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.

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 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 standard for BCM was only published back in 2012 in form of the ISO 22301 (2012) (in German: ISO 22301, 2014). The standard specifies requirements to plan, establish, realize, run, monitor and review a continuity management system and to improve it continuously. It replaced the previously existing British Standard BS 25999 (2007). More international standards are the US-American NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs (2013) as well as the Canadian CSA Z1600: Essential Emergency Management and Business, based upon it.

The German BSI-standard 100-4 (2008) for emergency management in enterprises shows a systematic way to ensure the continuity of business operations. Challenges for an emergency management are therefore to increase the reliability and to adequately prepare the institution for emergencies and crises, so that the important business operations can be quickly resumed. It is the goal to minimize damages caused by emergencies and crises and to secure the existence of the government agency or the enterprise even in major critical situations.

There are many reservations about emergency management (Bundesamt für Sicherheit in der Informationstechnik, 2014): the denial of possible risks, the fear, that the necessary activities and the measures to implement for emergency prevention are only going to complicate the processes in the organization, a certain carelessness (“Things always worked out fine before”), the exclusive treatment of this topic from the angle of costs, or the aversion to deal with this task without any direct external force. But also if more open mindedness for this topic existed, it wouldn’t necessarily lead to actually doing more for emergency prevention. These are declarations of intents, which however take a back seat quickly in the daily business. Furthermore an institution leaves it at isolated technical measures (“better data protection”) without examining, if these measures are sufficiently effective in emergency situations or crises.

Examples are easy to find: In 2006 the transfer of the ocean liner Norwegian Pearl from the shipyard at the Ems to the North Sea could entail power failure up to North Africa (in consequence of the selective shutdown of a small part of the grid in order to facilitate the safe transfer of the Norwegian Pearl, and a concatenation of unfortunate circumstances). In October 2008 because of the failure of a substation in Hannover in about 150 banks the cash machines, bank statement printers and the Online-Banking couldn‘t be used anymore throughout whole Germany. In January 2009 faultily performed maintenance work in a computer center resulted in the fact, that no rail tickets could be sold throughout Germany for hours, the trains had substantial delays or were cancelled and furthermore in many places several customers complained about the, from their perspective, insufficient information from the concerned transport company. The volcanic eruption of Eyjafjallajökull in April 2010 (Reuter et al., 2012) in Iceland, could lead to a nearly complete standstill of the air traffic in Europe for days. This for example raised the fear of production interruptions in several companies because of delayed supplies.

The examples have in common, that ostensible local events brought along unexpected broad effects and considerable damages. The instances show how cross-linked, and thus simultaneously vulnerable modern industrial countries and their institutions are.

3 RESEARCH FINDINGS ON THE PERCEPTION OF INFRASTRUCTURE BREAKDOWNS

Remarkably, power failures as examples for causes, are hardly perceived as a real threat in the population (Lorenz, 2010). According to a survey on a London power failure in 2003, many respondents reacted surprised by the fact, that failures like this can happen at all (Brayley et al., 2005). The lack of the power supply is not combined with fear or concerns. If devices necessary for the household, like a refrigerator or stove or even the computer are not working anymore, it is accepted in the first place. However, according to the respondents, longer-term failures would quite be noticed, in particular the absence of critical infrastructures. Furthermore, the fact, that the supra-regional media report little about power failures, leads to a lower risk perception among the population (Lorenz, 2010). According to Lorenz (2010, p. 29) certain information is not aware in the population and cannot be adequately implemented until it is integrated in a broad dialogue about possible dangers because of power or infrastructure failures. Therefore the Federal Ministry for nutrition gives the advice to get a stock of food lasting for 14 days, to be capable of acting in emergency situations (Bundesministerium für Ernhährung, 2010).

