A

PROJECT REPORT

ON

"Financial Analytics"

UNDERTAKEN AT

"MIT School of Distance Education"

IN PARTIAL FULFILMENT OF

"Executive MBA Finance"

MIT SCHOOL OF DISTANCE EDUCATION, PUNE.

GUIDED BY

"Krishna Jeeyar"

SUBMITTED BY

"Jhanhavi L"

STUDENT REGISTRATION NO.: MIT2021C00283

MIT SCHOOL OF DISTANCE EDUCATION PUNE - 411 038

YEAR 2021-23

Exempt Certificate - If you're not able to provide the Project Executed Certificate

To
The Director
MIT School of Distance Education,

Respected Sir,

This is to request you to kindly exempt me from submitting the certificate for Project Work due to the reason mentioned below:

Tick the right option
✓1. As per the Rules of the Organisation
2. Self Employed
3. Working in Public Sector
4. Full-time Student

Thanking you in anticipation of your approval to my request.

Regards

Student Sign: - Jhanhavi

Student Name:- Jhanhavi L

Student ID: MIT2021C00283

DECLARATION

I hereby declare that this project report entitled **“Fraud Detection and Risk Management”** bonafide record of the project work carried out by me duri ng the academic year **2021-2023**, in fulfillment of the requirements for the awar d of **“E- MBA Finance”** of MIT School of Distance Education.

This work has not been undertaken or submitted elsewhere in connection with any other academic course.

Sign:- Jhanhavi

Name:- Jhanhavi L

Student ID: MIT2021C00283

ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere thanks and gratitude to **“**Krishna Jeeyar (ex MIT student)**”**, Faculty of MIT School of D istance Education, for allowing me to do my project work in your esteem ed organization. It has been a great learning and enjoyable experience.

I would like to express my deep sense of gratitude and profound thanks to all staff members of MIT School of Distance Education for their kind support and cooperation which helped me in gaining lots of knowledge and experience to do my project work successfully.

At last but not least, I am thankful to my Family and Friends for their moral support, endurance and encouragement during the course of the project.

Sign:- Jhanhavi

Name:- Jhanhavi L

Student ID: MIT2021C00283

OBJECTIVES

This is the study on Fraud Detection and Risk Management.

Enhance the accuracy and effectiveness of fraud detection systems to identify fraudulent behavior with greater with greater precision while minimizing the false positives.

Reduce Fraud Losses by minimizing financial losses resulting in the fraudulent activitiess, such as unauthorized transactions, identify theft, anti money laundering or fraudulent insurance claims.

Improve Detection Accuracy by enhancing the accuracy and effectiveness of fraud detection systems to identify fraudulent behaviour with greater precision while minimizing false positives.

Fraud represents a significant problem for governments and businesses and specialized analysis techniques for discovering fraud using them are required. Some of these methods include knowledge discovery in databases , data mining , machine learning and statistics. They offer applicable and successful solutions in different areas of electronic fraud crimes.

In general, the primary reason to use data analytics techniques is to tackle fraud since many internal control systems have serious weaknesses. For example, the currently prevailing approach employed by many law enforcement agencies to detect companies involved in potential cases of fraud consists in receiving circumstantial evidence or complaints from whistleblowers. As a result, a large number of fraud cases remain undetected and unprosecuted. In order to effectively test, detect, validate, correct error and monitor control systems against fraudulent activities, businesses entities and organizations rely on specialized data analytics techniques such as data mining, data matching, the sounds like function, regression analysis, clustering analysis, and gap analysis.Techniques used for fraud detection fall into two primary classes: statistical techniques and artificial intelligence.

Risk management is the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Risks can come from various sources including uncertainty in international markets, political instability, threats from project failures (at any phase in design, development, production, or sustaining of life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, deliberate attack from an adversary, or events of uncertain or unpredictable root-cause.

There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities. Risk management standards have been developed by various institutions, including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards (quality management standards to help work more efficiently and reduce product failures). Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety. Certain risk management standards have been criticized for having no measurable improvement on risk, whereas the confidence in estimates and decisions seems to increase.

Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some or all of the potential or actual consequences of a particular threat. The opposite of these strategies can be used to respond to opportunities (uncertain future states with benefits).

As a professional role, a risk manager will "oversee the organization's comprehensive insurance and risk management program, assessing and identifying risks that could impede the reputation, safety, security, or financial success of the organization", and then develop plans to minimize and / or mitigate any negative (financial) outcomes. Risk Analysts support the technical side of the organization's risk management approach: once risk data has been compiled and evaluated, analysts share their findings with their managers, who use those insights to decide among possible solutions. See also Chief Risk Officer, internal audit, and Financial risk management and Corporate finance.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

Fraud and risk are pervasive challenges that organizations face across industries. Fraud encompasses various deceptive practices, including financial fraud, identity theft, and cybercrime, aimed at exploiting vulnerabilities for illicit gain. The motivations behind fraud range from financial gain to revenge or coercion, posing significant threats to organizational integrity, financial stability, and reputation.
Effective fraud detection and risk management are crucial for safeguarding businesses against these threats. By implementing robust strategies and leveraging advanced technologies, organizations can identify, prevent, and mitigate the impact of fraudulent activities.

This document explores the intricacies of fraud detection and risk management, providing insights into the types of fraud, risk management frameworks, data analytics techniques, technological innovations, regulatory compliance, best practices, and future trends. Through comprehensive understanding and proactive measures, organizations can enhance their resilience against fraud and maintain trust in their operations.

Fraud is a multifaceted phenomenon that manifests in various forms, posing significant challenges to organizations worldwide. Understanding the nature and dynamics of fraud is essential for developing effective detection and prevention strategies.
Types of Fraud: Fraud can occur in numerous ways, including but not limited to:
1.Financial Fraud: Manipulation of financial records, embezzlement, and misappropriation of funds.
2.Identity Theft: Unauthorized use of personal information for fraudulent purposes, such as opening accounts or making purchases.
3.Cybercrime: Online scams, phishing attacks, malware infections, and ransomware incidents targeting individuals and businesses.
4.Insurance Fraud: Falsifying insurance claims or exaggerating damages for monetary gain.
5.Corporate Fraud: Fraudulent activities within organizations, including bribery, corruption, and insider trading.
6.Healthcare Fraud: Billing for services not rendered, providing unnecessary treatments, or submitting false claims to healthcare insurers.

Motivations Behind Fraudulent Activities: Understanding the motivations driving individuals to commit fraud is crucial for developing preventive measures. Motivations may include:

1.Financial Gain: The most common motivation, where individuals seek personal enrichment through fraudulent schemes.
2.Revenge or Retaliation: Disgruntled employees or individuals may engage in fraud as a form of retaliation against an organization or individual.
3.Pressure or Coercion: External pressures, such as financial difficulties or coercion by others, may compel individuals to commit fraud.
4.Thrill or Challenge: Some individuals are motivated by the excitement or challenge of circumventing security measures and getting away with fraudulent activities.
5.Ideological Reasons: In rare cases, individuals may engage in fraud for ideological reasons, such as activism or political agendas.

Impact of Fraud on Organizations: Fraud can have far-reaching consequences for organizations, including:

1.Financial Losses: Direct monetary losses resulting from fraudulent activities, including stolen funds or assets.
2.Reputational Damage: Negative publicity and loss of trust among stakeholders, including customers, investors, and partners.
3.Legal and Regulatory Consequences: Fines, lawsuits, and regulatory sanctions resulting from non-compliance with laws and regulations.
4.Operational Disruption: Disruption of business operations, loss of productivity, and increased costs associated with fraud investigations and remediation efforts.
5.Erosion of Employee Morale: Decline in employee morale and trust, leading to decreased productivity and increased turnover rates.

By understanding the types, motivations, and impacts of fraud, organizations can better prepare to detect, prevent, and mitigate fraudulent activities.

CHAPTER 2: RISK MANAGEMENT FRAMEWORK

Implementing an effective risk management framework is essential for identifying, assessing, mitigating, and monitoring risks associated with fraud and other threats. A robust risk management framework provides organizations with a systematic approach to proactively manage risks and enhance resilience against fraudulent activities.

Risk Identification: The first step in the risk management process is identifying potential risks and vulnerabilities that could lead to fraud or other adverse outcomes. This involves:

•Conducting risk assessments to identify internal and external threats.
•Analyzing past incidents and trends to identify recurring patterns.
•Engaging stakeholders across the organization to gather insights into potential risks.

Risk Assessment: Once risks are identified, they must be assessed to determine their likelihood and potential impact on the organization. This involves:

•Prioritizing risks based on their severity and likelihood of occurrence.
•Assessing the adequacy of existing controls and mitigation measures.
•Quantifying risks using risk assessment methodologies, such as risk matrices or scenario analysis.

Risk Mitigation Strategies: After assessing risks, organizations develop and implement strategies to mitigate or reduce the likelihood and impact of fraudulent activities. This may include:

•Implementing internal controls and security measures to prevent unauthorized access and fraudulent transactions.
•Enhancing employee training and awareness programs to educate staff about fraud risks and prevention measures.
•Implementing fraud detection technologies, such as anomaly detection systems or predictive analytics, to identify suspicious activities in real-time.
•Establishing incident response plans and protocols to quickly respond to and contain fraudulent incidents when they occur.

Risk Monitoring and Review: Risk management is an ongoing process that requires continuous monitoring and review to ensure the effectiveness of mitigation measures and adapt to evolving threats. This involves:

•Monitoring key risk indicators and performance metrics to track changes in risk exposure over time.
•Conducting regular audits and reviews to assess the effectiveness of controls and identify areas for improvement.
•Updating risk assessments and mitigation strategies in response to changes in the business environment or emerging risks.

By implementing a comprehensive risk management framework, organizations can proactively identify, assess, and mitigate fraud risks, thereby enhancing their resilience and safeguarding their assets and reputation.

CHAPTER 3: DATA ANALYSIS AND FRAUD DETECTION

Fraud represents a significant problem for governments and businesses and specialized analysis techniques for discovering fraud using them are required. Some of these methods include knowledge discovery in databases (KDD), data mining, machine learning and statistics. They offer applicable and successful solutions in different areas of electronic fraud crimes.

In general, the primary reason to use data analytics techniques is to tackle fraud since many internal control systems have serious weaknesses. For example, the currently prevailing approach employed by many law enforcement agencies to detect companies involved in potential cases of fraud consists in receiving circumstantial evidence or complaints from whistleblowers.[2] As a result, a large number of fraud cases remain undetected and unprosecuted. In order to effectively test, detect, validate, correct error and monitor control systems against fraudulent activities, businesses entities and organizations rely on specialized data analytics techniques such as data mining, data matching, the sounds like function, regression analysis, clustering analysis, and gap analysis. Techniques used for fraud detection fall into two primary classes: statistical techniques and artificial intelligence.

