Chapter 2
The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation:
The Role of Cyber and Information Technology Security in Automated Business Environments

Antoine Trad
Institute of Business and Information Systems Transformation Management, France

Damir Kalpić
University of Zagreb, Croatia

ABSTRACT

The business transformation project (BTP) of a modern business environment needs a well-designed information and cyber technology security automation concept (ITSAC) that, in turn, depends on measurable success factors. These factors are used for the evolution of the transformation process. During the last decade, due to the global insecurity and financial crisis, the security strategies are not efficient. That is mainly due to the fact that businesses depend on security standards, cyber and information technology evolution, enterprise architecture, business engineering, and multilevel interoperability. They are restricted to blindfolded infrastructure security operations. Major BTPs are brutally wrecked by various security violations that may cause a no-go decision.

DOI: 10.4018/978-1-5225-5927-6.ch002

INTRODUCTION

The Business Transformation Project (BTP) of a modern business environment needs a well-designed Information and cyber Technology Security Automation Concept (ITSAC) that, in turn, depends on measurable success factors; these factors are used for the evolution of the transformation process. During the last decade, the security strategies and measure are insufficient due to the global insecurity and financial crisis. That is mainly due to the fact that businesses depend on security standards, cyber and information technology evolution, enterprise architecture, business engineering, and multilevel interoperability. They are restricted to blindfolded infrastructure security operations. Major BTPs are brutally wrecked by various security violations that may cause a no-go decision. Most of such security misfits are used for internal politics, while highly important issues and teams' problems are simply ignored.

The most damaging fact is that business environments lose their transformational momentum, what can negatively affect their business sustainability and leave it open to security breaches and financial loses. Financial Technology (FinTech) is the latest technology buzzword that aims to change the traditional financial environment in the delivery of interactive financial services. In this article, the authors propose a set of managerial recommendations on how to avoid such critical situations.

Today many security architectures exist, and even when very advanced, unfortunately they often follow a silo model. This chapter can support the Cyberbusiness transformation process of the traditional business environment through the automation of all its security operations and their related business processes. Transforming a traditional security subsystem and the related archaic legal constraints is an important challenge, because of the probability that the security and legal team(s) resist to change. An ITSAC subsystem may provide the base for flexible business services for the future business environment to avoid the security-human dependency.

The aim of this chapter is to support business transformation managers or enterprise architects in managing frequent changes to business environments and the integration of automated ITSAC procedures. To achieve this goal, the authors offer an ITSAC automation pattern that could support transformation processes. Security controls for a business entity, regional body, government, or geopolitical entity is a set of interrelated activities from various domains like security architecture, financial engineering, geopolitical influence, governance and legal conformance. All that can be used to avoid financial crimes, business disruptions and corruption.

Complex transformation initiatives must be coherent with the entity's business and security strategic planning goals; where the main strategic goal is to minimize the various types of criminal acts. Security controls are the fuel of the entity's sustainable business growth and its integration in global economies. Security control schemes can be supported by security and risk frameworks, standards, and legal controls that are necessary for the company's business strategy that is based on a cybersecurity background (Trad & Kalpić, 2017a; Trad & Kalpić, 2017b)

BACKGROUND

In a holistic cybersecurity architecture, the Business Transformation Manager's (BTM) role is important and his or her (for simplicity, in further text – his) decisions are aided by using factors within an implemented applied mathematical model. A large set of factors can influence such a mathematical model, including: a) the role of the cybersecurity enforcement control by using ITSAC; b) global geopolitical