CHAPTER 1
INTRODUCTION

As the Internet and technology have developed, the frequency and forms of cyber security attacks have increased [1]. In 2023, there was a 72% increase in data breaches compared to 2021, representing a historical record high [2]. Healthcare data breaches impose significant financial costs on hospitals [3], [4], [5] and they have consistently represented the most costly data breaches for 14 consecutive years [6]. Technological solutions have been developed to prevent these incidents [7], [8], but they are insufficient alone, as 68% of data breaches are due to non-malicious human error [9]. Consequently, there is a notable shift in emphasis towards the information security conduct of healthcare providers.

Studies have found that many hospital security incidents are due to low security awareness among employees [10], [11], [12]. The human factor is one of the most significant factors for security breaches in healthcare institutions, and there are many factors that influence healthcare workers' information security behavior [13]. Not only individual factors, organizations also find it difficult to implement regulatory standards that have been set [14]. This is due to a lack of financial resources and lack of technical expertise [15]. Although human factors are the biggest factor, technical factors are also important to maintain security and increase cybersecurity awareness [13], such as healthcare information systems are also important. Therefore, a key research question emerges: How do individual, organizational, and technical factors collectively influence information security compliance and protection behavior in healthcare settings?

This study will use the Stimulus-Organism-Response (SOR) theory to address this research question. The organisational factors will be used to stimulate the organism (individual factors), and the response will be information security compliance and protection behavior. This approach aims to understand and improve information security in healthcare institutions.

This study aims to develop a model for improving information security compliance and protection behavior (ISCPB) using the SOR model. The aim is to understand how different things affect how people act in relation to information security. This model aims to help organisations make targeted changes to improve security awareness.

This paper looks at the SOR model as a way of understanding security compliance behaviors. The paper will then look at the things that affect how people comply with and protect information security. We will look at why information security awareness is important and how it helps people to comply with security rules. These are the main ideas that form the basis of the conceptual model that we're presenting in this study. We'll also be discussing the contributions and potential applications of the model.