Chapter 4
Deciphering the Myth About Non-Compliance and Its Impact on Cyber Security and Safety

Kwasi Danso Dankwa
University of Reading, UK

ABSTRACT

The use of computers and sophisticated technologies are on the rise, and organizations are constantly looking for ways to invest in technologies to stay ahead of the competitive market. As such, cyber security and safety measures have been put in place by the organizations to protect them from attacks and to ensure that products and services are safe. However, managing cyber security and safety is becoming more challenging in today's business because people are both a cause of cyber security incidents as well as a key part of the protection from them. It is however that non-compliance with policies and directives are major security breaches. What is not well known, however, are the reasons behind the non-compliance behaviours. This chapter seeks to explore the reasons behind the non-compliance behaviours by use of compliance assessment model (CAM). The chapter reviews a case study in a health centre and systematically assesses the reasons behind the non-compliance behaviour by using the CAM model.

INTRODUCTION

The ubiquitous changes in the technological space require stringent measures to ensure that data integrity and security are not compromised. As a result, many rules and regulations have been enacted to manage the risk to stakeholders' interaction in the technological space. These regulations are not only limited to organizations and businesses, but countries have also put cyber security measures in place to protect their institutions and citizens. As a result of the increased regulations, set of harmonized and consolidated compliance controls have been adopted by organizations to promote operational transparency (Silveira et al., 2012). Importantly, organizations have put in systems and applied commensurate effort to aid compliance to relevant laws, policies, and regulations. This reduces unwanted replication

DOI: 10.4018/978-1-7998-3149-5.ch004

of effort and waste of resources while ensuring that all relevant governance stipulations are attained (Dankwa & Nakata, 2018).

Moreover, without relevant systems and processes that enable compliance knowledge, organizations may repeat and duplicate compliance breaches and even risk information leak or loss as they struggle to learn from the past non-compliance experiences (Caroline & Meyer, 2012). Despite systems and measures in place to curtail impact on security and safety, there are many instances within organizations where non-compliances have been reported. The cause of the non-compliances has been indicated to be multifactorial with different impact on people, organizations and even countries. Again, some questions remain unanswered although there is improved appreciation of how IT systems boost corporate execution (Kim & Kim, 2017). In addition, there is minimal information about the efficacy of the compliance support network in place, promoting the compliance intention of individual employees and thus enabling the assessment of compliance behaviour. Thus, this chapter seeks to address these questions:

a) What are the reasons behind the non-compliance behaviours?
b) How can understanding the reasons behind non-compliance behaviours help organizations to address and improve their systems?

The chapter proposes that the understanding and resolution of these questions will enable organizations to make compliance support systems that promote overall employee compliance intention and hence improve compliance behaviour. Consequently, the author seeks to explain the myth about non-compliance by considering the reasons behind non-compliance and the impact of it on safety and security. The author seeks to approach this paper from the potential impact of security and safety breaches on patient treatment and other relevant stakeholders within the health care sector. The author proposes that in most cases, non-compliance occurs because stakeholders do not understand the importance and usefulness of the rules and regulations in place. The study further argues that, many of the non-compliances are due to people not knowing their role in the security and safety architecture, their role in adoption and use of the technology or resource available and the impact of their failures on safety and quality of patient treatment.

The remainder of the chapter is organized as follows: Section 2 summarizes the background of previous research and studies within the field of cyber security and safety. This further considers the various gaps and factors that impede compliance to security and safety procedures, rules and regulations. In section 3, the chapter introduces the methodology that will be followed in this study to address the questions that were posed. Section 4 considers the rationale for the chosen model for the appraisal of the intentions behind the non-compliance behaviour. This is followed in section 5 by review of a case study in the health care sector using the chosen model. In section 6, the chapter discusses the outcome of the assessment and considers the limitation of the study and further work. Section 7 then concludes the whole chapter.

BACKGROUND

The quest for organizations to stay on top of the competitive market has led to the need for adoption of computer and internet technology to greatly improve the way businesses operate (Sikolia, 2013). This is not confined to the business world as the Health sectors have also implemented computers and other complicated information systems for better patient management. Importantly, the extended use