Guest Editorial Preface

Special Issue on IT-Support for Crisis and Continuity Management

Christian Reuter, Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt, Darmstadt, Germany

Jens Pottebaum, Heinz Nixdorf Institute (HNI), Paderborn University, Paderborn, Germany

INTRODUCTION

On 21 January 2013, there was a fire at the central office of a telecommunications network operator in Siegen, which resulted in more than 500,000 telephone connections being collapsed for several hours and occasionally several days. Emergency calls were also not possible. The websites of the district and the control center were offline. The local radio which typically acts as a central point of information in such situations was out of service. But not only the civic-societal continuity, also the operational continuity was affected (Reuter et al., 2017). In this example, both continuity and crisis management are essential to recover to regular business resp. life.

Crisis management refers to the culmination and turning point of a dangerous trend, which can transform into harm or a catastrophe. The meaning of the word is a component of inflationary linguistic use. The Greek root word *krisis* (judgment, decision) shows the ambivalent possibilities and leads to a very important task in such situations: decision-making (Reuter, 2014) based on collaboration and information sharing (Pottebaum et al., 2016).

Continuity management, or especially business continuity management (BCM) is characterized 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…" (Reuter, 2015).

BCM as a kind of crisis management has created since the 1970s as a reaction to specific and operational perils concerning endeavors (Herbane, 2010). The global considerable standard for BCM was appropriated in type of the ISO 22301 (2012). The standard regulates essentials to design, build up, acknowledge, run, screen and audit a progression administration framework and to improve it continually.

This special issue takes both continuity and crisis management as well as their interdependencies into consideration. It received several submissions. After two rounds of peer review the resulting articles were selected and divided into two editions. The first set of articles is outlined in the following.

BUSINESS CONTINUITY MANAGEMENT IN MICRO ENTERPRISES

The first article *Business Continuity Management in Micro Enterprises: Perception, Strategies and Use of ICT* is written by Marc-André Kaufhold, Thea Riebe, Christian Reuter, Julian Hester, Danny Jeske, Lisa Knüver, Viktoria Richert (University of Siegen and Technische Universität Darmstadt, Germany). Considering the recent increase of man-made crises and natural disasters that potentially disrupt business operations, the aim of this article was to gain insights into the micro enterprises' perception of business continuity management and their strategies for preventing or overcoming

business disruptions. Hence, we conducted semi-structured interviews with 19 micro enterprises in Siegen (Germany) who experienced a total power failure in 2013 that resulted in a total of more than 500,000 telephone connections being non-functional. The empirical study highlights the low crisis awareness and varying technical dependency of micro enterprises and, depending on these influence factors, action and communications strategies currently applied. Based on these factors, a categorization of micro enterprises into preventive technicians, data-intensive chains and pragmatic jumpers was suggested.

INFLUENCE FACTORS FOR INNOVATION IN SELF-PREPAREDNESS SERVICES AND TOOLS

The second article *Influence factors for innovation in self-preparedness services and tools* was written by Iris Gräßler, Jens Pottebaum and Philipp Scholle (Paderborn University, Germany). IT support for crisis and continuity management covers all stages from prevention through preparedness to response and recovery. The application of innovative technologies often implies the need for reliable assessment of both future uses cases as well as business opportunities for providers of digital services and tools. Scenario-technique is a methodology to systematically assess possible future developments to derive conclusions for strategic planning. This methodology is adapted to the domain of self-preparedness and self-protection. The paper contributes 59 domain specific influence factors which are identified by literature research, analysis of historic data from four case studies and reflecting expert interviews. For each influence factor, projections are derived using different types of trend analysis and forecasting methods. Influence factors and projections build a knowledge base which enables generation of scenarios as a fundament for strategic decisions to support crisis and continuity management.

HANDLING INFORMATION OVERLOAD IN EMERGENCIES

The third article *Handling Information Overload in Emergencies: Usability Testing of a Social Media Tool for Journalists and Crisis Managers* is written by Klas Backholm, Joachim Högväg, Jenny Lindholm, Jørn Knutsen and Even Westwang (Åbo Akademi University, Finland; Oslo School of Architecture and Design; Institute of Design, Oslo, Norway). The article describes results of the investigation how to promote situation awareness in emergencies through the help of a technical innovation. The study introduces a tool that will support journalists and crisis managers with gathering information on social media. Two laboratory usability tests were conducted to identify if the user's mental models fit the product design. Results show that such a system needs to gather information from several social media channels and allow for varying, personalized modes. Users understood main tool concepts, but some features, such as saving content or manually evaluating information quality, were too time consuming. The study contributes to the field by identifying factors important for promoting a user-friendly design in emergencies. For instance, to avoid affecting user cognitive attention, the design needs to carefully balance between automated tasks and manual input.

REFERENCES

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, *52*(6), 978–1002. doi:10.1080/00076791.2010.511185

International standards organization. (2012). ISO 22301. (2012). Societal security - Business continuity management systems - Requirements. Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=50038

International standards organization. (2014). ISO 22301. (2014). *Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen (ISO 22301:2012); Deutsche Fassung EN ISO 22301:2014.*

Pottebaum, J., Schäfer, C., Kuhnert, M., Behnke, D., Wietfeld, C., Büscher, M., & Petersen, K. (2016). Common information space for collaborative emergency management. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1–6). doi:10.1109/THS.2016.7568904

Reuter, C. (2014). *Emergent collaboration infrastructures: technology design for inter-organizational crisis management* [Ph.D. Thesis].

Reuter, C. (2015). Towards efficient security: business continuity management in small and medium enterprises. *International Journal of Information Systems for Crisis Response and Management*, *7*(3), 69–79. doi:10.4018/IJISCRAM.2015070105

Reuter, C., Kaufhold, M.-A., Schorch, M., Gerwinski, J., Soost, C., & Hassan, S. S. … Wulf, Volker. (2017). Digitalisierung und Zivile Sicherheit: Zivilgesellschaftliche und betriebliche Kontinuität in Katastrophenlagen (KontiKat). In G. Hoch, H. Schröteler von Brandt, V. Stein et al. (Eds.), *Sicherheit (DIAGONAL Jahrgang 38)* (pp. 207–224). Göttingen: Vandenhoeck & Ruprecht. Retrieved from http://www.peasec.de/paper/2017/2017_ReuterKaufholdSchorchetal_DigitalisierungSicherheitKontiKat_Diagonal.pdf

Christian Reuter, PhD, is Professor for "Science and Technology for Peace and Security" (PEASEC) at Technische Universität Darmstadt and supervisor of the BMBF research group KontiKat at the University of Siegen, Germany. His research focuses on interactive and collaborative technologies such as social media in safety-critical environments, conflicts, crises and emergencies.

Jens Pottebaum, Dr.Ing., is senior researcher and lecturer at Paderborn University, Germany, in the Heinz Nixdorf Institute, department for Mechanical Engineering (research group 'Product Creation'). His research focuses on multi- and interdisciplinary approaches on applicability and application of Information Technology to solve challenges in (Product) Data Management and Virtual Engineering as well as complex situations in public safety and security.