Examples of statistical data analysis techniques are:

Data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data.

Calculation of various statistical parameters such as averages, quantiles, performance metrics, probability distributions, and so on. For example, the averages may include average length of call, average number of calls per month and average delays in bill payment.

Models and probability distributions of various business activities either in terms of various parameters or probability distributions.

Computing user profiles.

Time-series analysis of time-dependent data.

Clustering and classification to find patterns and associations among groups of data.

Data matching Data matching is used to compare two sets of collected data. The process can be performed based on algorithms or programmed loops. Trying to match sets of data against each other or comparing complex data types. Data matching is used to remove duplicate records and identify links between two data sets for marketing, security or other uses.

Sounds like Function is used to find values that sound similar. The Phonetic similarity is one way to locate possible duplicate values, or inconsistent spelling in manually entered data. The ‘sounds like’ function converts the comparison strings to four-character American Soundex codes, which are based on the first letter, and the first three consonants after the first letter, in each string.

Regression analysis allows you to examine the relationship between two or more variables of interest. Regression analysis estimates relationships between independent variables and a dependent variable. This method can be used to help understand and identify relationships among variables and predict actual results.

Gap analysis is used to determine whether business requirements are being met, if not, what are the steps that should be taken to meet successfully.

Matching algorithms to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Some forensic accountants specialize in forensic analytics which is the procurement and analysis of electronic data to reconstruct, detect, or otherwise support a claim of financial fraud. The main steps in forensic analytics are data collection, data preparation, data analysis, and reporting. For example, forensic analytics may be used to review an employee's purchasing card activity to assess whether any of the purchases were diverted or divertible for personal use.
By implementing a comprehensive risk management framework, organizations can proactively identify, assess, and mitigate fraud risks, thereby enhancing their resilience and safeguarding their assets and reputation.

Role of Data Analytics: Data analytics enables organizations to extract valuable insights from diverse data sources, including transaction records, customer information, and digital footprints. By leveraging data analytics, organizations can:

- Detect patterns and trends indicative of fraudulent activities.

- Identify anomalies and deviations from normal behavior.

- Predict and prevent fraud before it occurs.

- Optimize fraud detection processes and reduce false positives.

Techniques for Data Analysis: Several data analytics techniques are commonly used for fraud detection, including:

- Descriptive Analytics: Summarizes historical data to understand past trends and patterns.

- Diagnostic Analytics: Analyzes data to identify the root causes of fraudulent activities.

- Predictive Analytics: Utilizes statistical algorithms and machine learning models to predict future fraudulent behavior based on historical data.

- Prescriptive Analytics: Recommends actions to prevent or mitigate fraudulent activities based on predictive insights.

Predictive Modeling for Fraud Detection: Predictive modeling is a powerful technique used in fraud detection to identify and prioritize suspicious activities. Key steps in predictive modeling for fraud detection include:

- Data Preparation: Cleansing, transforming, and aggregating data from diverse sources to create a unified dataset.

- Feature Selection: Identifying relevant features or variables that are predictive of fraudulent behavior.

- Model Development: Building predictive models using machine learning algorithms, such as logistic regression, decision trees, random forests, or neural networks.

- Model Evaluation: Assessing the performance of predictive models using metrics such as accuracy, precision, recall, and area under the receiver operating characteristic (ROC) curve.

- Deployment and Monitoring: Deploying predictive models in production environments and continuously monitoring their performance to ensure effectiveness and reliability.

Artificial intelligence:

Fraud detection is a knowledge-intensive activity. The main AI techniques used for fraud detection include:

Data mining to classify, cluster, and segment the data and automatically find associations and rules in the data that may signify interesting patterns, including those related to fraud.

Expert systems to encode expertise for detecting fraud in the form of rules.

Pattern recognition to detect approximate classes, clusters, or patterns of suspicious behavior either automatically (unsupervised) or to match given inputs.

Machine learning techniques to automatically identify characteristics of fraud.

Neural nets to independently generate classification, clustering, generalization, and forecasting that can then be compared against conclusions raised in internal audits or formal financial documents.

Other techniques such as link analysis, Bayesian networks, decision theory, and sequence matching are also used for fraud detection.[4] A new and novel technique called System properties approach has also been employed where ever rank data is available.

Statistical analysis of research data is the most comprehensive method for determining if data fraud exists. Data fraud as defined by the Office of Research Integrity (ORI) includes fabrication, falsification and plagiarism.

Machine learning and data mining:

Early data analysis techniques were oriented toward extracting quantitative and statistical data characteristics. These techniques facilitate useful data interpretations and can help to get better insights into the processes behind the data. Although the traditional data analysis techniques can indirectly lead us to knowledge, it is still created by human analysts.

To go beyond, a data analysis system has to be equipped with a substantial amount of background knowledge, and be able to perform reasoning tasks involving that knowledge and the data provided. In effort to meet this goal, researchers have turned to ideas from the machine learning field. This is a natural source of ideas, since the machine learning task can be described as turning background knowledge and examples (input) into knowledge (output).

If data mining results in discovering meaningful patterns, data turns into information. Information or patterns that are novel, valid and potentially useful are not merely information, but knowledge. One speaks of discovering knowledge, before hidden in the huge amount of data, but now revealed.

The machine learning and artificial intelligence solutions may be classified into two categories: 'supervised' and 'unsupervised' learning. These methods seek for accounts, customers, suppliers, etc. that behave 'unusually' in order to output suspicion scores, rules or visual anomalies, depending on the method.

Whether supervised or unsupervised methods are used, note that the output gives us only an indication of fraud likelihood. No stand alone statistical analysis can assure that a particular object is a fraudulent one, but they can identify them with very high degrees of accuracy. As a result, effective collaboration between machine learning model and human analysts is vital to the success of fraud detection applications

Supervised learning:

In supervised learning, a random sub-sample of all records is taken and manually classified as either 'fraudulent' or 'non-fraudulent' (task can be decomposed on more classes to meet algorithm requirements). Relatively rare events such as fraud may need to be over sampled to get a big enough sample size. These manually classified records are then used to train a supervised machine learning algorithm. After building a model using this training data, the algorithm should be able to classify new records as either fraudulent or non-fraudulent.

Supervised neural networks, fuzzy neural nets, and combinations of neural nets and rules, have been extensively explored and used for detecting fraud in mobile phone networks and financial statement fraud.

Bayesian learning neural network is implemented for credit card fraud detection, telecommunications fraud, auto claim fraud detection, and medical insurance fraud.

Hybrid knowledge/statistical-based systems, where expert knowledge is integrated with statistical power, use a series of data mining techniques for the purpose of detecting cellular clone fraud. Specifically, a rule-learning program to uncover indicators of fraudulent behaviour from a large database of customer transactions is implemented.

Cahill et al. (2000) design a fraud signature, based on data of fraudulent calls, to detect telecommunications fraud. For scoring a call for fraud its probability under the account signature is compared to its probability under a fraud signature. The fraud signature is updated sequentially, enabling event-driven fraud detection.

Link analysis comprehends a different approach. It relates known fraudsters to other individuals, using record linkage and social network methods.

This type of detection is only able to detect frauds similar to those which have occurred previously and been classified by a human. To detect a novel type of fraud may require the use of an unsupervised machine learning algorithm.

Unsupervised learning

In contrast, unsupervised methods don't make use of labelled records.

Bolton and Hand use Peer Group Analysis and Break Point Analysis applied on spending behaviour in credit card accounts. Peer Group Analysis detects individual objects that begin to behave in a way different from objects to which they had previously been similar. Another tool Bolton and Hand develop for behavioural fraud detection is Break Point Analysis. Unlike Peer Group Analysis, Break Point Analysis operates on the account level. A break point is an observation where anomalous behaviour for a particular account is detected. Both the tools are applied on spending behaviour in credit card accounts.

A combination of unsupervised and supervised methods for credit card fraud detection is in Carcillo et al (2019).

Geolocation:

Online retailers and payment processors use geolocation to detect possible credit card fraud by comparing the user's location to the billing address on the account or the shipping address provided. A mismatch – an order placed from the US on an account number from Tokyo, for example – is a strong indicator of potential fraud. IP address geolocation can be also used in fraud detection to match billing address postal code or area code. Banks can prevent "phishing" attacks, money laundering and other security breaches by determining the user's location as part of the authentication process. Whois databases can also help verify IP addresses and registrants.

Government, law enforcement and corporate security teams use geolocation as an investigatory tool, tracking the Internet routes of online attackers to find the perpetrators and prevent future attacks from the same location.

Available datasets:

A major limitation for the validation of existing fraud detection methods is the lack of public datasets. One of the few examples is the Credit Card Fraud Detection dataset made available by the ULB Machine Learning Group.

The detection of fraudulent activities on a large scale is possible with the harvesting of massive amounts of financial data paired with predictive analytics or forensic analytics, the use of electronic data to reconstruct or detect financial fraud.

Using computer-based analytic methods in particular allows for surfacing of errors, anomalies, inefficiencies, irregularities, and biases which often refer to fraudsters gravitating to certain dollar amounts to get past internal control thresholds. These high-level tests include tests related to Benford's Law and possibly also those statistics known as descriptive statistics. High-level tests are always followed by more focused tests to look for small samples of highly irregular transactions. The familiar methods of correlation and time-series analysis can also be used to detect fraud and other irregularities.

Participants of a 2010 survey by the Association of Certified Fraud Examiners estimated that the typical organization loses five percent of its annual revenue to fraud, with a median loss of $160,000. Fraud committed by owners and executives were more than nine times as costly as employee fraud. The industries most commonly affected are banking, manufacturing, and government.

CHAPTER 4: FRAUD DETECTION TECHNIQUES

Fraud detection techniques encompass a range of strategies and methodologies aimed at identifying and preventing fraudulent activities. From traditional rule-based systems to advanced machine learning algorithms, organizations employ various techniques to detect and mitigate fraud effectively.

1. Rule-based Systems: Rule-based systems use predefined rules and thresholds to flag suspicious activities based on predefined criteria. These rules are typically based on known patterns of fraudulent behavior or deviations from normal behavior. Examples include:

•Transaction Monitoring Rules: Flagging transactions above a certain threshold or with unusual characteristics.

•Identity Verification Rules: Checking for inconsistencies in customer information or documentation.

2. Anomaly Detection: Anomaly detection techniques identify outliers or deviations from normal behavior that may indicate fraudulent activities. These techniques include:

•Statistical Methods: Analyzing deviations from statistical norms, such as mean and standard deviation.

•Machine Learning Algorithms: Training models to detect unusual patterns in data, such as clustering or outlier detection algorithms.

