Communications of the Association for Information Systems

Volume 37 Article 4

6-2015

Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework

Marko Niemimaa
Turku Centre for Computer Sciences / University of Turku, marko.niemimaa@utu.fi

Recommended Citation

Niemimaa, Marko (2015) "Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework," *Communications of the Association for Information Systems*: Vol. 37 , Article 4.
DOI: 10.17705/1CAIS.03704
Available at: https://aisel.aisnet.org/cais/vol37/iss1/4

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework

Marko Niemimaa

Department of Information Systems, Turku Centre for Computer Sciences / University of Turku, Turku School of Economics

marko.niemimaa@utu.fi

Abstract:

Hackers, malicious users, system malfunctions, and other incidents can disrupt organizational IS and cause severe organizational losses or even impact societies as a whole. In this paper, I review interdisciplinary literature on business continuity from an information systems (IS) perspective to increase understanding on how organizations can prepare for and respond to incidents. I use a narrative review approach with descriptive elements to review 83 peer-reviewed papers published between 2000-2012 across a wide array of journals and disciplines. I identify themes across the past contributions, join the currently isolated streams of literature under a concept of IS continuity, and identify research gaps in the current knowledge. The results suggest that one can understand past contributions in terms of four themes that emerged from the literature: 1) social aspects as IS continuity enabler, 2) technology as IS continuity enabler, 3) salience of IS continuity, and 4) models that improve IS continuity. To move toward an integration of the past research, and to pinpoint research gaps, I present an integrative framework. Further, the research contributes to forming an IS continuity community to facilitate cooperation and communications among scholars sharing a common interest.

Keywords: Business Continuity, Literature Review, IS Continuity, IS Security, IS Operations, Incident Preparations.

The manuscript was received 11/05/2013 and was with the authors 5 months for 2 revisions.

1 Introduction

As organizations and information systems (IS) increasingly commingle, any incident with organizational IS may cause significant organizational damage. Examples of past incidents where IS caused significant organizational damage are plentiful and vivid. Based on an international industry survey (730 validated responses) conducted in 62 countries, 40 percent of the organizations were disrupted by an incident in IS during 2012 (Business Continuity Institute, 2013).

Widely reported large-scale incidents help explain the severity and impact of incidents and the related complexity and difficulty organizations face preparing for them. For instance, in 2012, Hurricane Sandy caused significant damage to many countries. However, of interest here is the large scale damage it caused to IS. Due to heavy flooding, water flowed to data centers located on the east coast of the US, which shutdown servers hosted in the facilities and caused damage that took weeks to recover (Thibodeau, 2012). The damaged servers included the Huffington Post, BuzzFeed, and Gawker that, due to the incident, failed to provide services to their customers (Talbot, 2012a). Interestingly, as the hurricane was raging thousands of miles away, a movie theater's ticket sales in Finland came to a halt. The hurricane had caused an outage in Microsoft's cloud servers in the US and forced the company to move its U.S.-based customers to European cloud servers, which overloaded the European servers and finally halted the movie theater's electronic ticket sales system, which happened to use the cloud servers in Europe (Haapalainen, 2012). In overall, organizations that used cloud-based services (see Yang & Tate (2012) for a review of cloud based services) seemed to fare better than those relying on more traditional solutions (Talbot, 2012b).

But not only extreme weather cause such incidents. In 2011, one of the largest Nordic service providers (Tieto Co.) experienced an incident due to a problem in their data storage system, which damaged the company itself and a large number of other organizations dependent on their IS. Although the company has not disclosed the incident's exact details, the details of those affected are better documented. According to a post incident report conducted by the Swedish Civil Contingencies Agency (2011), more than 50 public and private organizations were directly affected by the incident in Tieto's IS. One of the affected organizations was an organization (or its IS) that handles electronically prescribed medicines in Sweden. Due to the incident, citizens could not obtain their medicine. While it is unclear whether the incident caused any patient injuries, hospital pharmacies and pharmacies in sparsely populated areas in particular found the incident inconvenient. The incident's impact further grew when the organization responsible for the electronically prescribed medicines also lost its public website due to the Tieto incident and could not disseminate information to pharmacies efficiently. The incident shows how an incident in one organization's IS caused damage that affected much of Swedish society (Swedish Civil Contingencies Agency, 2011).

