Chapter 4
Protection of Critical Infrastructure Using an Integrated Cybersecurity Risk Management (i-CSRM) Framework

Halima Ibrahim Kure
University of Central Lancashire, UK

Augustine O. Nwajana
https://orcid.org/0000-0001-6591-5269
University of Greenwich, UK

ABSTRACT

Risk management plays a vital role in tackling cyber threats within the cyber-physical system (CPS) for overall system resilience. It enables identifying critical assets, vulnerabilities, and threats and determining suitable proactive control measures to tackle the risks. However, due to the increased complexity of the CPS, cyber-attacks nowadays are more sophisticated and less predictable, which makes risk management task more challenging. This chapter proposes an integrated cyber security risk management (i-CSRM) framework for systematically identifying critical assets through the use of a decision support mechanism built on fuzzy set theory, predicting risk types through machine learning techniques, and assessing the effectiveness of existing controls through the use of comprehensive assessment model (CAM) parameters.

DOI: 10.4018/978-1-6684-3855-8.ch004

INTRODUCTION

The primary objective of critical infrastructure is resilience by delivering its users with uninterrupted services, thus, relying on their most valuable assets such as information and communication networks, and digital data, for its continuous services (Wu et al., 2015). These assets necessitate the attainment of reliability, stability, and performance, all of which necessarily require the tight integration ofcontrol technological systems, computing and communication (Kim & Kumar, 2013). However, the cyber-physical systems (CPS) complexity and the interdependencies among its various components (people, processes, technology, multiple distributed and independently operating systems) has made it an excellent target for cybercriminals. Such systems face different security threats, including system failures (e.g., device failure, system overload), human errors (e.g., lack of access control, medical system configuration error), supply chain failures (e.g., network provider failure, power outage) and malicious actions (e.g., malware, hijacking, cyber espionage (Jalali & Kaiser, 2018). Cyber-security threats lead to any potential risks, and risks can affect all aspects of critical infrastructure. The probability of loss (Dalziell & McManus, 2004)or an uncertain occurrence that may occur and affect the organization's accomplishment of strategic, operational, and financial objectives is referred to as risk(Jasmin Harvey & Service, 2007).

The significance of protecting the critical infrastructure is significant since it can strongly affect the international market economy and the trust foundations between people and societies. Now, more than ever, shielding and securing critical infrastructures is essential, especially in the healthcare sector. The COVID19 pandemic has stressed the healthcare sector's requirements since malicious entities aggressively exploit this emergency for their benefit. For example, there is a considerable number of registered domains on the Internet that contain terms related to keywords, such as "corona", "covid", "covid19". While many of them are legitimate and focus on the pandemic, numerous domains are used to spread malware via phishing and spam campaigns. Therefore, the presence of any successful cyber-attack on the systems causes a devastating effect on the organization's critical infrastructure, its business processes, and availability of its services, reputation and the economy at large.

On the other hand, the cyber-threat landscape is evolving rapidly because threat actors' motivation and goal, attack pattern, "tactics, techniques and procedure (TTP)", tools to breach systems are becoming increasingly sophisticated. This affects the understanding of risk, its severity, and cascading risk impact level, making risk management challenging for critical infrastructure systems (Fossi et al., 2011). According to a recent Experian report, almost half of all business organisations experience at least one security incident each yea(Experian, 2015). That is why global cybersecurity spending is continuously rising to 96 billion US dollars in 2018 (Boyson,

Urban Telecommunications Network: Technology Convergence and Urban Infrastructure

Tan Yigitcanlar and Hoon Jung Han (2012). *Wireless Technologies: Concepts, Methodologies, Tools and Applications (pp. 1136-1149).*

www.igi-global.com/chapter/urban-telecommunications-network/58835?camid=4v1a

New Methods for Improved Indoor Signal Strength Positioning

Ian Sharp and Kegen Yu (2018). *Positioning and Navigation in Complex Environments (pp. 1-49).*

www.igi-global.com/chapter/new-methods-for-improved-indoor-signal-strength-positioning/195712?camid=4v1a