3. Machine Learning Approaches: Machine learning algorithms enable organizations to detect fraud by learning from historical data and identifying patterns indicative of fraudulent behavior. Common machine learning approaches for fraud detection include:

•Supervised Learning: Training models on labeled datasets to classify transactions as fraudulent or legitimate.

•Unsupervised Learning: Identifying patterns and anomalies in data without labeled examples.

•Semi-supervised Learning: Combining labeled and unlabeled data to improve fraud detection accuracy.

4. Behavior Analysis: Behavior analysis techniques focus on identifying deviations from typical behavior patterns, such as changes in spending habits or transaction frequency. These techniques include:

•Customer Profiling: Creating profiles of normal behavior for individual customers and flagging deviations from these profiles.

•Social Network Analysis: Analyzing connections and relationships between entities to detect suspicious patterns, such as collusive fraud rings.

Rule Based System:

In computer science, a rule-based system is a computer system in which domain-specific knowledge is represented in the form of rules and general-purpose reasoning is used to solve problems in the domain.

Two different kinds of rule-based systems emerged within the field of artificial intelligence in the 1970s:

Production systems, which use if-then rules to derive actions from conditions.
Logic programming systems, which use conclusion if conditions rules to derive conclusions from conditions.
The differences and relationships between these two kinds of rule-based system has been a major source of misunderstanding and confusion.

Both kinds of rule-based systems use either forward or backward chaining, in contrast with imperative programs, which execute commands listed sequentially. However, logic programming systems have a logical interpretation, whereas production systems do not.

Production system rules
A classic example of a production rule-based system is the domain-specific expert system that uses rules to make deductions or choices. For example, an expert system might help a doctor choose the correct diagnosis based on a cluster of symptoms, or select tactical moves to play a game.

Rule-based systems can be used to perform lexical analysis to compile or interpret computer programs, or in natural language processing.

Rule-based programming attempts to derive execution instructions from a starting set of data and rules. This is a more indirect method than that employed by an imperative programming language, which lists execution steps sequentially.

Construction

A typical rule-based system has four basic components:

A list of rules or rule base, which is a specific type of knowledge base.
An inference engine or semantic reasoner, which infers information or takes action based on the interaction of input and the rule base. The interpreter executes a production system program by performing the following match-resolve-act cycle

Match: In this first phase, the condition sides of all productions are matched against the contents of working memory. As a result a set (the conflict set) is obtained, which consists of instantiations of all satisfied productions. An instantiation of a production is an ordered list of working memory elements that satisfies the condition side of the production.

Conflict-resolution: In this second phase, one of the production instantiations in the conflict set is chosen for execution. If no productions are satisfied, the interpreter halts.
Act: In this third phase, the actions of the production selected in the conflict-resolution phase are executed. These actions may change the contents of working memory. At the end of this phase, execution returns to the first phase.

Temporary working memory, which is a database of facts.
A user interface or other connection to the outside world through which input and output signals are received and sent.

Whereas the matching phase of the inference engine has a logical interpretation, the conflict resolution and action phases do not. Instead, "their semantics is usually described as a series of applications of various state-changing operators, which often gets quite involved (depending on the choices made in deciding which ECA rules fire, when, and so forth), and they can hardly be regarded as declarative".

Logic programming rules

The logic programming family of computer systems includes the programming language Prolog, the database language Datalog and the knowledge representation and problem-solving language Answer Set Programming (ASP). In all of these languages, rules are written in the form of clauses:

A :- B1, ..., Bn.
and are read as declarative sentences in logical form:

A if B1 and ... and Bn.
In the simplest case of Horn clauses (or "definite" clauses), which are a subset of first-order logic, all of the A, B1, ..., Bn are atomic formulae.

Although Horn clause logic programs are Turing complete, for many practical applications, it is useful to extend Horn clause programs by allowing negative conditions, implemented by negation as failure. Such extended logic programs have the knowledge representation capabilities of a non-monotonic logic.

Differences and relationships between production rules and logic programming rules

The most obvious difference between the two kinds of systems is that production rules are typically written in the forward direction, if A then B, and logic programming rules are typically written in the backward direction, B if A. In the case of logic programming rules, this difference is superficial and purely syntactic. It does not affect the semantics of the rules. Nor does it affect whether the rules are used to reason backwards, Prolog style, to reduce the goal B to the subgoals A, or whether they are used, Datalog style, to derive B from A.

In the case of production rules, the forward direction of the syntax reflects the stimulus-response character of most production rules, with the stimulus A coming before the response B. Moreover, even in cases when the response is simply to draw a conclusion B from an assumption A, as in modus ponens, the match-resolve-act cycle is restricted to reasoning forwards from A to B. Reasoning backwards in a production system would require the use of an entirely different kind of inference engine.

In his Introduction to Cognitive Science,[8] Paul Thagard includes logic and rules as alternative approaches to modelling human thinking. He does not consider logic programs in general, but he considers Prolog to be, not a rule-based system, but "a programming language that uses logic representations and deductive techniques".

He argues that rules, which have the form IF condition THEN action, are "very similar" to logical conditionals, but they are simpler and have greater psychological plausibility Among other differences between logic and rules, he argues that logic uses deduction, but rules use search and can be used to reason either forward or backward . Sentences in logic "have to be interpreted as universally true", but rules can be defaults, which admit exceptions. He does not observe that all of these features of rules apply to logic programming systems.

Anomaly Detection:

In data analysis, anomaly detection (also referred to as out-lier detection and sometimes as novelty detection) is generally understood to be the identification of rare items, events or observations which deviate significantly from the majority of the data and do not conform to a well defined notion of normal behavior. Such examples may arouse suspicions of being generated by a different mechanism, or appear inconsistent with the remainder of that set of data.

Anomaly detection finds application in many domains including cybersecurity, medicine, machine vision, statistics, neuroscience, law enforcement and financial fraud to name only a few. Anomalies were initially searched for clear rejection or omission from the data to aid statistical analysis, for example to compute the mean or standard deviation. They were also removed to better predictions from models such as linear regression, and more recently their removal aids the performance of machine learning algorithms. However, in many applications anomalies themselves are of interest and are the observations most desirous in the entire data set, which need to be identified and separated from noise or irrelevant outliers.

CHAPTER 5: TECHNOLOGY IN FRAUD DETECTION

Advancements in technology have revolutionized fraud detection, enabling organizations to deploy sophisticated tools and techniques to combat increasingly complex fraudulent activities. From artificial intelligence (AI) and machine learning to blockchain technology and biometric authentication, organizations leverage various technologies to enhance their fraud detection capabilities.

1. AI and Machine Learning Applications: AI and machine learning play a pivotal role in fraud detection by enabling organizations to analyze vast amounts of data and identify patterns indicative of fraudulent behavior.

Key applications include:

•Predictive Modeling: Building machine learning models to predict and prevent fraudulent activities based on historical data.

•Anomaly Detection: Leveraging machine learning algorithms to identify outliers and deviations from normal behavior.

•Natural Language Processing (NLP): Analyzing unstructured data, such as text documents and emails, to detect signs of fraudulent activities.

•Deep Learning: Utilizing deep neural networks to uncover complex patterns and relationships in data for fraud detection.

2. Blockchain Technology: Blockchain technology offers secure and transparent transactional records, making it an ideal solution for fraud prevention in industries such as finance and supply chain management.

Key features include:

•Immutable Ledger: Providing tamper-resistant records of transactions, reducing the risk of data manipulation or fraud.

•Smart Contracts: Automating contract execution and enforcement, reducing the risk of fraudulent transactions or disputes.

•Supply Chain Traceability: Enhancing transparency and accountability in supply chains by tracking the movement of goods from origin to destination.

3. Biometric Authentication: Biometric authentication enhances security by verifying individuals' identities based on unique biological traits, such as fingerprints, iris patterns, or facial features.

Key applications include:

•Facial Recognition: Authenticating users based on facial characteristics captured by cameras or imaging devices.

•Fingerprint Scanning: Verifying users' identities by analyzing their unique fingerprint patterns .

•Voice Recognition: Authenticating users based on their unique vocal characteristics and speech patterns.

4. Fraud Detection Tools and Platforms: Numerous software solutions and platforms offer advanced fraud detection capabilities, integrating AI, machine learning, and data analytics to identify and prevent fraudulent activities.

These tools provide:

•Real-time Monitoring: Monitoring transactions and activities in real-time to detect suspicious behavior as it occurs.

•Pattern Recognition: Identifying patterns and trends indicative of fraudulent activities across diverse datasets.

•Alerting and Reporting: Generating alerts and reports to notify stakeholders of potential fraud risks and incidents.

5. Cybersecurity Measures: Robust cybersecurity measures, such as encryption, multi-factor authentication, and intrusion detection systems, are essential for protecting sensitive data and preventing unauthorized access, reducing the risk of fraud and data breaches.

By leveraging advanced technologies such as AI, machine learning, blockchain, biometric authentication, and fraud detection tools, organizations can enhance their capabilities to detect, prevent, and mitigate fraudulent activities effectively in today's digital landscape.

Artificial intelligence (AI):

Artificial intelligence (AI) has been used in applications throughout industry and academia. Similar to electricity or computers, AI serves as a general-purpose technology that has numerous applications. Its applications span language translation, image recognition, decision-making, credit scoring, e-commerce and various other domains. AI which accommodates such technologies as machines being equipped perceive, understand, act and learning a scientific discipline.

A recommendation system predicts the rating or preference a user would give to an item. Artificial intelligence recommendation systems are designed to offer suggestions based on previous behavior. These systems have been used by companies such as Netflix, Amazon, Instagram and YouTube, where they generate personalized playlists, product suggestions, and video recommendations.

Machine learning is also used in web feeds such as for determining which posts should show up in social media feeds. Various types of social media analysis also make use of machine learning and there is research into its use for (semi-)automated tagging/enhancement/correction of online misinformation and related filter bubbles.

AI is used to target web advertisements to those most likely to click or engage in them. It is also used to increase time spent on a website by selecting attractive content for the viewer. It can predict or generalize the behavior of customers from their digital footprints.Both AdSense and Facebook use AI for advertising.

Online gambling companies use AI to improve customer targeting.

Personality computing AI models add psychological targeting to more traditional social demographics or behavioral targeting. AI has been used to customize shopping options and personalize offers.

Intelligent personal assistants use AI to understand many natural language requests in other ways than rudimentary commands. Common examples are Apple's Siri, Amazon's Alexa, and a more recent AI, ChatGPT by OpenAI.

Bing Chat has used artificial intelligence as part of its search engine.

Machine learning can be used to fight against spam, scams, and phishing. It can scrutinize the contents of spam and phishing attacks to attempt to identify malicious elements. Some models built via machine learning algorithms have over 90% accuracy in distinguishing between spam and legitimate emails. These models can be refined from new data and evolving spam tactics. Machine learning also analyzes traits such as sender behavior, email header information, and attachment types.