In addition, hackers and malicious users cause incidents. Harmful and costly attacks that prevent online payments and access to websites, referred to as denial-of-service attacks, that hacktivists (i.e., hackers with ideological goals) and other malicious groups cause are numerous. One severe, high-impact attack was an attack allegedly carried out by the hackitivist group Anonymous. A denial-of-service attack cost Paypal, Visa, and Mastercard millions of pounds as their customers were unable to use their services (Daily Telegraph, 2013).

Even though the incidents' source largely differs in each case, the incidents caused severe organizational consequences. The above examples also illustrate the breadth of damage an incident may inflict and the possible costs associated to an incident. As such, it is not surprising that IT technology-related incidents are the leading causes of concerns among managers (Business Continuity Institute, 2013).

Despite the organizational significance and the central role IS managers have in preparing organizations for these types of incidents (Pitt & Goyal, 2004), "IS research provides little guidance for managers who must evaluate investments in this area, craft policies, train personnel, and adjust organizational structures to enhance business continuity" (Butler & Gray, 2006, p. 218). Past contributions are spread to multiple IS subdisciplines, such as IS security (e.g., Botha & von Solms, 2004; Stanton, 2005), IS operations (Butler & Gray, 2006), and IS strategy (Gibb & Buchanan, 2006). The research's fragmentation likely explains its absence from the mainstream management and IS literature (cf. Pearson & Clair, 1998). However, a multidisciplinary group of scholars interested in business continuity (hereafter BC) have studied ways in which organizations can prepare for incidents of all sort, including those related to IS. Research on BC has appeared in several other disciplines such as supply chain management (Norrman & Jansson, 2004;

Zsidisin, Melnyk & Ragatz, 2005), water & wastewater management (Moyer & Novick, 2012), healthcare (Iyer & Bandyopadhyay, 2000), crisis, disaster and emergency management (Lindström, Samuelsson, & Hägerfors, 2010a; McConnell & Drennan 2006), strategic management (Herbane, Elliott & Swartz, 2004) and business history (Herbane, 2010). Hence, looking beyond the boundaries of IS discipline to see how the business continuity appears in discussions of other disciplines may have a positive impact on related discussions in IS.

In this paper, I review the past literature on BC from an IS perspective to increase understanding on 'how organizations can prepare for and respond to incidents'. I see an incident here broadly as an event that is not part of an IS's standard operation and which causes or may cause an interruption to, or a reduction in, an organization's ability to continue business (adopted and adjusted from International Organization for Standardization, 2011). I acknowledge the aforementioned question is not the only question to which literature on BC has potential to contribute to. However, it is a timely question for three reasons. First, organizations' operations have increasingly become dependent on IS (Orlikowski & Scott, 2008). Second, technology's ever-increasing complexity increases the possible ways in which it can fail. Third, the interconnectedness of IS and the increase of Internet-connected systems that pervade everyday life (e.g., the "Internet of Things" (Atzori, Iera, & Morabito, 2010)) increases the possibilities for malicious attackers to cause incidents.

In this research, I identify common themes across isolated streams of literature and identify routes for future research. In other words, I structure the past to prepare for the future (Webster & Watson, 2002). I present an integrative framework to integrate the past literature and pinpoint gaps in knowledge. I use the "IS continuity" concept to denote the reviewed literature and to contribute to forming a community around the shared research concern to increase communication and collaboration among scholars.

The paper is structured as follows. In Section 2, I overview business continuity and its various definitions as background information. In Section 3, I summarize the reviewed papers and outline the methodological choices for collecting, analyzing, and structuring the literature. In Section 4, I present the analyzed literature's central contributions and, in Section 5, I discuss the findings and make suggestions for future research. In Section 6, I conclude the paper.

2 Background: Business Continuity Definitions and Uses

Before discussing IS continuity specifically, I overview business continuity (BC) by introducing various BC definitions, the similarities they share, and the breadth of research that characterizes the multidisciplinary discussions around BC. This discussion serves two more specific purposes apart from introducing BC's background: first, the definitions form a basis for the integrative framework in Section 5. Second, indicative examples of the breadth of current research on BC motivate narrowing the review to a certain part of BC literature: to IS continuity.

Although the term "business continuity" implies a tight connection to businesses, the research on business continuity studies organizations of all types. Following the paths paved by practitioners (Zsidisin et al., 2005), scholars interested in business continuity study ways to prepare for incidents of all types. Central to research on BC is accepting the underlying assumption that, even though each incident may exhibit some unique characteristics, they also share some common patterns that enable organizations to prepare for them.