Necessarily the question arises whether solely the communication throughout the population should be supported in an infrastructure failure or if moreover possibilities should be worked out to meet the information needs among the population already before the failure (Reuter, 2014a). Furthermore the capacity for self-help of the population is the most important factor to determine, how much time goes by from the beginning of the catastrophe to the irreversible destruction of social structures (Lorenz, 2010, p. 34). This capacity for self-help implies that people are able to communicate with each other in a crisis and receive or share crisis-relevant information.

In many cases the population is just seen as a passive and needy receiver of help, which at best takes thankfully and at worst complicates the organizational processing of the problem situation by professional actors due to its conduct (Lorenz, 2010). In other words the population is assigned a victim role (Hunt, 2003). These conclusions turn out to be premature. On the contrary the population has to play the role of an important participant during a crisis. Thus many citizens use their social groups and networks to help each other and receive or share information (Drabek, 2013; Murphy, 2004). Quarantelli (1993, p. 73) describes that population groups immediately try to tackle the problems caused by a crisis in such situations. Moreover the population names coordination and a decentralized decision making as the most effective ways to react to a crisis. “Contrary to what is often portrayed, local citizens are the true ‘first responders’ in emergency situations”, Palen, Hiltz, & Liu (2007, p. 54) wrote and emphasized that citizens often act as first-aiders and bring victims or injured people to the hospitals. Coombs (2009) demands so-called *Instructing Information*, which points out how affected persons can protect themselves and behave before or in a crisis. When an exceptional situation already occurred such information must also be provided to supply the persons, which haven’t received these information before the crisis (Reuter, 2014a). The importance of the population as a participating actor to react to a crisis therefore implies appropriate possibilities for the acquisition and dissemination of relevant information.

The necessity of communication during a crisis scenario is also the result of the information needs of the individual (Reuter, 2014a). A power failure which endures for longer than 24 hours could already have serious consequences for the patients in a hospital. The UPS

(uninterruptible power supply) ensures an emergency operation in the first 24 hours. Individual organizational areas, like the administration are already restricted. After 24 hours the failure of the UPS leads to the point that certain medical devices no longer function or medical products cannot be cooled anymore (Hiete et al., 2010). The power failure in the Münster region entailed the situation, that 20.000 people couldn't be supplied with power up to four days later (Birkmann, Bach, Guhl, & Witting, 2010). The scenario of a hospital without access to electricity for a longer time is thus quite realistic and dangerous. Hence information needs exist in particular for the population outside the hospital, because the patients on-site can be informed by the employees. In the Münster region the power failed because of the storm Torsten due to a low pressure area, which is kind of a crisis before the crisis (Birkmann, Bach, Guhl, & Witting, 2010). Information about hospitals with emergency power supplies can be vital for persons, which for example were injured due to falling trees landing on their motor vehicles and thus must be treated urgently, because they possibly can't get the needed treatments without the information.

4 RESEARCH FINDINGS ON THE USE OF BCM IN SME

BCM is dedicated for all kinds of enterprises regardless of its size. According to the definition of the EU-Commission (2003) an enterprise belongs to the SME if it does not have more than 249 employees and annual sales not higher than 50 million Euro or a total asset of 43 million Euro at most. The safety of SME is essential for the European economy because they represent 99% of all enterprises (Thiel & Thiel, 2010) and SME are sometimes considered to be most vulnerable to the impacts from various disruptions. Therefore the need for SME to implement effective coping mechanisms to manage the effects of extreme weather events is increasing (Wedawatta et al., 2010).

However, according to a study of the Network Electronic Trading only every fifth SME prepares an emergency plan for IT and every fourth SME lacks in a standardized procedure for dealing with IT emergencies as quickly as possible (Duscha, 2009). Other studies discovered that 45% of the US-American and European SME could not show a BCM concept (ENISA, 2009). Another study in Great Britain shows that BCM is significantly less present in SME (Musgrave & Woodman, 2001). Furthermore rather 41% of the enterprises do not plan for crises of all kind at all (Semantec, 2011).