Speech translation technology attempts to convert one language's spoken words into another. This potentially reduces language barriers in global commerce and cross-cultural exchange by allowing speakers of various languages to communicate with one another.

AI has been used to automatically translate spoken language and textual content, in products such as Microsoft Translator, Google Translate and DeepL Translator. Additionally, research and development are in progress to decode and conduct animal communication.

Meaning is conveyed not only by text, but also through usage and context (see semantics and pragmatics). As a result, the two primary categorization approaches for machine translations are statistical and neural machine translations (NMTs). The old method of performing translation was to use a statistical machine translation (SMT) methodology to forecast the best probable output with specific algorithms. However, with NMT, the approach employs dynamic algorithms to achieve better translations based on context.

AI has been used in facial recognition systems, with a 99% accuracy rate. Some examples are Apple's Face ID and Android's Face Unlock, which are used to secure mobile devices.

Image labeling has been used by Google to detect products in photos and to allow people to search based on a photo. Image labeling has also been demonstrated to generate speech to describe images to blind people. Facebook's DeepFace identifies human faces in digital images.

Games have been a major application of AI's capabilities since the 1950s. In the 21st century, AIs have beaten human players in many games, including chess (Deep Blue), Jeopardy! (Watson), Go (AlphaGo), poker (Pluribus and Cepheus), E-sports (StarCraft), and general game playing (AlphaZero and MuZero). AI has replaced hand-coded algorithms in most chess programs. Unlike go or chess, poker is an imperfect-information game, so a program that plays poker has to reason under uncertainty. The general game players work using feedback from the game system, without knowing the rules.

Blockchain Technology:

A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). Since each block contains information about the previous block, they effectively form a chain (compare linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.

A blockchain was created by a person (or group of people) using the name (or pseudonym) Satoshi Nakamoto in 2008 to serve as the public distributed ledger for bitcoin cryptocurrency transactions, based on previous work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. The implementation of the blockchain within bitcoin made it the first digital currency to solve the double-spending problem without the need for a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. The blockchain may be considered a type of payment rail.

Private blockchains have been proposed for business use. Computer world called the marketing of such privatized blockchains without a proper security model "snake oil"; however, others have argued that per missioned blockchains, if carefully designed, may be more decentralized and therefore more secure in practice than permission less ones.

CHAPTER 6: CASE STUDIES

Real-world case studies provide valuable insights into the challenges organizations face in fraud detection and risk management, as well as the strategies and solutions employed to address them. Examining these cases offers practical lessons and best practices for organizations seeking to enhance their fraud detection capabilities and mitigate risks effectively.

1. **Enron Corporation Scandal:**

The Enron Corporation scandal, one of the largest corporate fraud cases in history, underscores the importance of robust internal controls and ethical leadership in fraud prevention. Enron, once regarded as one of the most innovative companies in the United States, collapsed in 2001 due to accounting fraud and corporate mismanagement. Key lessons from the Enron scandal include the need for transparency in financial reporting, independent oversight of corporate governance practices, and the importance of whistleblower protections in uncovering fraudulent activities.

2. **Bernie Madoff Ponzi Scheme:**

The Bernie Madoff Ponzi scheme exemplifies the devastating impact of investment fraud on investors and financial markets. Bernie Madoff, a prominent Wall Street financier, orchestrated one of the largest Ponzi schemes in history, defrauding investors of billions of dollars over several decades. The Madoff case highlights the importance of due diligence and skepticism in investment decisions, as well as the need for regulatory authorities to enhance oversight and enforcement of financial markets to prevent similar fraud schemes in the future.

3. **Target Data Breach:**

The Target data breach of 2013 serves as a cautionary tale for organizations regarding the importance of cybersecurity and data protection in fraud prevention. Hackers gained access to Target's network through a third-party vendor and stole credit card information and personal data of millions of customers. The Target breach underscores the need for robust cybersecurity measures, including encryption, network segmentation, and intrusion detection systems, to protect sensitive customer information from cyber threats and data breaches.

4. **Wells Fargo Fake Accounts Scandal:**

The Wells Fargo fake accounts scandal highlights the risks of unethical sales practices and inadequate internal controls in the banking industry. Wells Fargo employees opened millions of unauthorized accounts and credit cards for customers without their consent to meet aggressive sales targets. The scandal resulted in significant reputational damage, regulatory fines, and legal settlements for Wells Fargo. Key lessons from the Wells Fargo scandal include the importance of ethical leadership, whistleblower protections, and strong internal controls to prevent misconduct and fraudulent behavior within organizations.

5. **Wirecard Accounting Scandal:**

The Wirecard accounting scandal illustrates the challenges organizations face in detecting and preventing financial fraud, particularly in the fintech sector. Wirecard, a German payment processing company, misrepresented its financial statements and inflated revenue through fraudulent accounting practices, deceiving investors and regulators. The Wirecard scandal underscores the importance of independent auditing, regulatory oversight, and transparency in financial reporting to maintain trust and credibility in the financial markets.

By analyzing these case studies and understanding the underlying factors contributing to fraud incidents, organizations can implement proactive measures and best practices to enhance their fraud detection capabilities, mitigate risks, and safeguard their assets and reputation.

Enron Corporation Scandal:

The Enron scandal was an accounting scandal involving Enron Corporation, an American energy company based in Houston, Texas. When news of widespread fraud within the company became public in October 2001, the company declared bankruptcy and its accounting firm, Arthur Andersen – then one of the five largest audit and accountancy partnerships in the world – was effectively dissolved. In addition to being the largest bankruptcy reorganization in U.S. history at that time, Enron was cited as the biggest audit failure.

Enron was formed in 1985 by Kenneth Lay after merging Houston Natural Gas and InterNorth. Several years later, when Jeffrey Skilling was hired, Lay developed a staff of executives that – by the use of accounting loopholes, the misuse of mark-to-market accounting, special purpose entities, and poor financial reporting – were able to hide billions of dollars in debt from failed deals and projects. Chief Financial Officer Andrew Fastow and other executives misled Enron's board of directors and audit committee on high-risk accounting practices and pressured Arthur Andersen to ignore the issues.

Shareholders filed a $40 billion lawsuit (and were eventually partially compensated with $7.2 billion), after the company's stock price, which achieved a high of US$90.75 per share in mid-2000, plummeted to less than $1 by the end of November 2001. The Securities and Exchange Commission (SEC) began an investigation, and rival Houston competitor Dynegy offered to purchase the company at a very low price. The deal failed, and on December 2, 2001, Enron filed for bankruptcy under Chapter 11 of the United States Bankruptcy Code. Enron's $63.4 billion in assets made it the largest corporate bankruptcy in U.S. history until the WorldCom scandal the following year.

Many executives at Enron were indicted for a variety of charges and some were later sentenced to prison, including former CEO Jeffrey Skilling. Then CEO and Chairman Kenneth Lay was indicted and convicted, but died before being sentenced. Arthur Andersen LLC was found guilty of illegally destroying documents relevant to the SEC investigation, which voided its license to audit public companies and effectively closed the firm. By the time the ruling was overturned at the Supreme Court, Arthur Andersen had lost the majority of its customers and had ceased operating. Enron employees and shareholders received limited returns in lawsuits, despite losing billions in pensions and stock prices.

As a consequence of the scandal, new regulations and legislation were enacted to expand the accuracy of financial reporting for public companies. One piece of legislation, the Sarbanes–Oxley Act, increased penalties for destroying, altering, or fabricating records in federal investigations or for attempting to defraud shareholders. The act also increased the accountability of auditing firms to remain unbiased and independent of their clients.

Rise of Enron

Kenneth Lay in a July 2004 mugshot

In 1985, Kenneth Lay merged the natural gas pipeline companies of Houston Natural Gas and InterNorth to form Enron.[6]:3 In the early 1990s, he helped to initiate the selling of electricity at market prices and, soon after, Congress approved legislation deregulating the sale of natural gas. The resulting markets made it possible for traders such as Enron to sell energy at higher prices, thereby significantly increasing its revenue. After producers and local governments decried the resultant price volatility and asked for increased regulation, strong lobbying on the part of Enron and others prevented such regulation.

As Enron became the largest seller of natural gas in North America by 1992, its trading of gas contracts earned $122 million (before interest and taxes), the second largest contributor to the company's net income. The November 1999 creation of the EnronOnline trading website allowed the company to better manage its contracts trading business.

In an attempt to achieve further growth, Enron pursued a diversification strategy. The company owned and operated a variety of assets including gas pipelines, electricity plants, paper plants, water plants, and broadband services across the globe. Enron also gained additional revenue by trading contracts for the same array of products and services with which it was involved. This included setting up power generation plants in developing countries and emerging markets including the Philippines (Subic Bay), Indonesia and India (Dabhol).

Enron's stock increased from the start of the 1990s until year-end 1998 by 311%, only modestly higher than the average rate of growth in the Standard & Poor 500 index. However, the stock increased by 56% in 1999 and a further 87% in 2000, compared to a 20% increase and a 10% decrease for the index during the same years. By December 31, 2000, Enron's stock was priced at $83.13 and its market capitalization exceeded $60 billion, 70 times earnings and six times book value, an indication of the stock market's high expectations about its future prospects. In addition, Enron was rated the most innovative large company in America in Fortune's Most Admired Companies survey.

Causes of downfall

Enron had published a manual of ethics earlier.
Enron's complex financial statements were confusing to shareholders and analysts. In addition, its complex business model and unethical practices required that the company use accounting limitations to misrepresent earnings and modify the balance sheet to indicate favorable performance. Furthermore, some speculative business ventures proved disastrous.

The combination of these issues later resulted in the bankruptcy of Enron, and the majority of them were perpetuated by the indirect knowledge or direct actions of Lay, Jeffrey Skilling, Andrew Fastow, and other executives such as Rebecca Mark. Lay served as the chairman of Enron in its last few years, and approved of the actions of Skilling and Fastow, although he did not always inquire about the details. Skilling constantly focused on meeting Wall Street expectations, advocated the use of mark-to-market accounting (accounting based on market value, which was then inflated) and pressured Enron executives to find new ways to hide its debt. Fastow and other executives "created off-balance-sheet vehicles, complex financing structures, and deals so bewildering that few people could understand them."

Revenue recognition

Further information: Revenue recognition
Enron earned profits by providing services such as wholesale trading and risk management in addition to building and maintaining electric power plants, natural gas pipelines, storage, and processing facilities. When accepting the risk of buying and selling products, merchants are allowed to report the selling price as revenues and the products' costs as cost of goods sold. In contrast, an "agent" provides a service to the customer, but does not take the same risks as merchants for buying and selling. Service providers, when classified as agents, may report trading and brokerage fees as revenue, although not for the full value of the transaction.

