International Journal of Information Systems for Crisis Response and Management
Volume 10 • Issue 1 • January-March 2018

Business Continuity Management in Micro Enterprises: Perception, Strategies, and Use of ICT

Marc-André Kaufhold, University of Siegen, Siegen, Germany
Thea Riebe, University of Siegen, Siegen, Germany
Christian Reuter, Technische Universität Darmstadt, Darmstadt, Germany
Julian Hester, University of Siegen, Siegen, Germany
Danny Jeske, University of Siegen, Siegen, Germany
Lisa Knüver, University of Siegen, Siegen, Germany
Viktoria Richert, University of Siegen, Siegen, Germany

ABSTRACT

Small and medium-sized enterprises (SMEs) represent 99% of enterprises in Germany and more than 95% in the European Union. Given the recent increase of natural disasters and man-made crises and emergencies, it seems an important economic goal to ascertain that SMEs are capable of maintaining their work, revenue and profit at an acceptable level. According to ISO 22301, business continuity management (BCM) is a holistic management process which identifies potential threats and their impact to an organization and serves as a framework to increase organizational resilience and response capabilities. Prior research identified that BCM is under-represented in SMEs and that their security level is partially in an uneconomical range. This article presents the analysis of interviews with 19 independent micro enterprises highlighting findings on their low crisis awareness, varying technical dependency, existing action strategies and communication strategies and proposing a categorization of micro enterprises as preventive technicians, data-intensive chains or pragmatic jumpers.

KEYWORDS

Action and Communication Strategies, *Business Continuity Management*, *Crisis Awareness*, *Micro Enterprises*, *Technical Dependency*

DOI: 10.4018/IJISCRAM.2018010101

1. INTRODUCTION

The safety of small and medium-sized enterprises (SMEs) is crucial for the European economy (Storey, 2016). Current reports indicate an increasing number of natural disasters, i.e. earthquakes, floods and hurricanes, as well as man-made crises and emergencies, i.e. accidents, economic sanctions, terror attacks and uprisings (Munich Re, 2016; Statista, 2017). Thus, ensuring the continuity and economic performance of SMEs during such events is a necessary issue for both practice and research. Business continuity management (BCM) is becoming increasingly important since precaution planning and response capabilities are just as vital as planning the growth and success of enterprises (Herbane, 2010). Nonetheless, research contributions indicate that SMEs are not always as protected as necessary (Reuter, 2015). According to a study by Forrester Research, approximately 45% of US and European SMEs have no business continuity concept; as a major reason for the issues of SMEs to catch up in the area of BCM, many experts argue that the corresponding standards are too complex and that their implementation is not affordable and too costly for SMEs (Thiel & Thiel, 2010). Another study of the European Network and Information Security Agency suggests that SMEs often have a poor understanding of protecting their information and a lack of resources and expertise (ENISA, 2009). As a result, SMEs cannot meet security and privacy requirements. Especially micro enterprises, defined as enterprises with less than ten employees (European Commission, 2005), therefore a subgroup of SMEs, face particular challenges in terms of business continuity and efficiency of security concepts, such as time and cost efficiency, availability of personnel and material resources, as well as adequacy and profitability of specific measures. Another problem is that only a few risk management frameworks are scalable to micro enterprises (Galan Manson et al., 2015). In addition, due to the relatively low likelihood of, for example, power outages in Western Europe, general preparation for such disasters is not optimal (Birkmann et al., 2010).

The aim of the study is to gain insight into the micro enterprises' perception, extent of impairment and measures taken during the 2013 Power Failure in Siegen (Germany) and similar incidents. Although previous research suggests that few SMEs have business continuity plans and security measures in general, little research focuses on the specific issues of micro enterprises. Thus, it seems to be important to investigate the perception and implementation of BCM measures by micro enterprises in the event of a disaster. The core study analyzes BCM regarding micro enterprises. However, since they are a subset of SMEs, the consideration of SME literature is required. This article seeks to provide exploratory and practical insights on the research questions "How do micro enterprises perceive business continuity management?" (RQ1) and "What are micro enterprises' strategies for preventing or overcoming business disruptions?" (RQ2).

The article follows with foundations and related work on SMEs, BCM and issues of SMEs implementing BCM measures (Section 2). Furthermore, a research gap is presented. Thereafter, the methodology of the empirical investigation and its exact procedure are discussed (Section 3) and the results of the case-by-case analysis, in-depth analysis as well as group comparisons and labeling are presented (Section 4). The article concludes with a summary of results, its contribution and contextualization with existing research, the study's limitations and an outlook for future research (Section 5). The results highlight the topics of crisis awareness, technical dependency, action plans and communication plans in micro enterprises, distinguishing between the types of preventive technicians, data-intensive chains and pragmatic jumpers.

2. RELATED WORK

This section provides a literature review on the characteristics and definitions of SMEs and BCM. Furthermore, the distribution of BCM in SMEs, with a special focus on micro enterprises, are discussed to motivate the research gap addressed in this article.

2.1. Definition and Scope of Small and Medium-Sized Enterprises

In the EU recommendation 2003/361, the European Commission defines SMEs according to quantitative criteria: an enterprise is one of the SMEs "[...] if it does not have more than 249 employees and has an annual turnover of not more than 50 million euros or a balance sheet total of not more than 43 million euros" (IfM Bonn, 2016). The SME definitions corresponds to the definition of the German "Institute for SME Research" (IfM Bonn), since the European Commission extends its definition of SMEs only by the balance sheet total €/year (IfM Bonn, 2005). However, IfM Bonn's higher threshold value of up to 499 employees takes into account "the specific size distribution of the German enterprise population" (IfM Bonn, 2016). Micro enterprises, which are the focus of our study, have less than 10 employees and have an annual turnover of up to 2 million euros (Table 1). In Germany, 99.6% of enterprises are SMEs, providing 60% of all jobs (BMWi, 2016) and training 81.8% of all apprentices (IfM Bonn, 2017). Since 2008, the number of SMEs has increased in Germany (Statista, 2017b), meaning that these enterprises are of particular importance for the German economy. According to the German "Federal Ministry for Economic Affairs and Energy" (BMWi), 56% of German economic output is created in SMEs, highlighting that SMEs are indispensable for growth, innovation and employment in Germany (BMWi, 2016).

