Towards Efficient Security:
Business Continuity Management in Small and Medium Enterprises

Christian Reuter, Institute for Information Systems, University of Siegen, Siegen, Germany

ABSTRACT

Business Continuity Management (BCM) is an integral part of civil security in terms of corporate crisis management. According to the ISO 22301 (2014) BCM is defined as a holistic management process which identifies potential threats to an organization and the impacts those threats might have on business operations. Looking at the current situation of studies conducted in this field it seems to be obvious that the use of BCM in Small and Medium Enterprises (SME) is underrepresented and that the security level is partially located in an uneconomical range. This paper presents a literature research on the use of BCM in SME and discusses research findings concerning this matter. Based on this a matrix for possible impacts vs. quality of the crisis management for different actors is derived. The article concludes with the presentation of lightweight und easy to handle BCM security solutions in form of Smart Services, as a possible solution for the increasingly IT relaying industry 4.0.

Keywords: *Business Continuity Management, Enterprises, Small and Medium Enterprises*

1. MOTIVATION AND INTRODUCTION

The power failures in India 2012 (670 million affected people), in Brazil and Paraguay 2009 (87 million affected people), in Europe 2006 (10 million affected people) and in the USA and Canada 2003 (55 million affected people) show that major unintended interruptions of the electrical power supply can still happen everywhere on the planet, even today (Reuter & Ludwig, 2013). The German parliament (2011) analyzed the threats for modern societies using the example of a long and large-scale breakdown of the power supply and came to the conclusion that based on the almost complete pervasion of the living and work environment with electronic driven devices the consequences can add up to a critical situation of outstanding quality.

Besides power failures there is a range of additional possible reasons - like the hurricane Kyrill in Europe 2007; the tsunami and earthquake disaster in Japan 2011; the hurricane Sandy in the USA 2012; and even events which seem slightly smaller. Some studies indicated that over the last decades the frequency and intensity of natural disasters increased (Berz, 1999). The consequences can be so large-scale that the security of the citizens is not only concerned

DOI: 10.4018/IJISCRAM.2015070105

in their private but even in their work environment. The negative influence on the continuous economic practice of enterprises is another possible consequence of a breakdown. This can lead to problems in business processes - for example if workflow-management components fail (Reuter & Georg, 2008) and cause additional extensive damage.

Since the third industrial revolution (digital revolution) - the usage of electronic and IT for automation of the production - and at least since the upcoming fourth industrial revolution - the merging of the real and the virtual world to become an internet of things which is being discussed as the future project of "industry 4.0" (Bundesministerium für Bildung und Forschung, 2015) - enterprises increasingly depend on the continuous use of IT.

However, due to the relative low chance e.g. of power failures in Western Europe the overall preparations are not optimal (Birkmann, Bach, Guhl, Witting, et al., 2010). The German Federal Ministry of the Interior (Bundesministerium des Inneren, 2009) calls this fact *vulnerability paradox*: In the dimension in which the supply performance of a country is less accident-sensitive, the effect of an accident is even stronger. Especially societies which use high industrialized and very complex technologies react more sensible to accidents because they are used to very high security standards and high supply reliability. Because of an increasing robustness and a lower accident-sensitivity it is possible that an illusory feeling of safety evolves. This can lead to the consequence that the impact of an accident which happens despite that is disproportionately high (Bundesministerium des Inneren, 2009, p. 10).

Conversely there exists a trend that public and even more private infrastructure carriers are in the area of conflict between consistently basic service and economic optimization (Kloepfer, 2005, p. 17). Therefore there is a risk that the availability of infrastructure is reduced to the contractual and businesslike minimum. Due to the resources we assume that the arising gap can at best be compensated by large enterprises, partially by SME and not at all by individuals.

BCM should contribute to the maintenance of the supply of production and/or service processes of an organization in previously defined levels; for those who would fail in case of an incident that causes a business interruption (Bundesamt für Sicherheit in der Informationstechnik, 2008). The safety of SME is essential for the European economy because they represent 99% of all enterprises (Thiel & Thiel, 2010). In this paper we aim to answer the research question if and how BCM can, could or should be used in SME.

Using the scientific literature databases available at the university a search for "BCM and SME" (abbreviated and unabbreviated) has been performed. We summarize the state of the art, propose a model for possible impacts vs. range and quality of the crisis management for different actors, and derive suggestions how to move towards efficient security.

2. DEFINING CONTINUITY MANAGEMENT

Business Continuity Management (BCM) is defined by the ISO 22301 (2014) as a "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause." BCM "provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities". According to the German Federal Office for Information Security (BSI, 2008) BCM is a "management process with the goal to discover fatal risks for an institution that could endanger the viability at an early stage and establish methods against them."

BCM as a kind of crisis management has evolved since the 1970s as a reaction to technical and operational risks concerning enterprises (Herbane, 2010a). The first international valid