Accepted Manuscript

Title: Information systems continuity process: conceptual foundations for the study of the 'social'

Author: Marko Niemimaa

PII: S0167-4048(16)30154-7
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2016.11.001
Reference: COSE 1055

To appear in: *Computers & Security*

Received date: 20-6-2016
Revised date: 9-10-2016
Accepted date: 4-11-2016

Please cite this article as: Marko Niemimaa, Information systems continuity process: conceptual foundations for the study of the 'social', *Computers & Security* (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.11.001.

Information Systems Continuity Process: Conceptual Foundations for the Study of the 'Social'

Author's name and affiliations: Marko Niemimaa, University of Turku, Turku School of Economics, Information Systems Sciences
Biography: Marko Niemimaa is a PhD candidate at the Turku Centre for Computer Sciences and University of Turku, Turku School of Economics in the department of Information Systems. His main research interests lie in the fields of IS security management, IS operations and sociomateriality. He has strong practical background in information systems security and business continuity that he has gained through years of work experience as a technical specialist and a consultant in the field.

Keywords: business continuity, information security management, IS continuity, incident, information systems, IS theories

Abstract

Organizations' value creation is dependent on the reliable and continuous operations of their inherently unreliable information systems (IS). Year after year industry and academic surveys show that IS-related incidents persist as a top concern on IS managers' agendas. While past research has addressed technological improvements and planning methodologies as a means of improving the continuity of organizational technologies (IS continuity), the 'social' part – that is, the humans and their social and cognitive processes – has largely remained in the background and under researched. This current research seeks to bring to the foreground the implications of the social for IS continuity by developing conceptual foundations of the social dynamics in the IS continuity process. This study proposes a framework of IS continuity process with three phases: (1) preparing for incidents; (2) coping with and mitigating the impact of incidents; and (3) recovering from incidents. Implications of and potential theoretical and conceptual foundations for the social in the IS continuity process are discussed together with their practical implications. Addressing the challenges that pertain to the management of IS continuity requires multidisciplinary approaches that broadly take use of social and cognitive theories on individual and collective levels of analysis.

1. Introduction

Organizations' business continuity, (i.e., their capability to sustain operations), is increasingly vulnerable to Information Systems (IS) incidents (e.g., Bajgoric, (2010); Butler & Gray, (2006)). Past incidents in which Information and Communications Technologies (ICTs) have failed suggests that despite technological advancements and improved overall reliability, ICTs can and will continue to fail. A brief glimpse at the news outlets often reveals several organizational incidents caused by ICT failures that vary from large scale interruptions to small scale annoyances. According to MIS Quarterly Executive's academic survey, organizational preparations for such incidents are among the top concerns for IS managers, and they have persistently remained among the core concerns for over a number of years (Kappelman et al., 2016). Recent industry surveys point to the same findings. A survey of 760 organizations based in 72 different countries showed that outages caused by cyberattacks and unplanned IT and telecommunications incidents top the list of issues (Business Continuity Institute, 2015). Ponemon Institute's (2015) survey found similar results. IS managers face the difficult problem of knowing that their ICTs will likely fail but not knowing when or how these fails will occur.

Despite the fact that it is the technologies that fail, failures in socio-technical systems (hereafter IS incidents), such as IS (Bostrom & Heinen, 1977) cannot be explained in terms of technology alone (Davis et al., 1992). Indeed,