Although trading companies such as Goldman Sachs and Merrill Lynch used the conventional "agent model" for reporting revenue (where only the trading or brokerage fee would be reported as revenue), Enron instead elected to report the entire value of each of its trades as revenue. This "merchant model" was considered much more aggressive in the accounting interpretation than the agent model. Enron's method of reporting inflated trading revenue was later adopted by other companies in the energy trading industry in an attempt to stay competitive with the company's large increase in revenue. Other energy companies such as Duke Energy, Reliant Energy, and Dynegy joined Enron in the largest 50 of the revenue-based Fortune 500 owing mainly to their adoption of the same trading revenue accounting as Enron.

Between 1996 and 2000, Enron's revenues increased by more than 750%, rising from $13.3 billion in 1996 to $100.7 billion in 2000. This expansion of 65% per year was extraordinary in any industry, including the energy industry, which typically considered growth of 2–3% per year to be respectable. For just the first nine months of 2001, Enron reported $138.7 billion in revenues, placing the company at the sixth position on the Fortune Global 500.

Enron also used creative accounting tricks and purposefully misclassified loan transactions as sales close to quarterly reporting deadlines, similar to the Lehman Brothers Repo 105 scheme in the 2008 financial crisis, or the currency swap concealment of Greek debt by Goldman Sachs. In Enron's case, Merrill Lynch bought Nigerian barges with an alleged buyback guarantee by Enron shortly before the earnings deadline. According to the government, Enron misreported a bridge loan as a true sale, then bought back the barges a few months later. Merrill Lynch executives were tried and in November 2004 convicted for aiding Enron in fraudulent accounting activities. These charges were thrown out on appeal in 2006, after the Merrill Lynch executives had spent nearly a year in prison, with the 5th U.S. Circuit Court of Appeals in New Orleans calling the conspiracy and wire fraud charges "flawed". Expert observers said that the reversal was highly unusual for the 5th Circuit, commenting that the conviction must have had serious issues in order to be overturned. The Justice Department decided not to retry the case after the reversal of the verdict.

Mark-to-market accounting

Further information: Mark-to-market accounting

In Enron's natural gas business, the accounting had been fairly straightforward: in each time period, the company listed actual costs of supplying the gas and actual revenues received from selling it. However, when Skilling joined Enron, he demanded that the trading business adopt mark-to-market accounting, claiming that it would represent "true economic value". Enron became the first nonfinancial company to use the method to account for its complex long-term contracts. Mark-to-market accounting requires that once a long-term contract has been signed, income is estimated as the present value of net future cash flow. Often, the viability of these contracts and their related costs were difficult to estimate. Owing to the large discrepancies between reported profits and cash, investors were typically given false or misleading reports. Under this method, income from projects could be recorded, although the firm might never have received the money, with this income increasing financial earnings on the books. However, because in future years the profits could not be included, new and additional income had to be included from more projects to develop additional growth to appease investors. As one Enron competitor stated, "If you accelerate your income, then you have to keep doing more and more deals to show the same or rising income." Despite potential pitfalls, the U.S. Securities and Exchange Commission (SEC) approved the accounting method for Enron in its trading of natural gas futures contracts on January 30, 1992. However, Enron later expanded its use to other areas in the company to help it meet Wall Street projections.

For one contract, in July 2000, Enron and Blockbuster Video signed a 20-year agreement to introduce on-demand entertainment to various U.S. cities by year's end. After several pilot projects, Enron claimed estimated profits of more than $110 million from the deal, even though analysts questioned the technical viability and market demand of the service. But in March 2001, the parties withdrew from the contract. Enron continued to claim future profits, even though the deal resulted in a loss.

Bernie Madoff Ponzi Scheme:

April 29, 1938 – April 14, 2021) was an American financial criminal and financier who was the admitted mastermind of the largest known Ponzi scheme in history, worth an estimated $65 billion. He was at one time chairman of the Nasdaq stock exchange. Madoff's firm had two basic units: a stock brokerage and an asset management business; the Ponzi scheme was centered in the asset management business.

Madoff founded a penny stock brokerage in 1960, which eventually grew into Bernard L. Madoff Investment Securities. He served as the company's chairman until his arrest on December 11, 2008. That year, the firm was the 6th-largest market maker in S&P 500 stocks. While the stock brokerage part of the business had a public profile, Madoff tried to keep his asset management business low profile and exclusive.

At the firm, he employed his brother Peter Madoff as senior managing director and chief compliance officer, Peter's daughter Shana Madoff as the firm's rules and compliance officer and attorney, and his now-deceased sons Mark Madoff and Andrew Madoff. Peter was sentenced to 10 years in prison in 2012, and Mark hanged himself in 2010, exactly two years after his father's arrest. Andrew died of lymphoma on September 3, 2014.

On December 10, 2008, Madoff's sons Mark and Andrew told authorities that their father had confessed to them that the asset management unit of his firm was a massive Ponzi scheme, and quoted him as saying that it was "one big lie". The following day, agents from the Federal Bureau of Investigation arrested Madoff and charged him with one count of securities fraud. The U.S. Securities and Exchange Commission (SEC) had previously conducted multiple investigations into his business practices but had not uncovered the massive fraud. On March 12, 2009, Madoff pleaded guilty to 11 federal felonies and admitted to turning his wealth management business into a massive Ponzi scheme.

The Madoff investment scandal defrauded thousands of investors of billions of dollars. Madoff said that he began the Ponzi scheme in the early 1990s, but an ex-trader admitted in court to faking records for Madoff since the early 1970s. Those charged with recovering the missing money believe that the investment operation may never have been legitimate. The amount missing from client accounts was almost $65 billion, including fabricated gains. The Securities Investor Protection Corporation (SIPC) trustee estimated actual direct losses to investors of $18 billion, of which $14.418 billion has been recovered and returned, while the search for additional funds continues. On June 29, 2009, Madoff was sentenced to 150 years in prison, the maximum sentence allowed. On April 14, 2021, he died at the Federal Medical Center, Butner, in North Carolina, from chronic kidney disease.

Target Data Breach:

On December 18, 2013, security expert Brian Krebs broke news that Target was investigating a major data breach "potentially involving millions of customer credit and debit card records". On December 19, Target confirmed the incident via a press release, revealing that the hack took place between November 27 and December 15, 2013. Target warned that up to 40 million consumer credit and debit cards may have been compromised. Hackers gained access to customer names, card numbers, expiration dates, and CVV security codes of the cards issued by financial institutions. On December 27, Target disclosed that debit card PIN data had also been stolen, albeit in encrypted form, reversing an earlier stance that PIN data was not part of the breach.

Target noted that the accessed PIN numbers were encrypted using Triple DES and has stated the PINs remain "safe and secure" due to the encryption. On January 10, 2014, Target disclosed that the names, mailing addresses, phone numbers or email addresses of up to 70 million additional people had also been stolen, bringing the possible number of customers affected up to 110 million.

According to Bloomberg Businessweek, Target's computer security team was notified of the breach via the FireEye security service they employed, had ample time to disrupt the theft of credit cards and other customer data, but did not act to prevent theft from being carried out.

Target encouraged customers who shopped at its US stores (online orders were not affected) during the specified timeframe to closely monitor their credit and debit cards for irregular activity. The retailer confirmed that it is working with law enforcement, including the United States Secret Service, "to bring those responsible to justice". The data breach has been called the second-largest retail cyber attack in history, and has been compared to the 2009 non-retail Heartland Payment Systems compromise, which affected 130 million credit cards, and to the 2007 retail TJX Companies compromise, which affected 90 million people. As an apology to the public, all Target stores in the United States gave retail shoppers a 10% storewide discount for the weekend of December 21–22, 2013. Target has offered free credit monitoring via Experian to affected customers. Target reported total transactions for the same time last year were down 3-4%, as of December 23, 2013.

According to Time magazine, a 17-year-old Russian teen was suspected to be the author of the Point of Sale (POS) malware program, "BlackPOS", which was used by others to attack unpatched Windows computers used at Target. The teen denied the allegation. Later, a 23-year-old Russian, Rinat Shabayev, claimed to be the malware author.

On January 29, 2014, a Target spokeswoman said that the individual(s) who hacked its customers' data had stolen credentials from a store vendor, but did not elaborate on which vendor or which credentials were taken.

As the fallout of the data breach continued, on March 6, 2014, Target announced the resignation of its chief information officer and an overhaul of its information security practices. In a further step to restore faith in customers, the company advised that it will look externally for appointments to both the CIO role and a new chief compliance officer role.

Wells Fargo Fake Accounts Scandal:

In September 2016, Wells Fargo was issued a combined total of $185 million in fines for opening over 1.5 million checking and savings accounts and 500,000 credit cards on behalf of customers without their consent. The Consumer Financial Protection Bureau (CFPB) issued $100 million in fines, the largest in the agency's five-year history, along with $50 million in fines from the City and County of Los Angeles, and $35 million in fines from the Office of Comptroller of the Currency. The scandal was caused by an incentive-compensation program for employees to create new accounts. It led to the firing of nearly 5,300 employees and $5 million being set aside for customer refunds on fees for accounts the customers never wanted. Carrie Tolstedt, who headed the department, retired in July 2016 and received $124.6 million in stock, options, and restricted Wells Fargo shares as a retirement package.

On October 12, 2016, John Stumpf, the then chairman and CEO, announced that he would be retiring amidst the scandals. President and chief operating officer Timothy J. Sloan succeeded Stumpf, effective immediately. Following the scandal, applications for credit cards and checking accounts at the bank plummeted. In response to the event, the Better Business Bureau dropped accreditation of the bank. Several states and cities ended business relations with the company.

An investigation by the Wells Fargo board of directors, the report of which was released in April 2017, primarily blamed Stumpf, who it said had not responded to evidence of wrongdoing in the consumer services division, and Tolstedt, who was said to have knowingly set impossible sales goals and refused to respond when subordinates disagreed with them. Wells Fargo coined the phrase, "Go for Gr-Eight" – or, in other words, aim to sell at least 8 products to every customer. The board chose to use a clawback clause in the retirement contracts of Stumpf and Tolstedt to recover $75 million worth of cash and stock from the former executives.

In February 2020, the company agreed to pay $3 billion to settle claims by the United States Department of Justice and the Securities and Exchange Commission. The settlement did not prevent individual employees from being targets of future litigation. The Federal Reserve put a limit to Wells Fargo's assets, as a result of the scandal. In 2020, Wells Fargo sold $100 million in assets to stay under the limit.

In December 2022, the bank agreed to a settlement with the CFPB of $3.7 billion over abuses tied to the fake account scandal as well as mortgages and auto loans. The total was split between $1.7 billion for a civil penalty and $2 billion for customers. Separately, in May 2023, the bank agreed to pay $1 billion to settle a shareholder class-action suit.

