plans, etc.).
- Receiving free or below market value goods and services from suppliers.
- Unauthorised private use of company property.
- Employees trading for their own account.

Procurement

- Altering legitimate purchase orders.
- Falsifying documents to obtain authorisation for payment.
- Forging signatures on payment authorisations.
- Submitting for payment false invoices from fictitious or actual suppliers.
- Improper changes to supplier payment terms or other supplier details.
- Intercepting payments to suppliers.
- Sending fictitious or duplicate invoices to suppliers.
- Improper use of company credit cards.

Improper revenue recognition

•Holding the books open after the end of the accounting period.
•Inflation of sales figures which are credited out after the year end.
•Backdating agreements.
•Recording fictitious sales and shipping.
•Improper classification of revenues.
•Inappropriate estimates for returns, price adjustments and other concessions.
•Manipulation of rebates.
•Recognising revenue on disputed claims against customers.
•Recognising income on products shipped for trial or evaluation purposes.
•Improper recording of consignment or contingency sales.
•Over/under estimating percentage of work completed on long-term contracts.
•Incorrect inclusion of related party receivables
•Side letter agreements (agreements made outside of formal contracts).
•Round tripping (practice whereby two companies buy and sell the same amount of a commodity at the same price at the same time. The trading lacks economic substance and results in overstated revenues).

Misstatement of assets, liabilities and/or expenses

- Fictitious fixed assets.
- Overstating assets acquired through merger and acquisitions.
- Improper capitalisation of expenses as fixed assets (software development, research and development, start up costs, interest costs, advertising costs).
- Manipulation of fixed asset valuations.
- Schemes involving inappropriate depreciation or amortisation.
- Incorrect values attached to goodwill or other intangibles.
- Fictitious investments.
- Improper investment valuation (misclassification of investments, recording unrealised investments, declines in fair market value/overvaluation).
- Fictitious bank accounts.
- Inflating inventory quantity through inclusion of fictitious inventory.
- Improper valuation of inventory.
- Fraudulent or improper capitalisation of inventory.
- Manipulation of inventory counts.

Kickbacks

- Kickbacks to employees by a supplier in return for the supplier receiving favourable treatment.
- Kickbacks to senior management in relation to the acquisition of a new business or disposal of part of the business.
- Employee sells company-owned property at less than market value to receive a kickback or to sell the property back to the company at a higher price in the future.
- Purchase of property at higher than market value in exchange for a kickback.
- Preferential treatment of customers in return for a kickback.

Personal interests

- Collusion with customers and/or suppliers.
- Favouring a supplier in which the employee has a financial interest.
- Employee setting up and using own consultancy for personal gain (conflicts with the company's interests).
- Employee hiring someone close to them over another more qualified applicant.
- Transfer of knowledge to a competitor by an employee who intends to joins the competitor's company.
- Misrepresentation by insiders with regard to a corporate merger, acquisition or investment.
- Insider trading (using business information not released to the public to gain profits from trading in the financial markets).