Herbane (2010b) empathized the economically meaning and vulnerability of SME. Through the comparison of research literature in the area of SME research and crisis management he summarizes that more attention towards a combined observation of both areas is necessary. Especially the use of BCM in and for SME was not much examined yet (Herbane, 2013). Other studies indicate that the security level in SME is significantly lower than in large enterprises (Duscha, 2009; European Network and Information Security Agency (ENISA), 2009; Musgrave & Woodman, 2001). A questionnaire survey, conducted as part of a "Community Resilience to Extreme Weather" research project, identified that SME mostly rely on "generic business continuity strategies as opposed to property level protection measures" (Wedawatta et al., 2010). A case study investigated five SME' actual crisis management practices. The results show that "SME, in spite of their resources constraints and relatively weak market positions, display resilient market responsiveness" (Hong et al., 2012).

An essential reason against the introduction of BCM in SME is the effort to implement abstract and generic described safety precautions in the working practice (ENISA, 2009). The

complexity of BCM was identified as a problem for SME: Guidelines have to be translated into an individually fitting and understandable language; this step is hard to do for a SME (Thiel & Thiel, 2010). According to the European Network and Information Security Agency (ENISA, 2009) there is a huge need for simplified approaches regarding safety und crisis management. The *natural disaster syndrome*, as indicated by Hurricane Katrina is another observation: "Prior to a disaster, individuals in hazard-prone regions do not voluntarily adopt cost-effective loss reduction measures. The federal government then comes to the rescue with disaster assistance even if it claimed it had no intention of doing so prior to the event" (Kunreuther, 2006).

5 MODEL: (IN-) EFFICIENT SECURITY

Taking the research findings of the previous chapter into consideration some conclusions are obvious: The security level in SME is lower than in large enterprises; BCM is also not as common in SME as in large enterprises; however, also SME have risks.

It is possible to turn these observations in a descriptive model (Figure 1): The x-axis of the graph shows the possible impact, the y-axis the quality of emergency management.

- *Individuals* (on the bottom left in Figure 1) normally do not have a dedicated safety management in terms of BCM and little safety engineering with normally little consequences in case of a breakdown. Reasons why individuals do not protect themselves prior to a disaster are that they "underestimate the likelihood of a future disaster, often believing that it will not happen to them; have budget constraints; are myopic in their behavior; and/or do not want to be the only one on the block modifying their structure" (Kunreuther, 2006).
- Large *enterprises* deal with this intensively by high economic consequences at the same time (e.g. production breakdowns, process interruptions).
- But particular *SME* – which have been shown in the previous sections - have a undersupply in this area in relation to the possible consequences, as mentioned above (e.g. Duscha, 2009; ENISA, 2009; Thiel & Thiel, 2010). Therefore it is needed to deduce approaches for enhancing the quality of the emergency management.

The position of the different groups is based on the findings discussed in the literature review – however it needs to be evaluated with empirical data explicitly observing the possible impact and the quality of emergency management, also to quantify the corridor of efficient security, which currently is just defined as the meaningful measure between potential risk and protection. Rather clear from the perspective or other studies is that most SME are not optimal protected – and it is agreed, that the level of security needs to be improved while avoiding high investments, but by providing SME appropriate solutions.

It has to be considered that the matrix looks different for different industries – and the aim is not to highlight all those differences, but to make aware that according to many articles SME are more likely to be in the corridor of non-efficient security. Still, some industries (including SME) are very security relevant (e.g. chemical industry) – therefore there are high requirements on BCM by law. Using the example of Germany, according to an emergency regulation - § 10 Störfallverordnung (Bundesrepublik Deutschland, 2015) - for some operation areas a safety report is required and the responsible emergency response authority

has to create an external emergency plan as well, where the data related to the operating range (prepared) measures of emergency authority are described.

