Chapter 16
Security Analysis of the Cyber Crime

Ratnesh Kumar Shukla
https://orcid.org/0000-0002-8279-7011
Shambhunath Institute of Engineering and Technology, India

Arvind Kumar Tiwari
Kamla Nehru Institute of Technology, Sultanpur, India

ABSTRACT

The primary driver of this expansion is the internet user, who is expected to connect 64 billion devices worldwide by 2026. Nearly $20 trillion will be spent on IoT devices, services, and infrastructure, according to Business Insider. Many cybercrimes and vulnerabilities related to cybercrime are committed with the use of data. Asset management, fitness tracking, and smart cities and homes are examples of internet security applications. The average person will most likely own two to six connected internet security devices by the end of the year, a significant increase over the total number of cell phones, desktop computers, and tablets. Although data provides a plethora of opportunities for its users, some have taken advantage of these advantages for illegal purposes. In particular, a great deal of cybercrime is made possible by the gathering, storing, analyzing, and sharing of data as well as the widespread gathering, storing, and distribution of data without the users' knowledge or consent and without the required security and legal protections. Furthermore, because data gathering, analysis, and transfer happen at scales that governments and organisations are unprepared for, there are a plethora of cybersecurity threats. Protection, privacy, and system and network security are all related.

INTRODUCTION

In a world where the majority of transactions take place on digital platforms, cybercrime has increased rapidly. Current trends in cybercrime indicate that by 2026, the worldwide cost of these attacks may amount to $20 trillion.

The word "cybercrime" is used to describe a broad range of illegal actions that are committed via a computer, network, or other collection of digital devices. Think of cybercrime as a catch-all word for

DOI: 10.4018/979-8-3693-2964-1.ch016

all kinds of illicit actions carried out by cybercriminals. These comprise ransomware, phishing, identity theft, hacking, and malware attacks, to name a few.

Cybercrime's reach transcends all geographic boundaries. There are victims, criminals, and technological infrastructure everywhere in the world. Because technology is used to exploit security flaws on both a personal and corporate level, cybercrime comes in various forms and is always changing. Because of this, preventing, properly investigating, and prosecuting cybercrime is a never-ending battle fraught with many shifting obstacles. Cybersecurity is something we use to prevent cybercrime. Cybersecurity is the process of protecting corporate or governmental computers, servers, and networks against harmful assaults and threats while also preventing unauthorized access to important data. While cyber-crime entails the theft of information, cash, or passwords through the use of vulnerabilities in human security of the systems (Mahammad & Kumar, 2023).

Cybercrime poses a severe risk to people, companies, and governmental organisations. It can lead to substantial financial loss, harm to one's reputation, and compromised data. The flow chart for cybercrime and cybersecurity acts is shown in Figure 1. The threat of cybercrime is increasing as technology develops and more people depend on digital devices and networks for daily tasks, making protection more crucial than ever.

Figure 1. Flow chart of cyber-crime and cyber security

Illegal use of computers or the internet is known as cybercrime. Here are a few instances of online fraud:

- ❖ Taking and selling corporate information.
- ❖ Demanding payment in order to avoid an attack.
- ❖ Virus installation on a targeted computer.
- ❖ Attempting to gain access to government or corporate computers.
- ❖ Email Scams.
- ❖ Social Media Fraud.
- ❖ eCommerce Fraud.
- ❖ Banking Fraud.
- ❖ Ransomware.