BRIBERY AND EXTORTION

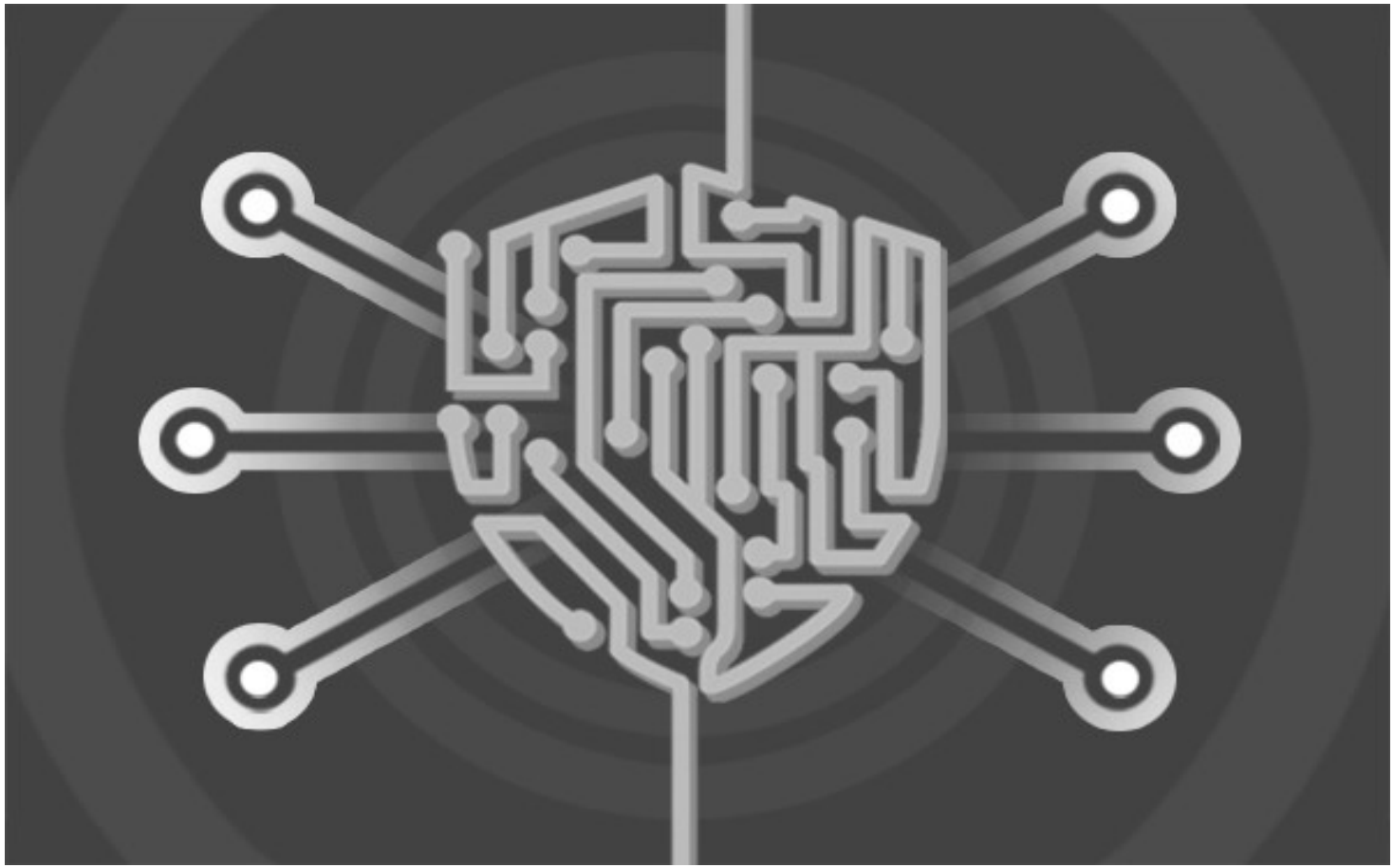
Bribery

- Payment of agency/facilitation fees (or bribes) in order to secure a contract.
- Authorising orders to a particular supplier in return for bribes.
- Giving and accepting payments to favour or not favour other commercial transactions or relationships.
- Payments to government officials to obtain a benefit (e.g. customs officials, tax inspectors).
- Anti-trust activities such as price fixing or bid rigging.
- Illegal political contributions.

Extortion

- Extortion (offering to keep someone from harm in exchange for money or other consideration).
- Blackmail (offering to keep information confidential in return for money or other consideration).

What Is Cybersecurity?



Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

What is cybersecurity all about?

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defence from cyber attacks.

•Watch a cyberattack unfold

People

Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Learn more about basic cybersecurity principles.

Processes

Organizations must have a framework for how they deal with both attempted and successful cyber attacks. One well-respected framework can guide you. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks. Watch a video explanation of the NIST cybersecurity framework.

Technology

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

Why is cybersecurity important?

In today's connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyber attack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open source tools. Their work makes the Internet safer for everyone.

Types of cybersecurity threats

Ransomware

Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

Malware

Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Social engineering

Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.

Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber attack. You can help protect yourself through education or a technology solution that filters malicious emails.