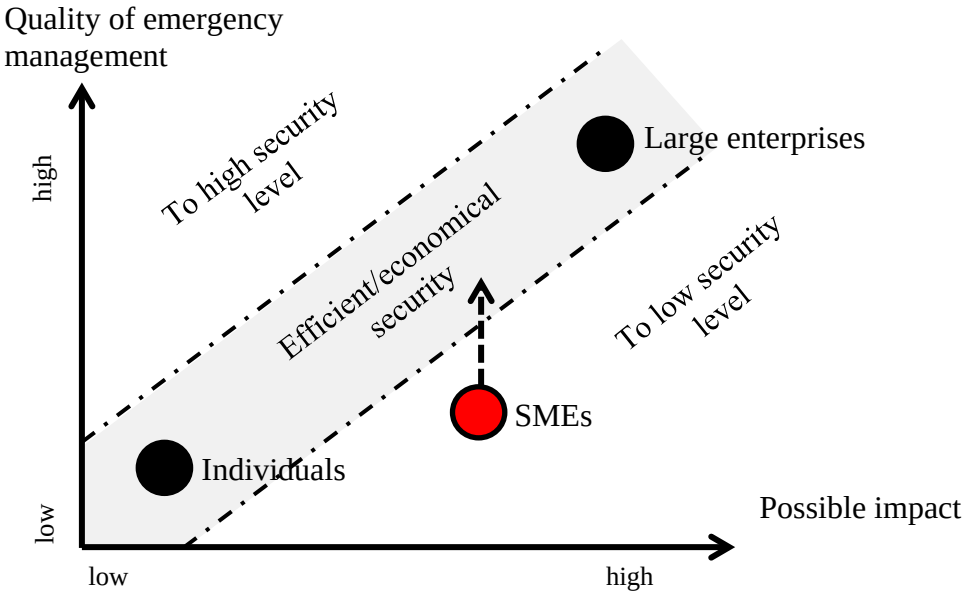

Figure 1: Efficient Security: Individuals, SME and large enterprises regarding impact vs. quality of the emergency management.

6 TOWARDS EFFICIENT SECURITY: APPROACHES FOR BCM IN SME

Besides the descriptive nature of the model (position of individuals/SME/enterprises) the model also contains a normative aspect on the intention to move SME towards efficient security.

Even if there was not too much research conducted in this area yet there already exist some approaches to improve BCM in SME: As Sullivan-Taylor & Branicki (2011) notice in their fittingly named article “why one size might not fit all”, enterprises of different sizes are leading to varying requirements for the use of BCM-systems. BCM for SME should consider the conditions of SME, like providing low personal resources, a lack of expert knowledge in risk management, and support for IT layman (Thiel & Thiel, 2010).

Based on a survey and interview study with 59 SME and resulting benchmarks Thiel & Thiel (2010) present a guideline of enterprise specific BCM for the implementation in SME which includes the individual SME characteristics, and which acts as a translator in the form of breaking the complex requirements down to the practice of SME. Another approach by Wedawatta & Ingirige (2012) suggests a combination of object-based safety measurements und generic BCM-measurements to strengthen the resilience of SME. Li et al. (2015) focus on the development of an agent-based model for simulating and deducting solution strategies for SME in case of a flood. Lee & Jang (2009) emphasize the information safety as a special aspect of BCM and develop an information security management system model for SME. Horváth (2013) also presents an integrated system for merging BCM with information security management activities. The tool, developed by Sapateiro et al. (2011), emphasizes the collaborative BCM activities and could be called a lightweight BCM solution,

independent of the size of the enterprise which addresses the collaboration, the knowledge management, the team performance and the awareness of the situation.

Lightweight, simple and efficient BCM as a service for SME currently still represents a gap in research and development. The development of new business models and hybrid value chains for lightweight and easy to handle BCM security solutions for SME should support the phase before the crises (identification of important data, processes and workplaces, risk evaluation, action plans, exercises, measurement of the effectivity und efficiency of the actions) as well as the phase after the occurrence of the crises to enhance the level of the safety management. Smart services - services that are integral part of a product (Allmendinger & Lombreglia, 2005) - could reduce the necessary level of investment and complexity for SME.