The characteristics of SMEs include a high degree of flexibility, short communication channels in the enterprise, unity of ownership and leadership, flat hierarchies, commitment and involvement of employees and leadership, relatively fast decision-making and implementation of decisions, responsible involvement of the management in all relevant decisions in the enterprise, as well as spatial and temporal proximity to the customer (Haag & Roßmann, 2015; Mugler, 2008; Pfohl, 2006). However, SMEs face unique challenges and risks that include market failures in finance, innovation, research and the organizational environment (Falkner & Hiebl, 2015). In addition, structural barriers such as lack of leadership and technical knowledge, lack of knowledge about the opportunities and rigid labor markets that need to be overcome, are affecting SMEs (European Commission, 2005). Moreover, SMEs have a chronic shortage of critical resources, such as low financial resources and lack of business data. Due to traditional thinking, flexibility is also limited and there is little willingness to cooperate with other enterprises (Schmidt & Baumhauer, 2016). In contrast to SMEs, micro enterprises are often even more scarce of resources and their business decisions are strongly dependent on the entrepreneur when it comes to marketing (Nikunen et al., 2017) or IT-security management (Heidenreich, 2017). At times, micro enterprises are even excluded from SME studies (ibid.) because of their heterogeneous behavior and decision making and less standardized processes.

2.2. Definition and Scope of Business Continuity Management

According to Niemimaa (2015), literature on business continuity can be categorized roughly into the approaches of business continuity planning (BCP) and business continuity management (BCM). While BCP focuses on the planning aspect (Choudhary & Bhattacharya, 2016), BCM emphasizes social and organizational embeddedness. Thus, BCM is defined as a "holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience

Table 1. IfM Bonn's Definition of SMEs (IfM Bonn, 2016)

Enterprise size	Number of employees	Annual turnover €
micro	max. 9	max. 2 million
small	max. 49	max. 10 million
medium	max. 499	max. 50 million
SME altogether	Less than 500	max. 50 million

with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities" (ISO 22301, 2014). Most models of BCP and BCM comprise the six phases of (1) project initiation, (2) risk assessment and business impact analysis, (3) design and development of the BCP, (4) creation of the BCP, (5) testing and exercising, as well as (6) maintenance and updating (Niemimaa, 2015). BCM covers a range of disciplines including risk management, civil protection, IT emergency planning and service continuity management, facility and supply chain management, occupational safety, environmental management, knowledge management, human resources, security and public relations, as well as communications (von Rössing, 2005). Furthermore, the ISO 22301 (ISO 22301, 2014) standard outlines that business continuity promotes a resilient society, requiring inclusion of the organizational environment and society as a whole into the process of recovery. Accordingly, a study proposes, designs and evaluates an inter-organizational business continuity information network "facilitating collaboration among local, state, federal agencies and the business community for rapid disaster recovery" (Saleem et al., 2008, p. 107).

Economies, populations, states and critical infrastructures depend on reliably functioning information and communication technology (ICT) due to increasing networking and use of worldwide information channels. Therefore, it is important for all industries to extensively and explicitly address the security of their own ICT-dependent critical business processes (Eckert et al., 2013). The dependence of ICT on electric power and the increase of electronic devices and technologies in society reinforce the 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" (Reuter, 2015). Thus, domino and cascade effects can be consequences of disruptions or failures that have the potential to cause enormous economic damage and bring social sectors to a standstill (Bundesministerium des Inneren, 2009). In the event of a total ICT failure, it is estimated that about 25% of enterprises would have to declare insolvency if the damages were not remedied in a very short time (Eckert et al., 2013). Appropriate preventive measures can increase the reliability and robustness of an enterprise's business processes (BSI, 2008). Tools to maintain and increase the stability of critical business processes include early warning systems, exercise in managing risks, adaptability and fault tolerance, continuity plans and resources, and technological improvements (Schettler et al., 2003). Enterprises have increasingly recognized the relevance of BCM since business continuity primarily affects core business, i.e. value-adding processes (Tammineedi, 2010; von Rössing, 2005).

2.3. Business Continuity Management in SMEs and Micro Enterprises

Business continuity and the efficiency of security policies pose major challenges to SMEs and micro enterprises, i.e. in terms of human and material resource availability, time and cost efficiency, and the adequacy and profitability of specific measures (European Commission, 2005). In comparison to large enterprises, SMEs have a significant need to catch up regarding BCM, since this type of continuity planning is by no means common in SMEs (Thiel & Thiel, 2010). Only 43% of all SMEs have continuity plans and 70% of all SMEs have never performed an IT security analysis (Lurz et al., 2015), although most SMEs have IT equipment. Due to this underrepresentation of BCM, the security level is partly at non-economic levels, meaning that SMEs are much less protected compared to their potential risks (Reuter, 2015). Since, according to Thiel & Thiel (2010), the standards and test regulations are perceived to be too complex and the implementation to be too expensive, business continuity plans are primarily found in large enterprises. Furthermore, it is not possible for SMEs to set up a BCM team because the employees have no expertise in this area and often have double occupations of the business tasks. Although there is a variety of different frameworks, models and solutions supporting BCM in SMEs (Coates et al., 2016; Gupta et al., 2016; Horváth, 2013; Irianto, 2016; Lee & Jang, 2009; Sapateiro et al., 2011; Wedawatta & Ingirige, 2012), micro enterprises face particular challenges since they only employ up to nine people and have scarce resources such as money, time and personnel (Bergmann & Crespo, 2009), which makes it difficult to discuss, develop and implement BCM plans and systems.

2.4. Research Gap

Considering the economic relevance of SMEs in Germany and the recent increase in natural disasters as well as man-made crises and emergencies, it is important for practice and research to provide measures for overcoming these potential business disruptions and ensure continuity. Although BCM promises measures against these issues for all enterprise sizes, there is a lack of continuity plans in SMEs possibly due to the complexity and cost of BCM implementation. Although, in contrast to small and medium enterprises, micro enterprises face even bigger challenges in terms of money, time and personnel (Nikunen et al., 2017), little research has focused on their perceptions of and specific issues of implementing BCM measures and some SME studies even exclude micro enterprises (Heidenreich, 2017). In order to obtain exploratory and practical insights on the low adoption of BCM measures and existing practices in micro enterprises, our qualitative study examines the micro enterprises' perception on BCM measures, trying to identify different groups of micro enterprises (RQ1) and their strategies for preventing or overcoming business disruptions, including the collaboration with other enterprises (RQ2).

3. METHOD

The goal of the BMBF-KontiKat research group is to encourage civic societal and business continuity through socio-technical networking (physical and virtual) using cooperative technologies (Reuter et al., 2017). In this project, not catastrophes and the handling are considered centrally, but the maintenance, continuation, and recovery of social and business life independent from the cause of disruption. The superordinate research goals aim at the theory of continuity management, accurate methods of self-organization and integrated findings of civic-societal and business continuity through socio-technical networking in disaster situations. KontiKat will implement qualitative and quantitative empirical studies, such as the case study of this article, examining the continuity and level of networking of SMEs. Based on this, KontiKat will develop and evaluate concepts and technologies for addressing current problem areas, such as the BCM of SME through cooperative technologies. This section introduces the 2013 Power Failure in Siegen study case and describes from a methodological point of view the development of the interview guideline as well as the analysis and sample of the study.