Learn how technology can help

Cyberattacks in India of Late

JULY 2016

UNION BANK OF INDIA HEIST

Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171 million, Prompt action helped the bank recover almost the entire money

MAY 2017

WANNACRY RANSOMWARE

The global ransomware attack took its toll in India with several thousands computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of West Bengal

MAY 2017

DATA THEFT AT ZOMATO

The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web

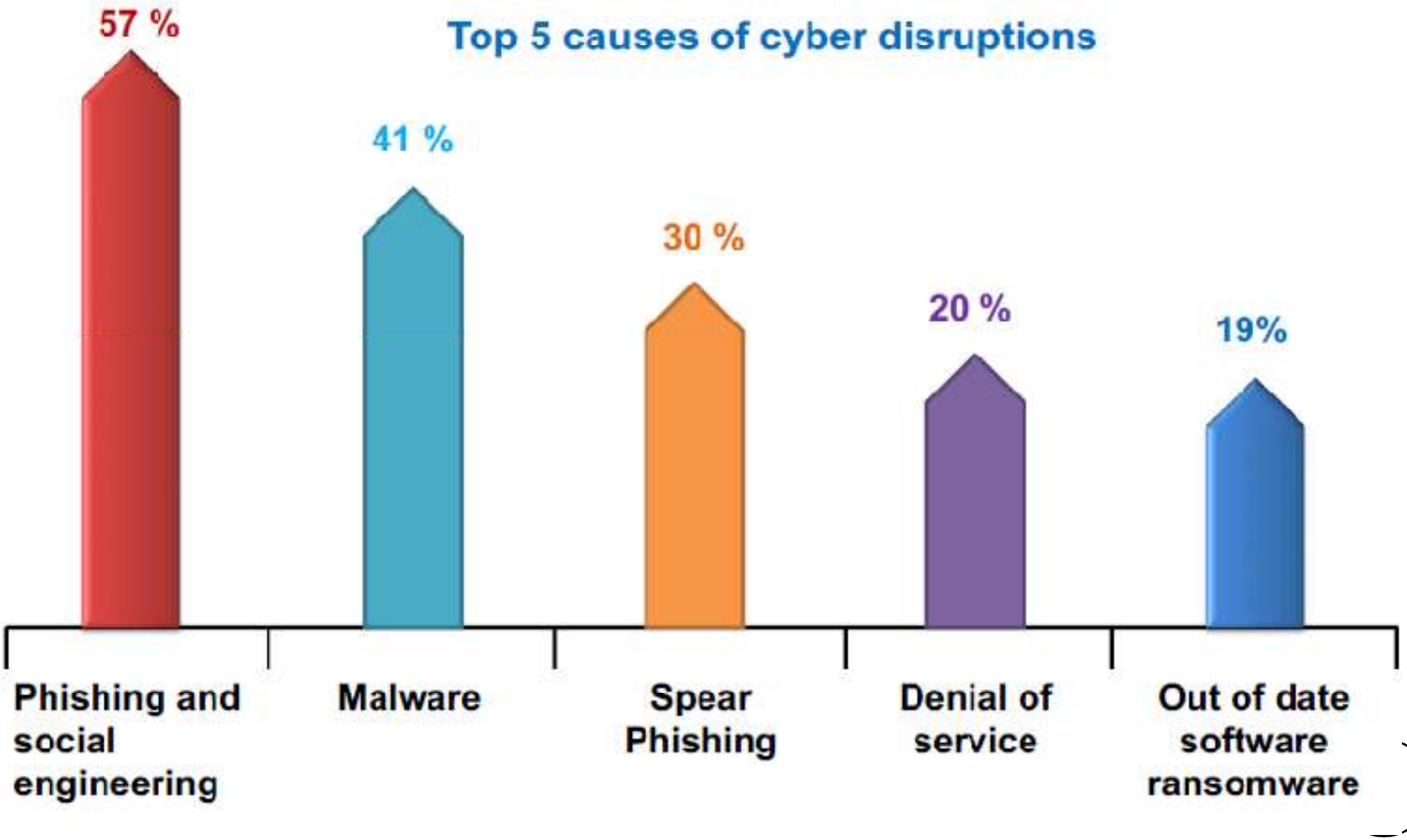
JUNE 2017

PETYA RANSOMWARE

The ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected

Cyber disruptions

> 50 % of the organization s reportedly affected in 2017



Thank You