Chapter 5
Cyber Forensics:
A Boon to Cybersecurity

Sameer Saharan
https://orcid.org/0000-0002-7487-6297
Mody University of Science and Technology, India

Shailja Singh
https://orcid.org/0000-0002-6425-1699
Mangalayatan University, Jabalpur, India

Debasis Bora
Mandsaur University, India

Geetika Saxena
Mody University of Science and Technology, India

ABSTRACT

Cyber forensics is a vital ally in safeguarding our digital world. This abstract explores its symbiotic relationship with cybersecurity. Cyber forensics not only investigates cybercrimes, but also aids in threat detection, incident response, and risk mitigation. Technology, including AI, empowers professionals in navigating digital crime scenes. Ethical and legal considerations remain pivotal. Cyber forensics, as an indispensable part of cybersecurity, fortifies our digital landscape against evolving threats, ensuring a safer digital future.

INTRODUCTION

The advent of the Digital Age has heralded a new era of extraordinary connection, information sharing, and technological innovation. The globe has grown more interconnected than ever before, thanks to the increasing integration of digital technologies into every aspect of our lives, from communication and business to governance and healthcare (Miller & West, 2009). This fundamental transformation has provided

DOI: 10.4018/978-1-6684-9576-6.ch005

tremendous benefits, but it has also exposed individuals, businesses, and society to a slew of cybersecurity dangers that necessitate strong safeguards. Data has become the vitality of modern civilisation in this Digital Age. Data is at the centre of innumerable activities and transactions, ranging from personal information and financial records to intellectual property and national security secrets (Huang et al., 2022). However, this reliance on data-driven procedures has created a vulnerability that malevolent actors can exploit. Cyber-attacks have evolved into a sophisticated and ubiquitous threat capable of destroying key infrastructure, stealing sensitive information, and incurring worldwide financial damages. The rising frequency, complexity, and severity of cyber threats necessitates the need for cybersecurity. Malware, phishing assaults, ransomware, and Distributed Denial of Service (DDoS) attacks are just a handful of the methods used by cybercriminals to circumvent security measures and corrupt digital systems (Li & Liu, 2021). These attacks have the potential to have far-reaching implications, affecting not only individuals but potentially organisations, governments, and even entire countries. In the Digital Age, the interconnection of devices and systems magnifies the potential impact of cyber threats. The Internet of Things (IoT) has introduced a slew of networked gadgets, ranging from smart home appliances to industrial control systems, resulting in a vast attack surface (Huang et al., 2022). Furthermore, the increasing reliance on cloud computing and internet platforms has broadened the channels via which hostile actors might infiltrate networks and access sensitive data. The consequences of a successful cyberattack go beyond monetary damages. Cyber incidents have the potential to undermine trust in organisations, interrupt key services, and jeoparadize personal privacy (Sukri et al., 2023). High-profile data breaches have exposed millions of people to identity theft and financial crime, emphasising the importance of protecting digital assets. Furthermore, state-sponsored cyber-attacks and cyber espionage endanger national security by targeting sensitive information and essential infrastructure. Strong cybersecurity measures are required to solve these concerns (Sukri et al., 2023). To secure their networks and data, organisations must invest in advanced threat detection, intrusion prevention systems, and encryption techniques. Furthermore, cybersecurity awareness and training programmes are critical for educating people about the dangers of digital interactions and promoting safe online behaviour.

Cyber forensics develops as a critical and dynamic component in the arena of modern cybersecurity, where the digital terrain is riddled with ever-evolving threats. Cyber forensics, also known as digital forensics, is critical in detecting, investigating, and mitigating cybercrime, ensuring that the digital environment is secure and resilient. Incident response is one of the key functions of cyber forensics (Saharan & Yadav, 2022). When a cyber incident occurs, whether it is a data breach, a malware assault, or unauthorised access, cyber forensics specialists are entrusted with determining the extent and scale of the breach as soon as possible. They acquire and preserve digital evidence in a forensically sound manner by using specialised tools and techniques. This data not only helps to understand the attack, but it also acts as an important foundation for legal procedures. Furthermore, cyber forensics helps with cybercrime attribution. Investigators can identify cyber incidents to specific individuals, groups, or businesses by tracing the origin of assaults, discovering digital traces, and analysing malware signatures. This attribution capacity acts as a deterrent, warning potential attackers about the risks of being recognised and held accountable (Brinson et al., 2006; Saharan & Yadav, 2022). Cyber forensics role extends beyond identifying and attributing cybercrimes. It helps organisations detect vulnerabilities and flaws in their systems and networks by assisting in root cause analysis. As a result, they may strengthen their cybersecurity procedures, close gaps, and prevent repeat attacks. Cyber forensics responds to obstacles like as encryption and obfuscation techniques used by cybercriminals by creating creative approaches