Chapter 2
A Comprehensive Cybersecurity Framework for Present and Future Global Information Technology Organizations

Wasswa Shafik
https://orcid.org/0000-0002-9320-3186
School of Digital Science, Universiti Brunei Darussalam, Gadong, Brunei & Digital Connectivity Research Laboratory (DCRLab), Kampala, Uganda

ABSTRACT

This chapter examines how education, technology, national and international regulations contribute to a comprehensive cybersecurity framework for present and future global IT companies. IT-driven enterprises may utilize the following security recommendations. Businesses who seek to examine their external and internal security with security upload and establish settings for success regardless of location must solve these issues. To produce more effective legislation, education efforts, and technologies that are resistant to cyberattacks, this work explores fundamental research gaps in cybersecurity and demonstrates how cybersecurity may be divided into these three fundamental categories and integrated to tackle problems such as the creation of training environments for authentic cybersecurity situations. It will explain links between technology and certification and discuss legislative standards and instructional frameworks for merging criteria for system accreditation and cybersecurity. The study finishes with wireless network security recommendations.

INTRODUCTION

There is a common misconception that security and usability are mutually exclusive system goals (Nyarko & Fong, 2023). Studies even go so far as to ask whether the phrase “useful security” is an oxymoron or not. When it comes to passwords, one of the security methods that is utilized daily, we see a typical illustration of how the goals of these two notions are diametrically opposed to one another (Conchon,

DOI: 10.4018/978-1-6684-9018-1.ch002

2023; Montasari, 2023). From a security point of view, it's best to have long, complicated (hard to guess), unique passwords that are changed every so often. However, from a usability point of view, these requirements are often a big burden on users and, as a result, the usability of a system (Netshakhuma, 2023).

Most of these more general security concerns also arise in the context of cybersecurity, where the focus is on the digital environment (Shaikh & Siponen, 2023). Therefore, the challenge that is faced by the fields of cybersecurity Usability and comparable Human-Computer Interaction and Security concepts are bridging the conceptual and application gaps, emphasizing the importance of fusing these two concepts, resulting in usable cybersecurity interfaces and systems (Kamariotou & Kitsios, 2023). This is especially true as functions and features related to security become increasingly integrated into software programs and end-user systems as standard components.

Common examples of these user-facing applications and systems include word processing software (with tasks such as adding digital signatures to facilitate subsequent document authentication), document readers (which allow setting viewing, access, and printing permissions), personal devices (with activities such as applying security pins and locks to mobile phones), personal security firewalls, and email encryption tools (Bukauskas et al., 2023). All these applications and systems are designed to interact directly with the user. All of these are related in some way to the regular activities that take place in the online world.

The purpose of this chapter is to provide a brief overview of some of the most significant advancements that have been made in the fields of cybersecurity usability and HCISec, particularly the guidance and recommendations offered for highly usable cybersecurity systems. Because of this, one of the most important things this study does is bring together work that has already been published and make an initial core list of general principles (AlKalbani et al., 2023). This is important because it provides a starting point for designers, developers, and users alike to begin considering the impact of usable cybersecurity on their projects.

While we do appreciate specific advice given in areas such as authentication, access control, encryption, firewalls, secure device pairing, and safe interaction, at this moment we are concentrating more on general and, as a result, generally context-independent suggestions. A list that is focused on that general level is necessary because it will form a central part of future work. This work will, among other things, include assessing the applicability (and possible targeting) of guidelines for using technologies in the standard operating procedure of organization in security controls perspective (Rawal et al., 2023). In this manner, we can develop a better understanding of how different processes and technologies can be effectively used to create secure systems. A list focused on that general level is necessary because it will form a central part of future work. We also believe that this list may have a value that extends beyond our immediate intentions because it provides a helpful state-of-the-art review that can be utilized by academics, system designers, and IT professionals (Camgöz Akdağ & Menekşe, 2023; Solar, 2023).

A framework is required to implement cybersecurity in contexts that are both national and international and that handle hyperconnectivity. The Mission Framework offers a framework that may be used to bring together the three most important aspects of cybersecurity, which are education, policies, and technologies (Purwanto et al., 2023). The education review includes a discussion of the accrediting agencies for programs connected to IT or computer science. This discussion provides insight into creative approaches to teaching cybersecurity coursework. An organization needs to do a thorough examination of the governing policies, tools, and strategies that can be advanced in the field of cybersecurity education (English & Maguire, 2023). To build a portion of the model, it is necessary to conduct additional research into a variety of ideas, including simulation, virtualization, and engineering standards.