3.1. The Study Case: 2013 Power and Telecommunication Failure in Siegen

On the 21st of January 2013, a fire broke out at the Deutsche Telekom exchange in Siegen that resulted in a total failure of telecommunications in Siegen and the surrounding area: more than 500,000 telephone connections did not work for several hours, and in some cases even for several days. Not only Telekom services were affected, but also services of other providers connected to the Telekom. Although the general power supply of the population was not impaired, emergency calls were not possible and the internet and the local radio in Siegen were out of service. In addition, numerous enterprises were affected by the power outage and could not carry out their daily business (Kommunale Datenzentrale Westfalen-Süd, 2013). The IHK Siegen conducted a survey on the effects of the fire, asking 1300 enterprises about the consequences. According to the sample, the consequences were serious. More than half of them suffered from a total failure of their fixed phone line that took two to three days and a failure of their mobile networks that took one day. The absence of external communication affected 88% of the enterprises surveyed, led to a lack of customer contact for 77%, postponed deliveries for 28% and even posed a threat to possible orders for 39%. Furthermore, internal processes were also impaired in 40% of the cases, for example internal accounting systems failed and cash register systems were no longer functional. Finally, 11% of the respondents even reported that they had to partially or completely close their businesses. The power failure resulted in damages in the double-digit million area (IHK Siegen, 2013). Due to the multiple possible effects on micro enterprises, as the power and the telecommunication failure, this study is not limited on any kind of business disruption.

3.2. Development of the Interview Guideline

After initial literature research, a guideline was prepared consisting of six questions. The first four questions were intended to provide insights into the micro enterprises' perception and implementation of BCM measures and what reasons are mentioned, for example, for the non-applicability of BCM (RQ1). The second part of the guideline asks for information about implemented BCM measures focusing the potential collaboration with other enterprises (RQ2). The guideline for conducting semi-structured interviews provided a framework for the data collection, but also facilitated the comparability of interview results (Bortz & Döring, 1995, p. 289), since the same questions were taken up in each interview, adopting their order and formulation to the flow of conversation (Stier, 1999, p. 188). Depending on the flow of conversation, additional questions were added to explain the facts and to gather important information. Due to this style of semi-structured conversation, the interviewees could be approached individually, including their own frame of reference. The guideline comprised the following six questions:

1. How did you, as part of your enterprise, experience the 2013 power and telecommunication failure in Siegen?
2. Did you implement security measures in your enterprise for the event of infrastructural shortcomings or interferences in the enterprise's infrastructure from outside? (Power failure, weather disaster, water pipe breakage, hacker attack, terrorist attack, etc.)
3. If your enterprise does not (or cannot) take action for some emergencies, what are the obstacles or reasons? (Budget, profitability, time, etc.)
4. Are the employees prepared or trained for emergencies?
5. Is there any form of collaboration with other (resident) enterprises, regardless of the issue of security?
6. In your opinion, what are the relevant possibilities for collaboration regarding safety-critical events?

Since research indicated that SMEs are unlikely to have established a continuous BCM process (Herbane, 2010; Thiel & Thiel, 2010), including structured business impact analyses and risk assessments, a more general terminology for the questions was used to have a broad entry point for discussion. The first question of the guideline addressed the experiences with the Telekom power failure to provide a thematic introduction and to gain the perception of micro enterprises regarding the power failure in Siegen, the extent of the impairment and any measures taken. The second and third questions specifically asked for plans and measures to investigate both the activities undertaken in the enterprise as well as the cause and reasoning for potential inactivity. Furthermore, to find out about the organizations' emergency preparedness, question four inquired about how and whether the employees are prepared internally for emergencies. The fifth question aimed at receiving information about whether employees see potential for possible collaborations with other enterprises in terms of safety-critical events. The last question asks about collaboration opportunities that employees can imagine regarding safety-critical events and which of these they consider most important. The aim was not only to get insights on virtual and technical ways of collaboration, but also about physical collaboration, for instance, with the "shop next door".

3.3. Sample and Analysis

During the period from 3rd to 9th of July 2017, a total of 19 individuals have been interviewed, each representing one independent micro enterprise in Siegen. The interviews have been done with two interviewers each, thus one interviewer could take field notes and the other ask the questions while leading the conversation. Two days later, the notes were reviewed and evaluated by both interviewers. The survey involved 19 micro enterprises that have been operating between 1 and 326 years (mean

= 30.06, standard deviation = 36.52) employing an average of 5 people (mean = 5.19, standard deviation = 3.22), with one enterprise not reporting on the number of employees. Only two enterprises are marginally above the limit with 10 and 12 employees. Since our sample was obtained through ad-hoc recruitment, our study participants consist largely of retailers, rather than secondary-sector manufacturing.

The evaluation of the data material was methodologically based on "thematic coding" according to Flick et al. (1995), which was divided into the three steps of (1) case-by-case analysis, (2) in-depth analysis and (3) case and group comparisons. The case-by-case analysis served as a brief description of each individual case (interview) and contained a typical statement for the interview, a concise presentation of the person (not relevant for this research project and therefore not included) and the topics of interest for the research subject. The in-depth analysis looked for relationships between individual statements and deductively develops a category system (Mayring, 2000). In the third step, similarities and differences between cases were identified with the goal of classification, whereby internally homogeneous and externally heterogeneous groups were formed, which are described with typical quotations (labels).

4. RESULTS OF THE EMPIRICAL STUDY

This section is segmented into the steps of case-by-case analysis, in-depth analysis and group comparisons with a final labeling. In this context, the aim of the evaluation is to consolidate the large number of qualitative data on a case-by-case basis and to identify similarities and differences across all cases, which allow interpretation in terms of the status quo and potentials of BCM in micro enterprises.

4.1. Case-By-Case Analysis

Regardless of the thematic structure of the interview guide, the key statements of the individual interviews will be shortly outlined. Considering the individual cases is useful, since the interview guideline only provided a framework for the course of the conversation and allowed the integration of individual discourse focuses. The main topics of conversation are summarized in Table 2.

First, it should be noted that the focus of the interviews was on the experience with and the management of the telecom network outage (4, 7, 8, 9, 10, 17, 19) or other emergencies (5, 16), if the enterprise was directly affected. In contrast, interviews with enterprises that had no previous experience of crises discussed adopted safety precautions and protective measures (2, 6, 13) or reasons why no action has been taken so far (1, 3, 11, 12, 14, 15, 18).

4.2. In-Depth Analysis and Category Development

In the in-depth analysis, the empirical data were evaluated based on the key questions of the interview guide. The aim of this step was to develop delimitable categories, outlining the background of actions, motivations and strategies of the interviewed micro enterprises.