While looking at specific security relevant industries, advanced BCM and security solutions are already implemented. Also insurances reward the use of BCM and security preparations – as long as their risk is reduced as well. Some insurance companies already provide services, such as weather warnings for free for their clients[1] and it is obvious that such services can also reduce the risk for the insurance company. Concerning SME, advanced services – besides consulting and insurance – might help them to move their behavior towards the area of efficient security.

According to the German Federal Office for Information Security SMEs use more and more virtualization technologies and cloud services to protect their IT based business processes against failure (Bundesamt für Sicherheit in der Informationstechnik, 2013). According to a recent study by BITKOM, however, the demand for cloud services will continue to grow worldwide. In 2014 the market for cloud computing rose by 46 percent to 6.4 billion euros. Until 2018, an increase of the cloud market is forecast at 19.4 billion euros, stating an annual growth rate of 35 percent (BITKOM, 2014)

7 CONCLUSION AND SUMMARY

The need to implement BCM for SME is incontrovertible. Apart from reasons such as ensuring the productivity and the continuation of the firm, different laws require the use of BCM.

Much prior research – as indicated by Herbane (2010b) – has focused on SME or crisis management, however a combination has seldom be considered. In order to review the few work that has been done in this field this article investigated the current research situation in the area of the business continuity management (BCM) in small and medium enterprises (SME) and has deduced a matrix for the positioning of SME in relation to possible impacts vs. quality of crisis management. The matrix provides a decent visualization of why research in this area is valuable and necessary.

The reviewed research findings lead to the conclusion that the use of BCM in SME seems to be low (Duscha, 2009). Other articles claim that exact findings are still missing (Herbane, 2013). It became especially obvious that SME have other requirements for the range of a solution, matching their individual risk and enterprise size (Sullivan-Taylor & Branicki, 2011). In order to address the specifics of SME lightweight and easy to handle BCM solution for SME as smart services are required and need to be researched.

[1] https://www.provinzial.de/web/html/privat/service/wind_und_wetter/

Considering the *IT usage in emergent situations* that are dynamic and not predictable (Reuter, 2014b) as well as the need for an *uninterruptible IT use* in the industry 4.0 – this therefore provides a research gap. In future work studies about the use of BCM in SME combined with lightweight BCM services might contribute to the available knowledge in this field.

8 REFERENCES

Allmendinger, G., & Lombreglia, R. (2005). Four strategies for the age of smart services. *Harvard Business Review*, *83*(10). doi:10.1225/R0510J

Berz, G. (1999). Naturkatastrophen an der Wende zum nächsten Jahrhundert – Trends, Schadenpotentiale und Handlungsoptionen der Versicherungswirtschaft. *Zeitschrift für die gesamte Versicherungswissenschaft*, *88*(2-3), 427–442.

Birkmann, J., Bach, C., Guhl, S., & Witting, M. (2010). State of the Art der Forschung zur Verwundbarkeit kritischer Infrastrukturen am Beispiel Strom / Stromausfall. Risk Management. In *Forschungsforum öffentliche Sicherheit*.

Birkmann, J., Bach, C., Guhl, S., Witting, M., Welle, T., & Schmude, M. (2010). *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom / Stromausfall*. *Risk Management*. Berlin, Germany. Retrieved from http://www.sicherheit-forschung.de/schriftenreihe

BITKOM. (2014). Markt für Cloud Computing wächst ungebrochen. Retrieved from http://www.bitkom.org/de/presse/81149_80724.aspx

Brayley, H., Redfern, M. a., & Bo, Z. Q. (2005). The Public Perception of Power Blackouts. *2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific*, 1–5.

British Standards Institution. (2007). *British Standard BS 25999: Business Continuity Management*.

