Chapter 9
Detection and Prevention of Fraud in the Digital Era

Evrim Vildan Altuk

https://orcid.org/0000-0003-2139-8081

Trakya University, Turkey

ABSTRACT

It is essential for businesses to keep up with the technological advances. Today nearly all the businesses depend on computer technologies and the Internet to operate as technological developments have introduced many practical methods for businesses. Yet, transformation of businesses technologically also presents new means for the criminals, which has led to new types of fraud. It is crucial for businesses to take measures to prevent fraud. Traditional methods to prevent or to detect fraud seems to be ineffective for new types of fraud in the digital era. Therefore, new methods have been used to prevent and detect fraud. This chapter reviews fraud as a form of cybercrime in the digital era and aims to introduce the methods that have been used to detect and prevent it.

INTRODUCTION

Fraud is an old story and has been there since the existence of human beings. The nature of fraud has changed over time. Fraud has become much more prevalent compared to the past. Many methods have been developed to prevent fraud but fraudsters have always been one step ahead. With the digital transformation of companies, fraud has also gone through transformation. Technological developments have enabled companies to present their products and services to meet customers' needs but fraudsters also perpetrate fraud through technological opportunities and there remains just a bit of imagination. Thus, technology seems to have two aspects: "good and bad". With the technological developments, some gaps have also emerged in the transactions that companies make, which also encourages fraudsters.

The invention of the Internet has introduced many investment opportunities. While the Internet has made information accessible more easily and given everything more transparency, it has also created more opportunities for fraudsters. Fraudsters often deceive unaware victims by promising spectacular returns (Cross, 2013).

In a digital world, companies often face both internal and external threats. Insider frauds can be perpetrated by employees of companies whereas outsider frauds are incidences, such as computer hacking and computer viruses. Some fraudsters are also capable of adapting old fraud schemes to the digital environment.

The term "cybercrime" has been introduced in this new era. Cybercrime is criminal activities in which a computer or network of computers is an integral part of the crime including activities such as spamming, theft of electronic intellectual property and other financial frauds. On the other hand, computer programmers have developed data analysis software that enables users to sift mass of information and transactions to detect fraudulent activities.

Cybercrime involves any crime committed through the Internet. This chapter reviews only cybercrimes against businesses. The present study also reviews the methods to prevent and detect fraud in the digital era.

BACKGROUND

There is not a common definition of fraud. Fraud involves a wide range of activities united by some form of misrepresentation by a party to provide that party with an advantage or cause a disadvantage to others including criminal, civil and regulatory acts of deviance (Button and Cross, 2017).

Fraud incorporates four basic elements:

- *"A false representation of nature of material*
- *Intent or knowledge that the representation is false, or intentional disregard for the accuracy*
- *Reasonably and justifiably relying on the representation*
- *Financial damages as a result of the preceding elements"* (Skalak, Golden, Clayton &Pill, 2011: p.2).

Fraud is defined as an intent to cheat or gain an unmerited benefit including a broad set of acts. The American Institute of Chartered Public Accountants (AICPA) describes two main categories of fraud, which are deliberate misstatement of financial information, and misappropriation of assets (or theft). The definition of fraud might be extended as follows:

"Fraud consists of an illegal act (the intentional wrongdoing), the concealment of this act (often only hidden via simple means), and the deriving of a benefit (converting the gains to cash or other valuable commodity)" (Coderre, 2009: p.3). From a business standpoint, fraud may be defined as the misuse of assets in an organization and misrepresentation of financial statements.

Although there are various types of fraud, it can broadly be divided into employee fraud or misappropriation of assets and financial statement fraud *(Skalak, Golden, Clayton &Pill,2011: p.5)*

Employee fraud or misappropriation of assets might be perpetrated by any officer and employer working for an organization. Examples of this type of fraud are *pilfering of cash and inventory, skimming* revenues, payroll fraud, and embezzlement.

Financial Statement fraud is the intentional misrepresentation or omissions of amounts or disclosures in financial reports to deceive the people who use financial statements. Particularly, it includes manipulation, falsification, or alteration of accounting records or supporting documents that are used to

Related Content

Autonomous Last Mile Shuttle ISEAUTO for Education and Research

Raivo Sell, Mairo Leier, Anton Rassõlkinand Juhan-Peep Ernits (2020). *International Journal of Artificial Intelligence and Machine Learning (pp. 18-30).*

www.irma-international.org/article/autonomous-last-mile-shuttle-iseauto-for-education-and-research/249250

Hybrid Attributes Technique Filter for the Tracking of Crowd Behavior

Hocine Chebi (2021). *Handbook of Research on Automated Feature Engineering and Advanced Applications in Data Science (pp. 38-47).*

www.irma-international.org/chapter/hybrid-attributes-technique-filter-for-the-tracking-of-crowd-behavior/268748

Pedagogical Ontology Modelling for Cell Biology Domain With an Algorithm for Question Generation

Gerard Deepak, Ayush Kumar, Santhanavijayan A., Pushpa C. N., Thriveni J.and Venugopal K. R. (2021). *Machine Learning Approaches for Improvising Modern Learning Systems (pp. 144-168).*

www.irma-international.org/chapter/pedagogical-ontology-modelling-for-cell-biology-domain-with-an-algorithm-for-question-generation/279383

Autonomous Navigation Using Deep Reinforcement Learning in ROS

Ganesh Khekareand Shahrukh Sheikh (2021). *International Journal of Artificial Intelligence and Machine Learning (pp. 63-70).*

www.irma-international.org/article/autonomous-navigation-using-deep-reinforcement-learning-in-ros/277434

Application of Odd-Even Congruence Graph Labeling in Secured Cyber Physical Systems

Kanakambika K.and Thamizhendhi G. (2022). *Real-Time Applications of Machine Learning in Cyber-Physical Systems (pp. 77-92).*

www.irma-international.org/chapter/application-of-odd-even-congruence-graph-labeling-in-secured-cyber-physical-systems/299156