Evaluation of the Key Questions

1. *How did you, as part of your enterprise, experience the 2013 power and telecommunication failure in Siegen?*

With ten micro enterprises, about half of the respondents remembered the power failure in 2013. It is noticeable that the larger subset reports stronger, far-reaching impacts on operations ("That was dramatic"; "That shows how dependent you are today"; "It was very bad in Siegen"; 4, 7, 8, 9, 10, 17, 19), while the smaller subset saw the restrictions as little relevant ("I do not need the phone, that hardly hits me"; 15, 18) or was not affected (12, 14, 16). The temporal extent of the restrictions varies from a few hours to three days. The participants reported the failure of the telephone connection

Table 2. Compression of interviews to a characteristic description (case-by-case analysis)

Case	Participant	Short description	Common statement
1	Tailoring	No incident	"That hardly hits me"
		No experience with safety-critical events; no preparations, also due to low technical dependency; but could not work without electricity; would ask the municipality	
2	Games library	No incident	"If it happens, it happens"
		Vending machines did not fail as there is an emergency generator; a responsible person for everything on-site; dealing with emergencies is regulated by a central office	
3	Hair salon	No incident	"It has not happened yet, thus you do not even think about it"
		There has never been an incident, so no preparations; incidents would be of limited duration, after half an hour everything would work again	
4	Bicycle shop	Experienced incident	"We lived from day to day"
		Experienced a shutdown lasting several days due to internet failure; strong technical dependence; would wait again in case of recurrence	
5	Bicycle shop	Experienced incident	"If the power goes down, I close the shop door or write invoices by hand"
		Major fire in Olpe led to the local branch being "on the back burner", and the branches were communicating via mobile phones	
6	Sleep systems	No incident	"A telephone failure would be bad"
		Preparation with emergency power generator and data backup in the cloud; however, no dependence on the internet, but rather on the telephone communication	
7	Insurance	Experienced incident	"Was very critical"
		One day without a phone and connection to the server of the central office; backup of all data on hard disks, so further work was possible	
8	Insurance	Experienced incident	"Had to send some employees home"
		No telephone availability for three days; reduction of workforce; data security is an obstacle to cooperation with local enterprises during incidents	
9	Pharmacy	Experienced incident	"What should we do?"
		During the power failure, no access to medicines, emergency operation at checkouts and emergency battery for computers; orders via mobile phones	
10	Bookstore	Experienced incident	"You noticed the dependence"
		During the power failure no incoming and outgoing of orders possible; due to dependence not possible to make arrangements	
11	Butcher's	No incident	"One should not always take everything too seriously and not go through life with too much fear"
		No arrangements for crises; power failure would lead to telephone coordination of refrigerated transport; logistically difficult	
12	Fashion store	No incident	"Much easier to cross over to the other shops"
		Arrangements are made especially by the caretaker; internet is hardly used; safety technology is associated with high costs	
13	Home Design	No incident	"I do not even know if you need to have something like that?"
		No precautions, but insurance against vandalism, theft, etc.; verbal communication seems completely adequate in a crisis	
14	Fashion store	No incident	"It is possible that the checkout/ phone/internet fails, but that is not that important"
		So far, no incidents; low dependence on checkout functionality, telephone and internet; good neighborhood is sufficient for crises	
15	Delicacies store	Experienced incident	"Hopefully not coming again"
		During the power failure, the phone did not work; hardly any restrictions, therefore no need for action	
16	Textiles store	Experienced incident	"The incident occurred suddenly and nothing could be saved"
		When installing pipes in front of the shop, the basement was flooded, devices were damaged; cooperation with technicians and an IT enterprise; encouraged business people to have a theme night for safety issues	
17	Estate brokerage	Experienced incident	"Runs by itself" (Note: related to possibilities of cooperation)
		During network failure without internet and telephone; daily double data backup in branch and central office; in addition, installed fire alarm system; sensitivity of employees is important	
18	Ice cream shop	No incident	"Everyone looks at his neighbor"
		Considers especially the risk of power failure, as cooling systems would be affected; costs for facilities that support emergency power are too high; in-depth local cooperation not necessary	
19	Leather goods	Experienced incident	"Office grapevine is important"
		During the power failure severely restricted, then a handwritten system (bills, etc.) was introduced for emergencies	

eight times, internet failures four times and non-functioning EC card readers three times. The impact on business continuity ranges from strong technical constraints, which resulted in employees being "sent home" (8), to failing ordering and billing systems (10, 19) and to "complete stop" of stationary and online business, what was commented by the interviewee with "We lived from day to day" (4). Insurers reduced their activity to local after-sales service (7, 8) and only one enterprise in the sample found a temporary solution in placing orders provisionally via mobile phones (9).

2. *Did you implement security measures in your enterprise for the event of infrastructural shortcomings or interference in the enterprise's infrastructure from outside? (Power failure, weather disaster, water pipe breakage, hacker attack, terrorist attack, etc.)*

Eleven enterprises responded with no ("It has not happened yet, thus you do not even think about it"; "If it happens again, we would also wait"). Cameras were mentioned as safety precautions by three micro enterprises; emergency generators, server protection, insurance, fire alarm system, and extinguishers each mentioned two times; and data cloud, local backups, firewall, emergency exit, and fire doors each mentioned once. However, due to the nature of the question, enterprises also expressed reasons for not taking precautionary measures before even asking the third question: For instance, previous incidents were too rare, making preventive measures too expensive, or the hardware/machinery was incompatible ("The old cooling systems cannot connect an emergency generator, new plants would cost too much, and they would not be as good as the old ones, so they will not be replaced"). Furthermore, other persons (boss, caretaker, technician, etc.) were considered responsible in case of emergency.

3. *If your enterprise does not (or cannot) take action for some emergencies, what are the obstacles or reasons? (Budget, profitability, time, etc.)*

Five enterprises expressed that an infrastructure failure would have no impact on day-to-day business. Furthermore, two enterprises claimed that the cost of adequate security measures is too high and that there are no safety-critical experiences so far, thus there was no perceived need for such measures. Other participants mentioned that there is only a partial influence on day-to-day business ("Anyone can overcome half an hour"), the takeover of the business by another branch, so that the responsibility for securing the building lied with the landlord, and indicated general helplessness, inexperience with opportunities of action or doubt about their effectiveness in disaster situations ("Little ones muddle through"; "One cannot take any precautions because one is dependent on others").

4. *Are the employees prepared or trained for emergencies?*

Twelve enterprises reported that their employees are not being trained in contrast to four enterprises that have already given employee training. In two enterprises, the chief was responsible for all forms of crisis management and, in one case, the enterprise was run by only one person. Some enterprises indicated the type of training, such as hygiene and informal raid training, both two times. Other participants indicated that training was not required for the staff, since backups were estimated to be sufficient for the enterprise; that the entrance door was locked every time the worker went to the bathroom, because there is only one employee at a time at the store; that in the case of "strange" or suspicious persons in the shop, employees went to positions near escape routes; and that pepper spray was bought for defense against attackers.