Bundesamt für Sicherheit in der Informationstechnik. (2008). *Notfallmanagement – BSI-Standard 100-4*. Bundesanzeiger Verlag. Retrieved from https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2013). Notfallmanagement mit der Cloud für KMUs. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Notfallmanagement_mit_der_Cloud_KMUs.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik. (2014). *Webkurs Notfallmanagement auf Basis von BSI-Standard 100-4*. Retrieved from https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/0_Startseite/StartseiteWebkurs_node.html

Bundesministerium des Inneren. (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. Berlin.

Bundesministerium für Bildung und Forschung. (2015). Zukunftsprojekt Industrie 4.0. Retrieved from http://www.bmbf.de/de/9072.php

Bundesministerium für Ernhährung. (2010). Private Vorsorge: Notvorrat.

Bundesrepublik Deutschland. (2015). Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung - 12. BImSchV). Retrieved from http://www.gesetze-im-internet.de/bundesrecht/bimschv_12_2000/gesamt.pdf

Coombs, W. T. (2009). Conceptualising Crisis Communication. In R. L. Heath & D. O'Hair (Eds.), *Handbook of Risk and Crisis Communication* (pp. 99–118). New York.

Deutscher Bundestag. (2011). *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung*. (T. Petermann, H. Bradke, A. Lüllmann, M. Poetzsch, & U. Riehm, Eds.). Retrieved from dip21.bundestag.de/dip21/btd/17/056/1705672.pdf

Drabek, T. E. (2013). *The human side of disaster*. CRC Press.

Duscha, A. (2009). Netz- und Informationssicherheit in Unternehmen 2009. Studie des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk". Retrieved from http://www.mittelstand-

digital.de/MD/Redaktion/DE/PDF/studie-it-sicherheit-2009-pdf

Europäische Union. (2003). *Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. (2003/361/EG). Artikel 2 des Anhangs*. Retrieved from http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=uriserv:OJ.L_.2003.124.01.0036.01.DEU

European Network and Information Security Agency (ENISA). (2009). Assessing a simplified Information Security approach. Retrieved from http://www.enisa.europa.eu/publications/archive/assessing-a-simplified-information-security-approach

Herbane, B. (2010a). 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

Herbane, B. (2010b). Small business research - Time for a crisis-based view. *International Small Business Journal*, *28*(1), 43–64. doi:10.1177/0266242609350804

Herbane, B. (2013). Exploring Crisis Management in UK Small and Medium Sized Enterprises. *Journal of Contingencies and Crisis Management*, *21*(2), 82–95. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/1468-5973.12006/full

Hiete, D. M., Merz, M., & Trinks, C. (2010). *Krisenmanagement Stromausfall Kurzfassung - Krisenmanagement bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg*. (Innenministerium Baden-Würtemerg & Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Eds.). Stuttgart.

Hong, P., Huang, C., & Li, B. (2012). Crisis management for SMEs: insights from a multiple-case study. *International Journal of Business Excellence*, *5*(5), 535–553. doi:10.1504/IJBEX.2012.048802

Horváth, G. K. (2013). Information Security Management for SMEs: Implementating and Operating a Business Continuity Management System (BCMS) Using PDCA Cycle. In *Proceedings of FIKUSZ* (pp. 133–141). Budapest, Hungary.

Hunt, A. (2003). Risk and moralization in everyday life. In R. V. Ericson & A. Doyle (Eds.), *Risk and morality* (pp. 165–192). Toronto: University of Toronto Press.

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

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

Kloepfer, M. (2005). *Schutz kritischer Infrastrukturen*. Nomos.

Kunreuther, H. (2006). Disaster Mitigation and Insurance: Learning from Katrina. *The ANNALS of the American Academy of Political and Social Science*, *604*(1), 208–227. doi:10.1177/0002716205285685

Lee, W., & Jang, S. (2009). A Study on Information Security Management System Model for Small and Medium Enterprises. *Recent Advances in E-Activities, Information Security and Privacy*, 84–87.

Li, C., Coates, G., Johnson, N., & Mcguinness, M. (2015). Designing an Agent-Based Model of SMEs to Assess Flood Response Strategies and Resilience. *International Journal of Social, Education, Economics and Management Engineering*, *9*(1), 7–12.