Wirecard Accounting Scandal:

The Wirecard scandal (German: Wirecard-Skandal) was a series of corrupt business practices and fraudulent financial reporting that led to the insolvency of Wirecard, a payment processor and financial services provider, headquartered in Munich, Germany. The company was part of the DAX index. They offered customers electronic payment transaction and risk management services, as well as the issuance and processing of physical cards. The subsidiary, Wirecard Bank AG, held a banking license and had contracts with multiple international financial services companies.

Allegations of accounting malpractices have trailed the company since the early days of its incorporation, reaching a peak in 2019 after the Financial Times published a series of investigations along with whistleblower complaints and internal documents. On 25 June 2020, Wirecard filed for insolvency after revealing that €1.9 billion was "missing", and the termination and arrest of its CEO Markus Braun. Questions have been raised about regulatory failure on the part of Federal Financial Supervisory Authority (BaFin), Germany's top financial watchdog, and possible malpractice of Wirecard's long time auditor Ernst & Young.

Rise of Wirecard

The company was founded in 1999. After Markus Braun joined as CEO in 2002, the company focused on online payment services, starting with porn and gambling websites as clients. By taking over the listing of InfoGenie AG, a defunct call centre group, Wirecard entered the Neuer Markt stock market segment, an action that has been criticised as avoidance of proper scrutiny during an initial public offering. This was achieved through a decision in an InfoGenie general meeting to transfer the non-listed Wirecard to InfoGenie AG by way of a capital increase against investment in kind, making Wirecard a stock corporation listed in the Prime Standard stock market segment through a reverse IPO. A clean audit from EY in 2007 allayed investors concerns. Wirecard was included in the TecDAX since 2006 and in the DAX since 2018. In 2018, Wirecard shares reached a peak, valuing the company at €24bn.

Wirecard attributed its fast growth to fast international expansion achieved through acquisition of local businesses, resulting in its revenue growth often outpacing general industry trends. In March 2017, Wirecard acquired Citi Prepaid Card Services and created Wirecard North America, entering the US market.[9] Also in 2007, Wirecard expanded into banking by purchasing XCOM Bank AG, allowing it to issue credit and debit cards through licensing agreements with both Visa and Mastercard. In November 2019, Wirecard entered the Chinese market by acquiring Beijing-based AllScore Payment Services.

Causes of downfall

Wirecard is suspected to have engaged in a series of fraudulent accounting activities to inflate its profit. Despite the allegations, BaFin ultimately took little action against the company before its eventual collapse, opting instead to file complaints against critics of the company and short sellers of the company's stock.

Accounting irregularities

Wirecard's combined banking (through its subsidiary Wirecard Bank) and non-banking (mainly payment processing) operations make its financial results harder to compare with peers, so investors had to rely on adjusted versions of the financial statements of the company. The "adjusted" accounts, unlike the reporting adhering to International Financial Reporting Standards, resulted in inflated earnings and cash flow figures.

Red flags were raised as early as 2008 when the head of a German shareholder association attacked Wirecard's balance sheet irregularities. After EY conducted a special audit in response to the criticisms, it took over as the main auditor for Wirecard and would remain so for the rest of the company's history. As a response, German authorities prosecuted two persons due to insufficient disclosure of holding Wirecard's stock.

In 2015, the Financial Times reported what it saw as a significant gap between the short-term assets and liabilities in Wirecard's payment business. This was a result of Wirecard's taking only a small commission from its payment processing volume, and the transient payment flow through Wirecard's accounts was adjusted to reflect Wirecard's small cut. In response, Wirecard retained the services of Schillings, a UK law firm, and FTI Consulting's public relations agency in London. Later in 2015, J Capital Research published a report that recommended shorting Wirecard's stock, as it saw the company's Asian operations to be much smaller than claimed. In 2016, a critical report published by a previously unknown entity named Zatarra Research led to share price crashes, prompting BaFin to launch an investigation into possible market manipulation.

In July 2021, Wirecard hired corporate investigations firm Alix Partners to perform a forensic investigation of the accounting practices that led to its insolvency.

Opaque acquisitions and corporate structure

Critics point to Wirecard's global acquisitions as a means to mask trouble with organic growth by adding revenues from external sources, a tactic referred to as a rollup. Early criticisms were directed towards Wirecard's purchases of smaller businesses at significantly above market value. In 2015, Wirecard purchased an Indian payments group for €340m, despite the founders of those businesses failing to raise funding while valuing their key assets at €46m. Wirecard responded to the reports by claiming that its payment technologies were superior and arguing that the rapid growth of the cashless fintech industry justified such valuations. A series of deals involving Wirecard's "buy and build" strategy, which intended to buy customers for the company's payment services, were criticized as being structured in an unusual manner, resulting in difficulty in verifying €670m of intangible assets.

In 2018, the Southern Investigative Reporting Foundation (now the Foundation for Financial Journalism) concluded after a seven-month investigation that according to documents filed, at least €175m from Wirecard's €340m purchase of an India-based payment processor in October 2015 were not transferred to the seller.

Artificial inflation of profit

In January 2019, Financial Times reported on irregularities uncovered by Wirecard's Singapore investigation, which began in March 2018 internally but a whistleblower feared was being squashed. Edo Kurniawan, head of accounting for Wirecard's Asian-Pacific operations, was accused of creating forged and backdated contracts in order to artificially inflate profit, creating questions about the reliability of Wirecard's accounts. In one instance, €37m was moved between Wirecard subsidiaries and external businesses, in a practice known as round-tripping. A preliminary report commissioned by Rajah & Tann and seen by FT pointed to several years of book-padding across Wirecard's Asian operations, with some degree of knowledge by Wirecard's Munich operation teams.

Despite the report, no actions were taken against key personnel named in the report. Singaporean authorities raided Wirecard as part of an ongoing investigation in February 2019. BaFin banned short selling of Wirecard's stock for two months citing falling investor confidence.

Third-party acquirers

Third-party acquirers are local companies who processed client transactions on behalf of Wirecard in exchange for a portion of the processing fees. According to Wirecard, they are used in transactions where Wirecard does not hold the necessary license, or when the nature of the transaction is unsuitable for direct processing on the part of Wirecard. In practice, this worked as follows: if a dubious dealer wanted to use Wirecard, for example an online shop, for ineffective hair restorers, then that was interesting for Wirecard, because such a customer pays high fees. However, Wirecard did not want to run such a shop as a Wirecard customer in its own database. So they referred such merchants to third-party acquirers who made sure the problem merchant could process payments.

According to internal whistleblowers, as of 2018, transactions originating from third-party acquirers accounted for half of global transaction volumes reported by Wirecard. Due to Wirecard's singular approach to counting its cash reserves, the cash held in trustee accounts of its third-party acquirers was counted in Wirecard's balance sheets. In 2019, it was reported that half of Wirecard's worldwide revenue and almost all of its profit were processed through three opaque and poorly audited third-party processors.

Wirecard announced lawsuits against the Singaporean authorities and the Financial Times in response to the allegations.

Aggressive attack on critics

Wirecard had a pattern of unusually aggressive tactics towards those who raised questions about the company's business operations or accounting. In 2019, the company hired former head of Libyan foreign intelligence Rami El Obeidi to conduct sting operations against journalists and public short sellers. El Obeidi presented evidence that the Financial Times colluded with short sellers, which the newspaper rejected after an investigation by an external law firm. And while prosecutors did not name his clients directly, the convicted felon Aviram Azari, a private detective caught in hacking-for-hire schemes, had targeted companies critical of Wirecard.

Auditing and regulatory failure

BaFin conducted multiple investigations against journalists and short sellers because of alleged market manipulation, in response to negative media reporting about Wirecard. BaFin lacked the authority to investigate Wirecard's core business or its accounting practices, and in fact, only had authority over Wirecard's bank business subsidiary.

As revealed by KPMG's special audit, Wirecard's long time auditor EY failed to verify the existence of cash reserves in what appeared to be fraudulent bank statements. KPMG was unable to verify the majority of Wirecard profits from 2016 to 2018 as part of its audit due to a lack of cooperation from Wirecard and its partners. During the special audit, Wirecard made misleading statements to investors, resulting in a criminal investigation after a complaint was referred to prosecutors by BaFin.

Role of sell side analysts

Sell side analysts were almost universally positive about Wirecard until as late as February 2020. Analysts at Goldman Sachs had a "Conviction Buy" rating until as late as September 2019. Commerzbank analysts who were positive on the shares even dubbed FT articles questioning the company "fake news". Analysts at Bank of America Merrill Lynch were among the very few skeptics. In 2018, they questioned Wirecard's poor positioning within the German e-commerce payments market and raised concerns related to financial controls.

Whistleblower

On 20 May 2021, Pav Gill, Wirecard's senior legal counsel based in Singapore who looked after all legal aspects of Wirecard's business and operations in the Asia-Pacific region, revealed himself to be the whistleblower who provided documents exposing the fraud to the Financial Times.

Convictions

During June 2023, Singapore's State Court sentenced James Wardhana, Wirecard's international finance manager to 21 months and Chai Ai Lim, Wirecard Asia's Head of Finance, to 10 months of imprisonment.

In November 2023, the United States District Court for the Southern District of New York sentenced Aviram Azari, the founder of an Israeli intelligence firm, to 80 months of imprisonment and 3 years of supervised release, as well as the forfeiture of the proceeds from his hacking activities.

Investors

With respect to criticisms against Wirecard, a set of smaller investors has long been supportive of the company by joining in both the company's and regulator's accusations against short sellers and market manipulation. Critics cite the German regulator, press and investor community's tendency to rally around Wirecard against what they perceive as unfair attack. Softbank invested in Wirecard with a €900m cash injection in 2019. After the company's failure was made public, Softbank's executives blamed what they saw as failures on the auditor's part and announced plans to sue EY for damages, joining other efforts to launch legal actions against the auditor.

Regulators

After initially defending BaFin's actions, its president Felix Hufeld later admitted the Wirecard scandal was a "complete disaster". In response, the European Commission called for an investigation into whether BaFin broke EU rules on financial reporting. Berlin announced plans to strengthen accounting regulations, beginning by severing ties with the Financial Reporting Enforcement Panel (FREP), a quasi-official accounting watchdog, and transferring its duties to BaFin. FT noted that FREP only had 15 employees and an annual budget of €6m. FREP was thought to be too under-resourced to adequately audit Wirecard, and only concluded that the published accounts were inadequate after the company became insolvent. Investors joined calls for union-wide regulation of market rules and for an EU body in charge of regulatory actions.