5. *Is there any form of collaboration with other (resident) enterprises, regardless of the is-sue of security?*

In this context, nine participants expressed that there is no collaboration at all. For the most part, enterprises did not see any added value of collaboration or only recognized a need for specific cases, such as referencing another enterprise in case of non-availability of important goods ("We only send customers to another pharmacy if we do not have the medicines"). Five of the surveyed enterprises named neighborly collaboration, primarily in the form of verbal communication by telephone or in person, and five cited business collaboration or outsourcing. Three enterprises mentioned collaborations with other branches, i.e. within the franchise or enterprise-internal structures, and one indicated a cooperation with a non-profit association.

6. *In your opinion, what are the relevant possibilities for collaboration regarding safety-critical events?*

Five enterprises express that there is no necessity of taking further collaboration opportunities, and three enterprises cannot imagine a realistic and meaningful form of collaboration ("The question is how?"; In reply to the question, if the neighbor could help: "She cannot help me either") and two enterprises would be basically interested, but saw no way to cooperate with others ("In theory, you can help others with your emergency generator, but I do not want to do it, because otherwise it has negative consequences for me and even electricity is missing and everything breaks down"). One participant said she would rather contact the municipality for help in an emergency and another one suggested to organize informative theme evenings for business people to preventively inform them about any risks and safety measures. Another idea, i.e. in case of a theft, was to make a direct call with perpetrator description for immediate publication, so that others could learn about it and would be warned. Further enterprises emphasized that they would not fear any major restrictions ("One should not always take everything too seriously and not go through life with too much fear").

Development of Categories

The deductive development of a category system revealed four main categories: crisis awareness (C1), technological dependence (C2), action strategies (C3) and communication strategies (C4). The interview data were critically examined for relations and interpreted to derive subcategories, i.e. deliberate confrontation (C1.1) and no confrontation (C1.2) for crisis awareness, and to assign the participants' statements to the subcategories. For each category, some statements served as anchors of category coding (Mayring, 2000), which are extended by further statements that are in line with the subcategory (Figure 1).

Crisis awareness: Regarding the crisis awareness of micro enterprises, the empirical data suggested a distinctness based on the confrontation with crises. In response to the Telekom power failure, a subset of the respondents showed a deliberate confrontation (C 1.1), while the other subset showed no confrontation (C 1.2). However, crisis awareness often focused on individual security-related issues, notably data security (6, 10, 16, 17), protection of business premises from fire, burglary, and damage (13, 18, 19) or cash register and ordering systems (9, 10). A comprehensive, process-oriented discussion, as formulated by the DIN standard (ISO 22301, 2014), did not take place. In contrast, among the participants who did not deal with crises, the perception dominated that crises happen rarely and pass quickly. Thus, adapting the workflow with responsibilities or additional processes was even seen as a distraction. The owner of a hairdressing salon expressed this concisely: "It has not happened yet, thus one does not even think about it" (3). When asked about the restrictions caused by the telecom power failure, one participant countered that this was the only incident so far, which hopefully will not happen again (15).

Technical dependency: "Dependence" was mentioned several times in the context of technical infrastructures (4, 8, 9, 10). A bookseller whose ordering systems did not work during the power failure stated: "It was terrifying, you noticed the dependence" (10). A pharmacist asked about security measures asked back: "What should we do?", she was dependent on external providers (9). Closer

inspection showed that the participants differed in their perceived technical dependence. Micro enterprises whose business continuity was limited during the power failure can be characterized by a high technical dependence (C 2.1) of infrastructures. Participants often named the failure of phones (4, 7, 8, 9, 17), checkout and ordering systems (9, 10, 19) and the internet (4). In contrast, many participants indicated a low technical dependency (C 2.2). These participants partly remembered the failure of the phones but consider this as "not that bad" (15, 18). The owner of a tailoring replied, "I do not need the phone, that hardly hits me" (1). A fashion store also considered the failure of the checkout system and the internet "not that important" (14). This group of participants saw a low relevance of the technical infrastructure for the business continuity. It should be noted at this point that the technical infrastructure of power supply is a special case, for which this group also recognized a large dependence. However, they faced the danger of a power failure pragmatically. "Anyone can bridge half an hour" (3), a three-day outage would be "still acceptable" (1) or variable: "If the power goes down, I close the door or write invoices by hand" (5).

Action strategies: In dealing with crises, the participants differed in their actions and attitudes. The examining of empirical data revealed the categories of active solution finding (C 3.1) and passive solution expectation (C 3.2). Some participants were actively seeking ways to manage or at least contain the crisis. In response to a power failure, two participants switched to communication (9) or product orders (7) via mobile phones and telephones after the mobile network itself became available again. In addition, some enterprises took precautionary measures to gain operational time during crises. However, measures of this kind were limited to emergency generators (2, 6, 9) and automated data backups (6, 10, 16, 17). Most participants saw themselves as having a passive role in crises, considering local institutions to be responsible. In the event of a power outage, one enterprise would "call the municipality" (1) and another enterprise would wait another half an hour since problems of this kind are usually resolved quickly (3). The inactivity was mainly motivated by the fact that, in case of a crisis, alternatives for the restoration of operability were missing (participants with large technical dependence) or that only a few crises negatively affected the business continuity at all (participants with low technical dependency). In the latter case, one participant remembered a flood in this context, but the enterprise was not affected (3). In individual cases, the responsibilities were "outsourced" to external services, such as IT security technicians and enterprises (16), caretakers (12) or corporate headquarters in chain stores (2, 17, 19).

Communication strategies: There were also differences regarding communication in crises, although the sample had a clear tendency toward less information- and solution-oriented communication, compared to action strategies. The sample includes micro enterprises that are motivated to communicate locally (C 4.1) in the event of a crisis. A fashion business store focused particularly on theft protection and was in close contact with local businesses to share information (12). Another participant mentioned in this context: "Everyone looks at their neighbors" (18). The owner of a textiles store considered personal discussions and exchanges with others on safety issues to be important and encouraged the idea of local theme evenings (16). However, it could not be determined to what degree this readiness to communicate locally can also be extended to disaster management. In addition to local communication, a motivation to internal communication (C 4.2) was recognizable. This category covers branches that in case of crisis coordinated with the head office (2, 8, 17) or other branches (5, 8). Communication with the corporate head office was usually used to obtain information about how to proceed. During the power failure, an insurance enterprise forwarded all incoming calls directly to an adjacent branch (8). However, most participants saw no benefit in cross-enterprise communication so that often no communication (C 4.3) took place at all. It is worth noting that the communication of security issues rarely took place even within enterprises. Responsibilities in a crisis were in many cases not fixed or the "boss is trying to fix everything" (7). The question of how collaboration with other enterprises can be designed meaningful was also raised (10, 13).

