Chapter 1
The Role of Human Factors in Cybersecurity Vulnerabilities

Harish Chandra Verma
https://orcid.org/0000-0002-5085-2004
ICAR-Central Institute for Subtropical Horticulture, Lucknow.India

Saurabh Srivastava
https://orcid.org/0000-0001-7654-0220
Moradabad Institute of Technology, India

ABSTRACT

This chapter explores the crucial influence that human behavior and decision-making have on information system security. Human factors continue to be a major source of weaknesses in cybersecurity plans, even while technology measures constitute its core. This study looks into the several ways that human factors—such as social engineering, cognitive biases, and insufficient training—affect cybersecurity risks. The chapter illustrates how human errors, such as weak password practices, and phishing vulnerability, can undermine even the strongest technology defenses by looking at case studies. It emphasizes the significance of strategy for cybersecurity. To lower the risks associated with people, it suggests extensive training plans, approachable system designs, and organizational guidelines. In an effort to reduce human error, the chapter also examines new developments in the field, such as behavioural biometrics and AI-driven monitoring systems. In the end, this chapter highlights how important it is to address human elements in order to improve overall cybersecurity resilience

DOI: 10.4018/979-8-3693-9235-5.ch001

INTRODUCTION

As the globe grows more digitally connected, cybersecurity is becoming a top priority for all parties—individuals, businesses, and governments. In accordance with the Computer Misuse Act (legislation.gov.uk, 1990), the UK National Cyber Security Centre (NCSC) defines a cyber-security incident as a violation of a system's security policy that affects its availability or integrity, as well as any unauthorised access or attempted access to a system or systems. Generally speaking, the following behaviours are acknowledged as violations of a standard security policy: 1) Unauthorised access attempts to systems and/or data; 2) Unauthorised data processing or storage on systems; 3) Modifications to a system's hardware, software, or firmware without the system owner's permission; and 4) Malevolent interference and/or suppression. Furthermore, by deploying several levels of security between computer systems, networks, and any data that needs to be kept private, the cybersecurity method can be successfully applied (Upadhyay & Sampalli, 2020. Cybersecurity incidents range from large-scale malevolent cyberattacks on businesses or government institutions to individuals using social engineering to get access to their social media accounts.

A cyberattack known as "social engineering" is used to psychologically manipulate a target into disclosing confidential information(Krombholz *et al*., 2015). Because the human inclination to trust is more easily exploited than other hacking software, criminals deploy social engineering techniques. Social engineering techniques account for over 95% of online attacks. A malevolent hacker initially investigates the intended victim in order to gather background data for the assault. The thief then makes an effort to win over the victim's trust and convince them to do other acts, including providing access to a personal profile or disclosing critical personal information, that will ultimately lead to breathing security (Contel, and Schmick, 2016).

Even though intrusion detection systems, firewalls, and encryption are crucial technological solutions, they are not perfect. The human element is among the most important—yet sometimes disregarded—aspects of cybersecurity. According to a study by Alsharif *et al.*(2022), the degree of awareness about cybersecurity issues has reached 61%, which is a startlingly low level that needs to be raised as much as possible. The findings demonstrate a lack of knowledge of email usage (22%), phishing (30%), social media (35%), social engineering (37%), antivirus (33%), and data protection (29%).

This chapter examines the several ways that organisational culture, psychology, and human behaviour affect cybersecurity vulnerabilities. We seek to clarify the crucial role that human factors play in both generating and reducing cybersecurity threats by an examination of case studies, psychological theories, and organisational practices.