Chapter 3
Role of Information Security and Protection in the Modern Era

Ahmad Tasnim Siddiqui
https://orcid.org/0000-0002-1884-9331
Sandip University, Nashik, India

Gulshaira Banu Jahangeer
https://orcid.org/0000-0003-4877-8738
Taif University, Saudi Arabia

Amjath Fareeth Basha
Taif University, Saudi Arabia

ABSTRACT

The purpose of information security is to protect data by mitigating the risks associated with it. It refers to preventing unauthorized access to disclosure, destruction, disruption, modification of information and the information that they process, store, and transmit. Every information, especially sensitive or confidential, must be protected. It is essential to consider technology, policies, procedures, and people when implementing an effective information security system. In addition, emerging threats and vulnerabilities need to be monitored, assessed, and adapted continuously. Cybercrime, theft, and espionage are some of the threats we face trying to protect our valuable information assets. The goal of information security is to safeguard valuable information assets against a variety of threats. No matter how information is stored, whether electronically or on paper, it must be protected to ensure privacy, integrity, and availability. This chapter talks about the role of information security in modern days.

INTRODUCTION

Protecting sensitive information held by an organization by maintaining its confidentiality, integrity, and availability (CIA) against attacks and threats is a big challenge in the current digital age. Apart from CIA triad, information security can also help in disaster recovery, authentication, encryption, and risk management etc. According to US law, information security is defined as "protecting infor-

DOI: 10.4018/979-8-3693-0472-3.ch003

mation and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction". It is widely accepted in the information security community that no system can be completely secure from all adversaries (Singla & Bertino, 2019). In order to protect their information, organizations around the world invest heavily in technological countermeasures. In spite of this, organizations rarely protect their information assets since they rely primarily on technical solutions that cannot meet their contextual requirements (Khando et al.., 2021). Consequently, organizations continuously struggle to protect their information assets, which forces them to invest a lot of money in technological measures. Information security, however, is a multidisciplinary field and human interaction plays a massive role in it. It is not enough to merely concentrate only on the technical aspects. In most security incidents, both intentional and unintentional misbehavior is the result of human errors.

Any hacker is interested in IT professionals' credentials, including their user names and passwords, as they may have access to sensitive network areas. Hackers could use the credentials of IT professionals to roam freely, download data from the network, or just monitor information of interest, including root access and network description. Hackers began to target the weakest element of the security infrastructure because security systems improved to counter known attack signatures. It has become increasingly clear that humans are the primary conduits for IT attacks. Phishing attacks were reported to have been successful in 84% of companies, and almost 91% were exposed to these attacks (Torten et al., 2018).

ENISA Threat Landscape (ETL) is the annual report on the state of cybersecurity threats released by ENISA, European Union Agency for Cybersecurity (ENISA, 2022). In this report, the report identifies prime threats, major trends concerning threats, threat actors, and attack techniques, as well as mitigation measures that should be implemented. ENISA organized threats into dissimilar groups, based on frequency and impact determine how prominent all of these threats still are:

- Ransomware: 60% of the organizations that have been attacked may have paid a ransom
- Malware: The year 2021 saw 66 leaks of zero-day vulnerabilities
- Social engineering: There are many different types of phishing, including whaling, spear-phishing, vishing, and smishing, but phishing has remained a popular technique for decades
- Threats against data: A proportional increase in the amount of data generated
- Threats against availability: There has never been a more significant Denial-of-Service (DDoS) attack perpetrated in Europe than in July 2022
- Internet: Internet traffic has been rerouted, infrastructure has been destroyed and outages have occurred
- Disinformation or misinformation: Deepfakes, disinformation-as-a-service, and AI-enabled disinformation are on the rise
- Supply chain targeting: In 2021, 17 percent of invasions are caused by third parties, compared to less than one percent in 2020

Organizational data is protected against multiple attacks by Information Security platforms, which are capable of identifying outliers and threats. Information security emphasizes confidentiality, integrity, and availability of data in order to protect them from both active and passive attacks (Alqahtani, 2017).