4.3. Group Comparisons and Labeling

The aim of the final analysis step was the identification and labeling of subgroups based on the previous categorization. The identified subgroups of preventive technicians, data-intensive chains and pragmatic jumpers, however, are not clearly defined without any overlap. In individual cases, the allocation was based on the dominating characteristics of the associated group. For example, the sample includes a preventive technician who saw his technical dependency as rather low (6) or a pragmatic jumper who was very aware of his dependency on technology (4). In the detailed case study, however, it became clear that the characterizing features were predominantly fulfilled. The empirical data suggested that most micro enterprises can be described as pragmatic jumpers, although the sample size and regional limitation of the empirical study allow only a first insight into underlying patterns.

Preventive Technicians: A first subgroup (participants: 6, 9, 10, 16, 19) is characterized by their high technical dependency (C 2.1). These enterprises recognize their dependency on technical infrastructures and are aware of the risk of failures and crises (C 1.1). Therefore, they have usually taken one or more preventive measures to ensure safety in the event of a crisis (C 3.1). Measures focus primarily on data security and emergency power. In a crisis, this group relies on improvisation with the resources available. They see little benefit in cross-enterprise networking but may be locally networked (C 4.1 and C 4.3).

Data-Intensive Chains: The second subgroup (participant: 2, 7, 8, 17) is also characterized by a high technical dependency (C 2.1) due to the interdependency of the respective enterprise with a superordinate corporate infrastructure. These are branches that exchange information with a central office and, if necessary, other branches. The information channels and responsibilities are often clearly structured within the enterprise (C 4.2). Enterprises in this group have an intensive and regulated data traffic. There is a strong awareness of the sensitivity of such infrastructures (C 1.1). These enterprises are often prepared for a crisis, especially regarding data security. In the event of an emergency, they benefit from regulated communication and fixed responsibilities, which means that solutions can be found quickly (C 3.1). However, in contrast to preventive technicians, on-site solution finding often focuses on the branch management, which coordinates actions with central offices.

Figure 1. Coding and quantification of category affiliation by participant assignment

Category	Subcategory	Participants anchors and assignment
C 1: Crisis awareness	C 1.1: Deliberate confrontation 12 participants (63 %)	Data security, business premises, checkout and ordering systems anchor[1]: 6, 9, 10, 13, 16, 17, 19 extended[2]: 2, 4, 7, 8
	C 1.2: No confrontation 7 participants (37 %)	Crises are rare and quickly over again anchor: 3, 15 extended: 1, 5, 11, 12, 14
C 2: Technical dependency	C 2.1: High technical dependency 9 participants (47 %)	Business continuity in case of failures perceived as restricted anchor: 4, 7, 8, 9, 10, 17, 19 extended: 2, 16
	C 2.2: Low technical dependency 10 participants (53 %)	Technical infrastructures are not important, hardly any restrictions anchor: 1, 3, 5, 14, 15, 18 extended: 6, 11, 12, 13
C 3: Action strategies	C 3.1: Active solution finding 10 participants (53 %)	Improvisation, reaction, prevention (emergency generator, data backup) anchor: 2, 6, 7, 9, 10, 16, 17, 19 extended: 5, 8
	C 3.2: Passive solution expectation 9 participants (47 %)	Local institutions in charge anchor: 1, 3, 12 extended: 4, 11, 13, 14, 15, 18
C 4: Communication strategies	C 4.1: Local communication 5 participants (26 %)	Local information exchange anchor: 12, 16, 18 extended: 11, 19
	C 4.2: Internal communication 4 participants (21 %)	Coordination with central office anchor: 2, 5, 8, 17 extended: -
	C 4.3: No communication 10 participants (53 %)	Lack of benefit anchor: 7, 10, 13 extended: 1, 3, 4, 6, 9, 14, 15

(1): anchor: participants whose statements define the subcategory (expressive)
(2): extended: participants whose statements are in line with the subcategory (interpretative)

Pragmatic Jumpers: The largest subgroup (participants: 1, 3, 4, 5, 11, 12, 13, 14, 15, 18) of the participants differs from the previous ones due to their low crisis awareness, having no deliberate confrontation with possible crisis scenarios (C 1.2). Therefore, this group remains reserved regarding the implementation of safety precautions (C 3.2). In the context of crises, this group mainly sees little benefit in cross-enterprise collaboration (C 4.3). In an emergency, they respond calmly and are optimistic that the crisis will soon be over. In contrast to the former groups, this one tends to be more flexible in times of crisis, if the power supply is guaranteed, as it has a rather low dependency on other technical infrastructures (C 2.2) and lacks preventive formal structures.

5. DISCUSSION

The conduction and investigation of 19 semi-structured interviews with micro enterprises in Siegen revealed differences in their crisis awareness, technical dependency, as well as implemented action and communication strategies, leading to the definition of the three subgroups of preventive technicians, data-intensive chains and pragmatic jumpers (Figure 2). In the following, we discuss our findings with regard to micro enterprises' perception of BCM (RQ1) and their strategies for overcoming business disruptions (RQ2).

"How do micro enterprises perceive business continuity management?" (RQ1): We found out that the perception and implementation of BCM in micro enterprises within our sample was influenced by their crisis awareness and technical dependency. In terms of crisis awareness, existing literature suggests that past incidents or hypothetical incident scenarios are strong drivers for the implementation of business continuity measures (Niemimaa, 2015). For a larger subset of micro enterprises, it must be stated that a crisis awareness is scarce. This group, characterized as pragmatic jumpers in the investigation, does not simply abandoned the use of management systems for BCM for economic reasons, but fundamentally doubts its necessity. Also, the preventive technicians do not see a need at all for appropriate management systems, although they highly depend on technical infrastructures and are aware of the risks. Finally, data-intensive chains are highly aware of the sensitivity of infrastructures as they can be characterized by a high technical dependency. While the businesses' increasing dependency on information systems (Orlikowski & Scott, 2008) seems to also increase the awareness of technological risks in micro enterprises, more efforts at persuasion in terms of BCM measures seem to be required for micro enterprises with low technical dependency, such as pragmatic jumpers.

