Chapter 3
Understanding the Human Factors in the Psychology of Cyber Threats

Mohd Saleem
Teerthanker Mahaveer University, India

Rajeev Kumar
Moradabad Institute of Technology, India

Chanchal Chawla
TMIMT, India

Mahendra Singh
Moradabad Institute of Technology, India

ABSTRACT

This chapter examines how human factors play a crucial part in cybersecurity vulnerabilities, highlighting the important influence of psychological and behavioral aspects on the vulnerability to and mitigation of cyber threats. It explores the psychological tricks used in social engineering, insider threats motivated by malice or incompetence, and the cognitive biases that affect cybersecurity judgment. The chapter demonstrates how businesses can create security interventions that effectively encourage safer behavior by utilizing behavioral economics concepts. Empirical case studies, encompassing significant episodes in India, demonstrate the pragmatic consequences of these human elements. The chapter emphasizes how crucial it is to create a culture of cybersecurity awareness and resilience through

DOI: 10.4018/979-8-3693-9235-5.ch003

thorough training, strict access controls, and well-thought-out behavioral interventions. Through the integration of technical measures and an understanding of human behavior, companies may strengthen their defences against the constantly changing cyber threat scenario.

I. OVERVIEW OF HUMAN FACTORS IN CYBERSECURITY

Human factors are an important, but frequently disregarded, component of cybersecurity. Human behavior is still a major susceptibility to cyber threats even with advances in technology security. This chapter explores the psychological aspects of cybersecurity, specifically how behavioural patterns, decision-making processes, and cognitive biases lead to security breaches. We can create more thorough and successful cybersecurity plans that address both technological and human-centric threats by comprehending these human components. Human factors continue to be one of the most important yet frequently disregarded components in the constantly changing field of cybersecurity. Although technological progress has greatly strengthened defences against cyberattacks, human error remains a serious vulnerability. The problem of cybersecurity is not just technological; it is also psychological (Salahdine & Kaabouch, 2019). This chapter explores the complex psychological aspects of cybersecurity and how behavioural patterns, decision-making processes, and cognitive biases lead to security breaches. There are many different factors that affect human behavior in the context of cybersecurity, including as psychological, social, and cultural dimensions. Overconfidence and the propensity to undervalue hazards are two examples of cognitive biases that frequently cause people to make decisions that jeopardize security. Convenience and an underestimating of the possible risks are two reasons why it's normal practice to reuse passwords across many accounts.

Understanding decision-making procedures is also essential to comprehending cybersecurity flaws. People frequently make snap decisions when under duress or with insufficient information, which can result in mistakes that cybercriminals can take advantage of. Phishing attacks, for instance, take advantage of people's innate inclination to reply to urgent requests without properly confirming the legitimacy of the source (Krombholz et al., 2015). Behavioural patterns can highlight how vulnerable people are to cyberattacks. Because routine tasks like downloading attachments or clicking links in emails are frequently carried out carelessly, they are frequently the focus of cyberattacks. It is possible to design ways to reduce these hazards by using behavioral interventions and awareness campaigns when these patterns are understood (Hadnagy, 2010).