On 1 September 2020, the German parliament announced that it would organise an inquiry in order to fully investigate the reasons why the government failed to prevent corporate fraud. The scandal has highlighted the close ties between German politicians and Wirecard. On 29 January 2021, Hufeld and deputy Elisabeth Roegele left BaFin as part of a plan to reform the agency.

Suspects

Former Wirecard CEO Markus Braun was arrested shortly after his resignation. Former COO Jan Marsalek disappeared shortly after he was fired from the company and was later found to have fled to Belarus. He is a fugitive wanted by the German police, he is listed on Europol's list of Europe's most wanted fugitives, and Interpol issued a Red Notice against him. Christopher Bauer, the company's former Asia manager and son of Paul Bauer-Schlichtegroll, former chairman of the advisory board, died in Manila, Philippines. Bauer was very close to Marsalek.

In 2020, the FinCEN Files showed that Aktif Bank helped launder money for Wirecard.

CHAPTER 7: BEST PRACTICES IN FRAUD DETECTION AND RISK MANAGEMENT

Implementing best practices in fraud detection and risk management is essential for organizations to effectively identify, prevent, and mitigate the impact of fraudulent activities. By adopting proactive measures and leveraging advanced technologies, organizations can enhance their resilience against fraud and safeguard their assets and reputation.

1. Proactive Risk Assessment:

Conduct regular risk assessments to identify potential fraud risks and vulnerabilities within the organization. Assess both internal and external threats, prioritize risks based on severity and likelihood, and develop mitigation strategies to address identified risks pro-actively.

2. Strong Internal Controls: Implement robust internal controls and security measures to prevent and detect fraudulent activities. This includes segregation of duties, dual authorization for sensitive transactions, regular reconciliation of accounts, and access controls to limit unauthorized access to sensitive data and systems.

3. Employee Training and Awareness: Provide comprehensive training and awareness programs to educate employees about fraud risks, red flags, and their role in fraud prevention. Foster a culture of ethics and integrity within the organization, encourage whistleblowing, and provide channels for reporting suspicious activities anonymously.

4. Data Analytics and Technology: Leverage data analytics, artificial intelligence, and machine learning technologies to analyze large volumes of data and detect patterns indicative of fraudulent behavior. Implement fraud detection tools and platforms that utilize advanced analytics and algorithms to identify anomalies and suspicious activities in real-time.

5. Collaboration and Information Sharing: Collaborate with industry peers, regulatory authorities, and law enforcement agencies to share information and best practices for fraud prevention. Participate in industry forums, share intelligence on emerging fraud trends, and collaborate on joint initiatives to combat fraud collectively.

6. Continuous Monitoring and Review: Establish processes for continuous monitoring and review of fraud detection controls and strategies. Regularly review and update risk assessments, evaluate the effectiveness of fraud prevention measures, and adapt strategies to address evolving fraud threats and regulatory requirements.

7. Third-Party Risk Management: Assess and monitor third-party vendors and partners for compliance with fraud prevention standards and security protocols. Conduct due diligence on vendors, establish contractual agreements outlining fraud prevention expectations, and monitor third-party activities for signs of fraudulent behavior.

8. Incident Response Planning: Develop and maintain incident response plans and protocols to guide the organization's response to suspected or confirmed fraud incidents. Define roles and responsibilities, establish communication channels, and coordinate with internal stakeholders and external parties, such as legal counsel and law enforcement, to effectively manage fraud incidents and minimize their impact.

9. Stakeholder Communication and Transparency: Maintain open and transparent communication with stakeholders, including customers, investors, regulators, and employees, about the organization's fraud prevention efforts and response to fraud incidents. Build trust and credibility by providing timely updates, disclosing relevant information, and demonstrating accountability in addressing fraud risks.

10. Continuous Improvement: Embrace a culture of continuous improvement in fraud detection and risk management practices. Solicit feedback from stakeholders, conduct post-incident reviews to identify lessons learned, and implement corrective actions to strengthen fraud prevention controls and enhance organizational resilience against future fraud threats.

By implementing these best practices, organizations can enhance their fraud detection and risk management capabilities, minimize the likelihood and impact of fraudulent activities, and maintain trust and confidence among stakeholders in their operations and integrity.

CHAPTER 8: FUTURE TRENDS AND CHALLENGES

Anticipating future trends and addressing emerging challenges is essential for staying ahead in fraud detection and risk management. As technology evolves and fraudsters adapt their tactics, organizations must continuously innovate and adapt their strategies to effectively combat fraud and mitigate risks.

1. Emerging Technologies: Advancements in artificial intelligence, machine learning, blockchain, and biometric authentication are poised to reshape fraud detection and risk management. Organizations will increasingly leverage these technologies to analyze large volumes of data, detect anomalies, and enhance security measures to stay ahead of evolving fraud threats.

2. Big Data and Analytics: The proliferation of data from diverse sources presents both opportunities and challenges for fraud detection. Organizations will need to invest in robust data analytics capabilities to harness the power of big data effectively while addressing data privacy concerns and ensuring compliance with regulatory requirements.

3. Cybersecurity Risks: As cyber threats continue to evolve in sophistication and scale, organizations face growing cybersecurity risks that can facilitate fraudulent activities, such as data breaches, ransomware attacks, and social engineering scams. Strengthening cybersecurity defenses and implementing proactive measures to protect sensitive data will be critical in mitigating fraud risks.

4. Regulatory Landscape: The regulatory landscape governing fraud detection and risk management is expected to evolve in response to emerging threats and technological advancements. Organizations will need to stay abreast of regulatory changes, adapt their compliance programs accordingly, and demonstrate accountability in meeting regulatory requirements.

5. Globalization and Cross-Border Transactions: The increasing globalization of business operations and cross-border transactions introduces complexities and challenges in fraud detection and risk management. Organizations must navigate regulatory differences across jurisdictions, address cultural and language barriers, and implement robust anti-fraud measures to mitigate risks associated with international operations.

6. Social Engineering and Insider Threats: Social engineering tactics, such as phishing, pretexting, and social manipulation, pose significant risks to organizations by exploiting human vulnerabilities to gain unauthorized access or deceive individuals into fraudulent activities. Educating employees about social engineering threats and implementing robust security awareness training programs will be crucial in mitigating these risks.

7. Ethical Considerations: As organizations leverage advanced technologies and data analytics for fraud detection, ethical considerations surrounding data privacy, transparency, and algorithmic bias become increasingly important. Organizations must uphold ethical principles, prioritize consumer privacy, and ensure fairness and equity in their fraud detection practices.

8. Collaboration and Information Sharing: Collaboration and information sharing among industry peers, regulatory authorities, and law enforcement agencies will play a vital role in combating fraud effectively. Establishing partnerships, sharing intelligence on emerging threats, and coordinating responses to fraudulent activities will strengthen collective efforts to mitigate fraud risks.

9. Continuous Learning and Adaptation: Continuous learning and adaptation are essential for staying ahead of fraudsters and evolving fraud threats. Organizations must foster a culture of innovation, encourage experimentation with new technologies and methodologies, and embrace a proactive approach to fraud detection and risk management.

10. Resilience and Agility: Building resilience and agility in fraud detection and risk management is crucial for effectively responding to unexpected challenges and disruptions. Organizations must develop contingency plans, implement agile frameworks, and remain flexible in their strategies to adapt to changing fraud landscapes and emerging threats.

By anticipating these future trends and challenges, organizations can proactively enhance their fraud detection and risk management capabilities, minimize vulnerabilities, and safeguard their assets and reputation in an increasingly complex and dynamic environment.

Emerging Technologies:

Emerging technologies are technologies whose development, practical applications, or both are still largely unrealized. These technologies are generally new but also include older technologies finding new applications. Emerging technologies are often perceived as capable of changing the status quo.

Emerging technologies are characterized by radical novelty (in application even if not in origins), relatively fast growth, coherence, prominent impact, and uncertainty and ambiguity. In other words, an emerging technology can be defined as "a radically novel and relatively fast growing technology characterised by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domain(s) which is observed in terms of the composition of actors, institutions and patterns of interactions among those, along with the associated knowledge production processes. Its most prominent impact, however, lies in the future and so in the emergence phase is still somewhat uncertain and ambiguous."

Emerging technologies include a variety of technologies such as educational technology, information technology, nanotechnology, biotechnology, robotics, and artificial intelligence.

New technological fields may result from the technological convergence of different systems evolving towards similar goals. Convergence brings previously separate technologies such as voice (and telephony features), data (and productivity applications) and video together so that they share resources and interact with each other, creating new efficiencies.

Emerging technologies are those technical innovations which represent progressive developments within a field for competitive advantage; converging technologies represent previously distinct fields which are in some way moving towards stronger inter-connection and similar goals. However, the opinion on the degree of the impact, status and economic viability of several emerging and converging techno

Big Data and Analytics:

Big data primarily refers to data sets that are too large or complex to be dealt with by traditional data-processing application software. Data with many entries (rows) offer greater statistical power, while data with higher complexity (more attributes or columns) may lead to a higher false discovery rate. Though used sometimes loosely partly due to a lack of formal definition, the best interpretation is that it is a large body of information that cannot be comprehended when used in small amounts only.

Big data analysis challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy, and data source. Big data was originally associated with three key concepts: volume, variety, and velocity.[4] The analysis of big data presents challenges in sampling, and thus previously allowing for only observations and sampling. Thus a fourth concept, veracity, refers to the quality or insightfulness of the data. Without sufficient investment in expertise for big data veracity, the volume and variety of data can produce costs and risks that exceed an organization's capacity to create and capture value from big data.

Current usage of the term big data tends to refer to the use of predictive analytics, user behavior analytics, or certain other advanced data analytics methods that extract value from big data, and seldom to a particular size of data set. "There is little doubt that the quantities of data now available are indeed large, but that's not the most relevant characteristic of this new data ecosystem." Analysis of data sets can find new correlations to "spot business trends, prevent diseases, combat crime and so on". Scientists, business executives, medical practitioners, advertising and governments alike regularly meet difficulties with large data-sets in areas including Internet searches, fintech, healthcare analytics, geographic information systems, urban informatics, and business informatics. Scientists encounter limitations in e-Science work, including meteorology, genomics, connectomics, complex physics simulations, biology, and environmental research.