Figure 2. Summary of procedure and results of the empirical investigation

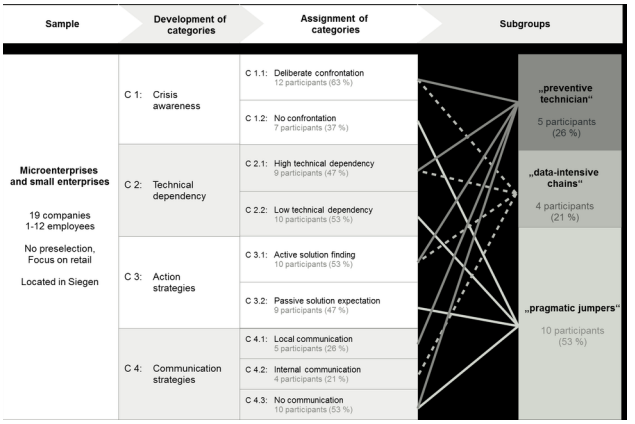

Table 3. Observed features and their manifestations in micro enterprises

Features (Categories)	Manifestations (Subcategories)
Crisis awareness	Deliberate confrontation (a, b), no confrontation (c)
Technical dependency	High technical dependency (a, b), low technical dependency (c)
Action strategies	Active solution finding (a, b), passive solution expectation (c)
Communication strategies	Local (a, c), internal (b) or no communication (a)

"What are micro enterprises' strategies for preventing or overcoming business disruptions?" (RQ2): We identified that depending on the degree to which businesses are crisis aware and technically dependent, different action and communication strategies are applied. While pragmatic jumpers react optimistically in a crisis not cooperating with other enterprises and waiting until the crisis is over, the preventive technicians prevent possible restrictions on business continuity and rely on improvisation in times of crisis. The data-intensive chains are most likely to show a process orientation through structured information channels and responsibilities, which, however, are usually limited to the branch management and, in its low complexity, are not comparable to current standards. In accordance with previous studies (Manson et al., 2015; Thiel & Thiel, 2010), standards such as ISO 22301, promoting formalized and documented processes of business impact analysis and risk assessment, are proving to be too rigid and complex for immediate applicability to micro enterprises that benefit from high flexibility, low formalization and frequent improvisation.

The results of the empirical study show that BCM does not generally take place on a process-oriented level in micro enterprises. The discrepancy between reality and the assumed importance of BCM, for example as the "core value" of an enterprise according to Estall (2012), is obviously visible in micro enterprises. This is remarkable since the standard claims to be applicable to enterprises of all sizes. Against this background, ICT support potentials and measures must be found that take into account the limited resources of micro enterprises and make targeted use of their strengths in terms of flexibility and improvisation. That, in combination with "lightweight, simple and efficient BCM as a service" (Reuter, 2015) might help micro enterprises (and SMEs) increasing their crisis awareness, understanding their technical dependencies, as well as developing more robust action and communication strategies to close the gap to formalized and documented processes, for instance, as suggested by ISO 22301.

6. CONCLUSION

The recent increase of man-made crises and natural disasters that potentially disrupt business operations motivates the need for business continuity management (BCM) in small and medium-sized enterprises (SME). However, previous research revealed a lack of continuity plans in SMEs, probably due to the complexity and cost of implementing BCM (Herbane, 2010; Thiel & Thiel, 2010). Micro enterprises face particular challenges in terms of money, time and personnel (Bergmann & Crespo, 2009; European Commission, 2005). Furthermore, the security level in SMEs is partly at non-economic levels, meaning that they are insufficiently prepared compared to their potential risks (Reuter, 2015).

The aim of the study was to gain new insights into the micro enterprises' perception of BCM and their strategies for handling business disruptions. To address our research questions, a survey was conducted with 19 independent 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 communication strategies

currently applied. Based on these factors, a categorization of micro enterprises into (a) preventive technicians, (b) data-intensive chains and (c) pragmatic jumpers was suggested (Table 3).

This study has limitations due to its exploratory character and small sample size: the relative distribution of the identified subgroups is significantly influenced by the random selection of enterprises, resulting in a large number of retailers, and the study design imposes a bias due to the regional focus. Thus, the results are only of limited significance and do not display micro enterprises in a representative way, limiting the deduction of general statements. Instead, the results can only serve as trends that need further examination. However, our results relate to the findings of Niemimaa (Niemimaa, 2015), who categorizes business continuity enablers in terms of salience, technology, models and social aspects, which correspond to our derived categories of crisis awareness, technological dependence, action plans and communication plans.

Taking the limitation of this study into account, it would be necessary to develop a more advanced classification scheme for business continuity states and enablers, trying to identify differences between micro enterprises, SMEs and large enterprises in a more systematic manner. Furthermore, a pre-clustering of enterprises in terms of branch affiliation would help to acquire a more representative sample for assessing the need of BCM across branches. Since qualitative empirical data can help to better understand specific needs, attitudes and motivations towards BCM, we plan to develop a more comprehensive qualitative study. We already interviewed six SMEs of bigger size and plan to interview further 20 enterprises using a more advanced guideline. The qualitative insights, a systematic literature review and a market survey on current BCM systems will be used to design a representative survey of German SMEs to achieve more generalizable results.

ACKNOWLEDGMENT

The research group KontiKat (Reuter et al., 2017) is funded by the German Federal Ministry of Education and Research (BMBF) (no. 13N14351).

REFERENCES

Bergmann, L., & Crespo, I. (2009). Herausforderungen kleinerer und mittlerer Unternehmen. In U. Dombrowski, T. Lacker, & S. Sonnentag (Eds.), *Modernisierung kleiner und mittlerer Unternehmen: Ein ganzheitliches Konzept* (pp. 5–30). Berlin: Springer. doi:10.1007/978-3-540-92927-7_2

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*. Berlin, Germany: Risk Management.

BMWi. (2016). *Aktionsprogramm Zukunft Mittelstand*. Berlin: BMWi.

Bortz, J., & Döring, N. (1995). *Forschungsmethoden und Evaluation für Sozialwissenschaftler (2.)*. Springer. doi:10.1007/978-3-662-07301-8

BSI. (2008). *BSI-Standard 100-4: Notfallmanagement*. Bonn: Budesanzeiger Verlag.

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

Choudhary, R., & Bhattacharya, K. (2016). Business Continuity Planning: A Study of Frameworks, Standards and Guidelines for Banks IT Services. *International Journal of Emerging Research in Management & Technology*, *5*(8), 33–40.

Coates, C., Li, C., Wright, N., & Ahlian, S. (2016). Investigating the Flood Responsiveness of Small and Medium Enterprises Using Agent-Based Modelling and Simulation. *International Journal of Safety and Security*, *6*(3), 627–635. doi:10.2495/SAFE-V6-N3-627-635

Eckert, C., Habbel, F. R., Harnisch, R., Kowalski, B., Memmert, A., & Rogall-Grothe, C. (2013). Schutz kritischer Infrastrukturen. In *Dokumentation der 12. Fachkonferenz*. In *Bürgernahe Sicherheitskommunikation für Städte und Gemeinden*. Stuttgart: Alcatel-Lucent Stiftung für Kommunikationsforschung & der Deutsche Städte- und Gemeindeverbund.

ENISA. (2009). Assessing a simplified Information Security approach. https://www.enisa.europa.eu/publications/archive/assessing-a-simplified-information-security-approach

Estall, H. (2012). *Business Continuity management systems: implementation and certification to ISO 22301*. Swindon: Chartered Institute for IT.

European Commission. (2005). The New SME Definition. *Official Journal of the European Union*, *C*(October), 1–52.