Lorenz, D. F. (2010). Kritische Infrastrukturen aus Sicht der Bevölkerung. *Schriftenreihe Forschungsforum Öffentliche Sicherheit der FU Berlin*, *3*, 1–97.

Murphy, B. L. P. D. (2004). Emergency Management and the August 14th, 2003 Blackout. In *Institute for Catastrophic Loss Reduction* (pp. 1–9).

Musgrave, B., & Woodman, P. (2001). Weathering the storm - The 2013 Business Continuity Management Survey. *Airline Business*. doi:10.1111/j.1751-486X.2009.01490.x

National Fire Protection Association (NFPA). (2013). NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs. Retrieved from http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600

Palen, L., Hiltz, S. R., & Liu, S. B. (2007). Online forums supporting grassroots participation in emergency preparedness and response. *Communications of the ACM*, *50*(3), 54. doi:10.1145/1226736.1226766

Quarantelli, E. L. (1993). Community Crises: An Exploratory Comparison of the Characteristics and Consequences of Disasters and Riots. *Journal of Contingencies and Crisis Management*, *1*(2), 67–78. doi:10.1111/j.1468-5973.1993.tb00009.x

Reuter, C. (2014a). Communication between Power Blackout and Mobile Network Overload. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, *6*(2), 38–53.

Reuter, C. (2014b). *Emergent Collaboration Infrastructures: Technology Design for Inter-Organizational Crisis Management (Ph.D. Thesis)*. Siegen, Germany: Springer Gabler. Retrieved from http://www.springer.com/springer+gabler/bwl/wirtschaftsinformatik/book/978-3-658-08585-8

Reuter, C., & Georg, C. (2008). Entwicklung eines webbasierten Dokumentenmanagement-Systems für eine Fluggesellschaft. *Journal WIRTSCHAFTSINFORMATIK*, *50*(2), 142–145.

Reuter, C., & Ludwig, T. (2013). Anforderungen und technische Konzepte der Krisenkommunikation bei Stromausfall. In M. Hornbach (Ed.), *Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt* (pp. 1604–1618). Koblenz, Germany: GI-Edition-Lecture Notes in Informatics (LNI).

Reuter, C., Marx, A., & Pipek, V. (2012). Crisis Management 2.0: Towards a Systematization of Social Software Use in Crisis Situations. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, *4*(1), 1–16.

Sapateiro, C., Baloian, N., Antunes, P., & Zurita, G. (2011). Developing a Mobile Collaborative Tool for Business Continuity Management. *Journal of Universal Computer Science (j.ucs)*, *17*(2), 164–182.

Semantec. (2011). SMB Disaster Preparedness Survey. Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=dpsurvey

Sullivan-Taylor, B., & Branicki, L. (2011). Creating resilient SMEs: why one size might not fit all. *International Journal of Production Research*, *49*(18), 37–41. doi:10.1080/00207543.2011.563837

Thiel, C., & Thiel, C. (2010). Business Continuity Management für KMU. *Datenschutz und Datensicherheit - DuD*, *34*(6), 404–407. doi:10.1007/s11623-010-0114-3

Wedawatta, G., & Ingirige, B. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management: An International Journal*, *21*(4), 474–488.

Wedawatta, G., Ingirige, B., & Jones, K. (2010). Coping strategies against extreme weather events: a survey of SMEs in the UK. In *COBRA 2010*. RICS.

CV

Dr. Christian Reuter studied Information Systems at the University of Siegen, Germany and the École Supérieure de Commerce de Dijon, France (Dipl.-Wirt.Inf.; M.Sc.) and received a PhD for his work on (inter-)organizational collaboration technology design for crisis management (Dr. rer. pol.) with summa cum laude. He has worked as a web developer, consultant and researcher and has published more than 60 scientific articles. He is voluntary founding spokesman of the section "human computer interaction in security relevant systems" of the German Informatics Society.