The size and number of available data sets have grown rapidly as data is collected by devices such as mobile devices, cheap and numerous information-sensing Internet of things devices, aerial (remote sensing) equipment, software logs, cameras, microphones, radio-frequency identification (RFID) readers and wireless sensor networks. The world's technological per-capita capacity to store information has roughly doubled every 40 months since the 1980s; as of 2012, every day 2.5 exabytes (2.17×260 bytes) of data are generated. Based on an IDC report prediction, the global data volume was predicted to grow exponentially from 4.4 zettabytes to 44 zettabytes between 2013 and 2020. By 2025, IDC predicts there will be 163 zettabytes of data. According to IDC, global spending on big data and business analytics (BDA) solutions is estimated to reach $215.7 billion in 2021. While Statista report, the global big data market is forecasted to grow to $103 billion by 2027. In 2011 McKinsey & Company reported, if US healthcare were to use big data creatively and effectively to drive efficiency and quality, the sector could create more than $300 billion in value every year. In the developed economies of Europe, government administrators could save more than €100 billion ($149 billion) in operational efficiency improvements alone by using big data. And users of services enabled by personal-location data could capture $600 billion in consumer surplus. One question for large enterprises is determining who should own big-data initiatives that affect the entire organization.

Cyber Security:

Computer security, cybersecurity, digital security or information technology security (IT security) is the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

The field is significant due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi. It is also significant due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

While most aspects of computer security involve digital measures such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering.

In April 2023, the United Kingdom Department for Science, Innovation & Technology released a report on cyber attacks over the last 12 months. They surveyed 2,263 UK businesses, 1,174 UK registered charities and 554 education institutions. The research found that "32% of businesses and 24% of charities overall recall any breaches or attacks from the last 12 months." These figures were much higher for "medium businesses (59%), large businesses (69%) and high-income charities with £500,000 or more in annual income (56%)." Yet, although medium or large businesses are more often the victims, since larger companies have generally improved their security over the last decade, small and midsize businesses (SMBs) have also become increasingly vulnerable as they often "do not have advanced tools to defend the business." SMBs are most likely to be affected by malware, ransomware, phishing, man-in-the-middle attacks, and Denial-of Service (DoS) Attacks.

Regulatary Landscape:

Bank regulation in the United States is highly fragmented compared with other G10 countries, where most countries have only one bank regulator. In the U.S., banking is regulated at both the federal and state level. Depending on the type of charter a banking organization has and on its organizational structure, it may be subject to numerous federal and state banking regulations. Apart from the bank regulatory agencies the U.S. maintains separate securities, commodities, and insurance regulatory agencies at the federal and state level, unlike Japan and the United Kingdom (where regulatory authority over the banking, securities and insurance industries is combined into one single financial-service agency). Bank examiners are generally employed to supervise banks and to ensure compliance with regulations.

U.S. banking regulation addresses privacy, disclosure, fraud prevention, anti-money laundering, anti-terrorism, anti-usury lending, and the promotion of lending to lower-income populations. Some individual cities also enact their own financial regulation laws (for example, defining what constitutes usurious lending).

Globalization and Cross-Border Transactions:

Globalization, or globalisation (Commonwealth English; see spelling differences), is the process of interaction and integration among people, companies, and governments worldwide. The term globalization first appeared in the early 20th century (supplanting an earlier French term mondialisation), developed its current meaning sometime in the second half of the 20th century, and came into popular use in the 1990s to describe the unprecedented international connectivity of the post-Cold War world.[1] Its origins can be traced back to 18th and 19th centuries due to advances in transportation and communications technology. This increase in global interactions has caused a growth in international trade and the exchange of ideas, beliefs, and culture. Globalization is primarily an economic process of interaction and integration that is associated with social and cultural aspects. However, disputes and international diplomacy are also large parts of the history of globalization, and of modern globalization.

Economically, globalization involves goods, services, data, technology, and the economic resources of capital. The expansion of global markets liberalizes the economic activities of the exchange of goods and funds. Removal of cross-border trade barriers has made the formation of global markets more feasible. Advances in transportation, like the steam locomotive, steamship, jet engine, and container ships, and developments in telecommunication infrastructure such as the telegraph, the Internet, mobile phones, and smartphones, have been major factors in globalization and have generated further interdependence of economic and cultural activities around the globe
.

Social Engineering and Insider Threats:

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in the sense that it is often one of the many steps in a more complex fraud scheme. It has also been defined as "any act that influences a person to take an action that may or may not be in their best interests."

Research done in 2020 has indicated that social engineering will be one of the most prominent challenges of the upcoming decade. Having proficiency in social engineering will be increasingly important for organizations and countries, due to the impact on geopolitics as well. Social engineering raises the question of whether our decisions will be accurately informed if our primary information is engineered and biased.

Social engineering attacks have been increasing in intensity and number, cementing the need for novel detection techniques and cyber security educational programs.

Insiders may have accounts giving them legitimate access to computer systems, with this access originally having been given to them to serve in the performance of their duties; these permissions could be abused to harm the organization. Insiders are often familiar with the organization's data and intellectual property as well as the methods that are in place to protect them. This makes it easier for the insider to circumvent any security controls of which they are aware. Physical proximity to data means that the insider does not need to hack into the organizational network through the outer perimeter by traversing firewalls; rather they are in the building already, often with direct access to the organization's internal network. Insider threats are harder to defend against than attacks from outsiders, since the insider already has legitimate access to the organization's information and assets.

An insider may attempt to steal property or information for personal gain or to benefit another organization or country. The threat to the organization could also be through malicious software left running on its computer systems by former employees, a so-called logic bomb.

Ethical Considerations:

Ethics or moral philosophy is the philosophical study of moral phenomena. It investigates normative questions about what people ought to do or which behavior is morally right. It is usually divided into three major fields: normative ethics, applied ethics, and metaethics.

Normative ethics discovers and justifies universal principles that govern how people should act in any situation. According to consequentialists, an act is right if it leads to the best consequences. Deontologists hold that morality consists in fulfilling duties, like telling the truth and keeping promises. Virtue theorists see the manifestation of virtues, like courage and compassion, as the fundamental principle of morality. Applied ethics examines concrete ethical problems in real-life situations, for example, by exploring the moral implications of the universal principles discovered in normative ethics within a specific domain. Bioethics studies moral issues associated with living organisms including humans, animals, and plants. Business ethics investigates how ethical principles apply to corporations, while professional ethics focuses on what is morally required of members of different professions. Metaethics is a metatheory that examines the underlying assumptions and concepts of ethics.

Collaboration and Information Sharing:

Information exchange or information sharing means that people or other entities pass information from one to another. This could be done electronically or through certain systems. These are terms that can either refer to bidirectional information transfer in telecommunications and computer science or communication seen from a system-theoretic or information-theoretic point of view. As "information," in this context invariably refers to (electronic) data that encodes and represents the information at hand, a broader treatment can be found under data exchange.

Information exchange has a long history in information technology. Traditional information sharing referred to one-to-one exchanges of data between a sender and receiver. Online information sharing gives useful data to businesses for future strategies based on online sharing. These information exchanges are implemented via dozens of open and proprietary protocols, message, and file formats. Electronic data interchange (EDI) is a successful implementation of commercial data exchanges that began in the late 1970s and remains in use today.

Some controversy comes when discussing regulations regarding information exchange. Initiatives to standardize information sharing protocols include extensible markup language (XML), simple object access protocol (SOAP), and web services description language (WSDL).

From the point of view of a computer scientist, the four primary information sharing design patterns are sharing information one-to-one, one-to-many, many-to-many, and many-to-one. Technologies to meet all four of these design patterns are evolving and include blogs, wikis, really simple syndication, tagging, and chat.

Continuous Learning and Adaptation:

Continuous learning and adaptation is very important in every field. Most importantly when it comes to Fraud, we need to be one step ahead. Adapting to new technology, using the advanced AI technology using logic and emotional intelligence is the need of the hour. Fraud can happen in any field. Being vigilant is very important. Continuous learning in every field is core strength of every employee be it in bank, small shop, big industry or any other field. Every day we hear, see and experience fraud in all walks of life. Money Laundering, Fake ID's, insufficient due diligence is all the reason for fraud.

Resilience and Agility:

Cyber resilience refers to an entity's ability to continuously deliver the intended outcome, despite cyber attacks. Resilience to cyber attacks is essential to IT systems, critical infrastructure, business processes, organizations, societies, and nation-states. A related term is cyberworthiness, which is an assessment of the resilience of a system from cyber attacks. It can be applied to a range of software and hardware elements (such as standalone software, code deployed on an internet site, the browser itself, military mission systems, commercial equipment, or IoT devices).

Adverse cyber events are those that negatively impact the availability, integrity, or confidentiality of networked IT systems and associated information and services. These events may be intentional (e.g. cyber attack) or unintentional (e.g. failed software update) and caused by humans, nature, or a combination thereof.

Unlike cyber security, which is designed to protect systems, networks and data from cyber crimes, cyber resilience is designed to prevent systems and networks from being derailed in the event that security is compromised. Cyber security is effective without compromising the usability of systems and there is a robust continuity business plan to resume operations, if the cyber attack is successful.

Cyber resilience helps businesses to recognize that hackers have the advantage of innovative tools, element of surprise, target and can be successful in their attempt. This concept helps business to prepare, prevent, respond and successfully recover to the intended secure state. This is a cultural shift as the organization sees security as a full-time job and embedded security best practices in day-to-day operations. In comparison to cyber security, cyber resilience requires the business to think differently and be more agile on handling attacks.

The objective of cyber resilience is to maintain the entity's ability to deliver the intended outcome continuously at all times. This means doing so even when regular delivery mechanisms have failed, such as during a crisis or after a security breach. The concept also includes the ability to restore or recover regular delivery mechanisms after such events, as well as the ability to continuously change or modify these delivery mechanisms, if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms.

CHAPTER 9: CONCLUSION

Fraud detection and risk management are critical components of organizational integrity, financial stability, and reputation. In today's dynamic and interconnected business landscape, organizations face diverse and evolving fraud threats that require proactive and innovative approaches to detection, prevention, and mitigation.

By understanding the various types of fraud, motivations behind fraudulent activities, and the impact of fraud on organizations, stakeholders can appreciate the importance of robust fraud detection and risk management practices. Implementing a comprehensive risk management framework, leveraging advanced technologies such as AI and machine learning, and adhering to regulatory compliance standards are essential steps in mitigating fraud risks effectively.

Real-world case studies provide valuable insights into the challenges organizations face in fraud detection and risk management, as well as the strategies and solutions employed to address them. By analyzing these cases and embracing best practices, organizations can enhance their fraud detection capabilities, minimize the likelihood and impact of fraudulent activities, and maintain trust and confidence among stakeholders.

Looking ahead, organizations must anticipate future trends and challenges in fraud detection and risk management, including emerging technologies, cybersecurity risks, regulatory changes, and globalization. By staying ahead of these trends, fostering a culture of continuous learning and adaptation, and prioritizing resilience and agility, organizations can effectively navigate the evolving fraud landscape and safeguard their assets and reputation in an increasingly complex business environment.

In conclusion, proactive and collaborative efforts are essential in combating fraud effectively and mitigating risks to ensure the integrity, resilience, and sustainability of organizations in the face of evolving fraud threats.

End of Project Report