Falkner, E. M., & Hiebl, M. R. W. (2015). Risk management in SMEs: A systematic review of available evidence. *The Journal of Risk Finance*, *16*(2), 122–144. doi:10.1108/JRF-06-2014-0079

Flick, U., von Kardorff, E., Keupp, H., von Rosenstiel, L., & Wolff, S. (1995). *Handbuch Qualitative Sozialforschung: Grundlagen, Konzepte, Methoden und Anwendungen*. Beltz.

Galan Manso, C., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). Information security and privacy standards for SMEs: Recommendations to improve the adaption of information security and privacy standards in small and medium enterprises. European Network and Information Security Agency.https://www.enisa.europa.eu/publications/standardisation-for-smes

Gupta, S., Saxena, K., & Saini, A. K. (2016). Towards Risk Managed Cloud Adoption: A Conceptual Framework. In *Proceedings of the 2016 International Conference on Industrial Engineering and Operations Management*.

Haag, P., & Roßmann, P. (2015). *Management kleiner und mittlerer Unternehmen: Strategische Aspekte, operative Umsetzung und Best Practice*. Berlin: De Gruyter Oldenbourg. doi:10.1515/9783110413939

Heidenreich, M. (2017). How to design a method for measuring IT security in micro enterprises for IT security level measuring? A literature analysis. In *2017 9th International Scientific Conference on Communication and Information Technologies, KIT 2017 - Proceedings*. doi:10.23919/KIT.2017.8109447

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

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).

IfM Bonn. (2005). KMU-Definition der EU Kommission. https://www.ifm-bonn.org/definitionen/kmu-definition-der-eu-kommission/

IfM Bonn. (2016). KMU-Definition des IfM Bonn. https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/

IfM Bonn. (2017). Der Mittelstand im Überblick. https://www.ifm-bonn.org/fileadmin/data/redaktion/ueber_uns/ifm-flyer/IfM-Flyer-2017.pdf

Irianto, D. (2016). Collaborative Manufacturing for Small-Medium Enterprises. *IOP Conference Series. Materials Science and Engineering*, *114*(1), 1–6.

ISO 22301. (2014). Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen (ISO 22301:2012); Deutsche Fassung EN ISO 22301:201.

Kommunale Datenzentrale Westfalen-Süd. (2013). Telekom-Brand am 21.01.2013.

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

Lurz, H., Scheben, B., & Dolle, W. (2015). Das IT-Sicherheitsgesetz: Herausforderungen und Chancen für Unternehmen – vor allem für KMU. *Betriebs-Berater*, *46*, 2755–2762.

Mayring, P. (2000). Qualitative Inhaltsanalyse. Forum: Qualitative Sozialforschung, 1(2).

Mugler, J. (2008). *Grundlagen der BWL der Klein- und Mittelbetriebe*. Wien: Facultas.

Munich Re. (2016). *Schadenereignisse in Deutschland 1980 – 2015*. https://www.munichre.com/site/touch-naturalhazards/get/documents_E1964457554/mr/assetpool.shared/Documents/5_Touch/_NatCatService/Focus_analyses/1980-2014-Schadenereignisse-weltweit.pdf

Niemimaa, M. (2015). Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework. *Communications of the Association for Information Systems*, *27*(July), 69–102.

Nikunen, T., Saarela, M., Oikarinen, E.-L., Muhos, M., & Isohella, L. (2017). Micro-Enterprises' Digital Marketing Tools for Building Customer Relationships. *Management*, *12*(2), 171–188. doi:10.26493/1854-4231.12.171-188

Orlikowski, W. J., & Scott, S. V. (2008). 10 Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, *2*(1), 433–474. doi:10.5465/19416520802211644

Pfohl, H. C. (2006). Abgrenzung der Klein- und Mittelbetriebe von Großbetrieben. In H. C. Pfohl (Ed.), *Betriebswirtschaftslehre der Mittel- und Kleinbetriebe: Größenspezifische Probleme und Möglichkeiten zu ihrer Lösung (4. Auflage)*. Berlin: Erich Schmidt Verlag.

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

Saleem, K., Luis, S., & Deng, Y. (2008). Towards a business continuity information network for rapid disaster recovery. In *Proceedings of the 29th Annual International Digital Government Research Conference Towards* (pp. 107–116).

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

Schettler, H., Wieczorek, M., & Philipp, M. (2003). Operationale Risiken und Notfallplanung. In M. Wieczorek, U. Naujoks, & B. Bartlett (Eds.), *Business Continuity* (pp. 3–33). Berlin: Springer. doi:10.1007/978-3-642-19002-5_1

Schmidt, C., & Baumhauer, J. (2016). *Kleinunternehmen führen und organisieren: Nachhaltiger Unternehmenserfolg in Betrieben bis 15 Mitarbeitern*. Offenbach: GABAL.

IHK Siegen. (2013). Telekom-Ausfall: Millionenschäden in Unternehmen und Forderung nach Konsequenzen – IHK plant Erfahrungsaustausch.

Statista. (2017a). Number of casualties due to terrorism worldwide between 2006 and 2016. https://www.statista.com/statistics/202871/number-of-fatalities-by-terrorist-attacks-worldwide/

Statista. (2017b). Anzahl der KMU in Deutschland nach Unternehmensgröße von 2008 bis 2015. https://de.statista.com/statistik/daten/studie/732032/umfrage/kmu-in-deutschland-nach-unternehmensgroesse/

Stier, W. (1999). *Empirische Forschungsmethoden (2. Auflage)*. Springer. doi:10.1007/978-3-642-58460-2

Storey, D. (2016). *Understanding the Small Business Sector (2. Auflage)*. London: Routledge.

Tammineedi, Rama Lingeswara. (2010). Business Continuity Management: A Standards-Based Approach. *Information Security Journal: A Global Perspective, 19*(1), 36-50.

Thiel, C. & Thiel, C. (2010). Business Continuity Management für KMU. *Datenschutz Und Datensicherheit - DuD, 34*(6), 404-407.

von Rössing, R. (2005). *Betriebliches Kontinuitätsmanagement*. Bonn: mitp-Verlag.

Wedawatta, G., & Ingirige, B. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management*, *21*(4), 474–488. doi:10.1108/09653561211256170

Marc-André Kaufhold, MSc, is a researcher at the BMBF research group KontiKat at the University of Siegen. His research focuses on continuity management, crisis information systems, and authorities' and citizens' emergency response via social media.

Thea Riebe, MA, is a researcher at the BMBF research group KontiKat at the University of Siegen. Her research focuses on continuity management, security practices and technology in conflict and crisis.

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.

Julian Hester, BSc, Danny Jeske, BA, Lisa Knüver, BA, and Viktoria Richert, BA, are students of the master course "Human Computer Interaction" at the University of Siegen, Germany. Their work contributed to the examination of micro enterprises in the BMBF research group KontiKat.