Various definitions, uses of BC, and scopes of what BC covers exists (see Table 1 for explicit definitions). While the definitions are in broad sense concerned with the continuity of organizational operations, they express some significant nuances. One can categorize the definitions by the way the BC concept appears as part of the definition to three groups. The first group refers to BC as an organizational capability to resist and recover from a disruption of any kind. Asgary and Mousavi-Jahromi (2011) relate BC to an organization's capability to withstand power outage; thus, the capability can be improved with power outage mitigation technologies (e.g., uninterrupted power supply (UPS)). Similarly using the BC concept, Momani (2010) argues that "[b]y considering such (legal) requirements the organization will both follow existing requirements and improve its business continuity capability" (p. 277). In this sense, the capability is a continuum instead of a mere binary (i.e., the capability exists or does not exist). To indicate the continuum, Lindström et al. (2010a) developed a staircase maturity model for indicating the different levels of business continuity maturity.

The second group refers to BC as a means to achieve a given (organizational) end (i.e., as a model/methodology to achieve a certain goal, such as establishing a policy (e.g., Momani, 2010)). As I discuss in Section 4, much research on business continuity has focused on different approaches (e.g., models/methodologies, frameworks). As such, BC as a concept and the means to achieve a certain end have become intermingled.

The third group refers to BC as an organizational state in which an organization is under normal conditions and from which it diverges after an incident. As such, BC represents an organizational state in which an organization is able to continue operations; thus, maintaining the state becomes crucial. Moyer and Novick (2012) provide a good example of such use of the BC concept:

> *"…it is also crucial to plan for delegating special authority that may be needed to maintain business continuity while responding to an incident"* (p. 38, italics mine).

While the individual definitions seem varied, they share similarities and interrelate with one another. The first and third groups share similarities in that the BC is already an outcome of a certain processes, whereas the second group sees BC as the means to achieve those ends. The first and third groups, however, differ in their view of BC because the first group sees BC as a capability that is a continuum, whereas the third group sees it as a state that is closer to a binary. Viewing BC as a binary state does not mean that all organizations would be same in relation to BC but that organizations differ in the degree of their ability to *maintain* the state. For the first group, who see BC as a capability, the capability is then the ability to *maintain* operations/business, which is also a state.

As a subject of study, BC is multidisciplinary, which one can illustrate with some examples that present some of the BC literature's extremes: Conseil, Mounier-Jack, and Coker (2008) examine the effects of pandemic influenza on public and private organizations' BC and argue that most pandemic influenza research only focuses on public health systems; Hassanain and Al-Mudhei (2006) examine ways to minimize the effects of facilities renovations and focus on office building renovations and on organizations' capability to sustain BC; Kadam (2010) apply the BC to the individual level of analysis and contribute to literature by suggesting steps that each (private) person should take to prepare for unexpected events, such as death, injury, or severe illness.

BC originates from IT recovery but has shifted to a holistic view (as the above discussion suggests) (Herbane, 2010). Although preparing organizations for any sort of incident is significant, this wide range of topics covered under the "BC" concept has led to what Copenhaver and Lindstedt (2010) refer to as a "cacophony of voices"; that is, "an unfocused assortment of ideas, approaches and advice" (p. 165) that make up the research around BC. Although Copenhaver and Lindstedt (2010) and Lindstedt (2008) seek to create a new discipline (that of BC), I suggest an alternative way is to identify currently disjointed streams of literature and unite them to achieve more focused contributions in the future by setting up communities of interest that facilitate discussion and cooperation among those with an interest in BC.

So far, IS scholars interested in BC have contributed to a wide array of IS subdisciplines. In addition, the wider multidisciplinary community has contributed with closely related research: in the disaster management discipline, Iyer and Bandyopadhyay (2000) discuss the significance of health management information system (HMIS) on healthcare organizations' (HCO) BC, and Moyer and Novick (2012) describe their efforts of creating a supporting IS for BC in the water and wastewater management discipline. These contributions suggest there is a disjointed community of scholars who share a common concern on the part that IS has for organizations' BC. I use the term IS continuity throughout the rest of this paper to denote this stream of BC literature.

Table 1. Definitions of Business Continuity

Type of use	Author	BC definition
Organizational capability	Bajgoric (2006)	“The term ‘business continuance’ [business continuity] has been introduced in order to emphasize the ability of a business to continue with its operations even if some sort of disaster occurs.” (p. 450)
	Bajgoric & Moon (2009)	“The term, ‘business continuity’ (business continuance, business resilience) refers to the ability of a business to continue with its operations even if some sort of failure or disaster occurs.” (p. 74)
	British Standards Institution (2006)	BC is the “strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level” (p. 1).
	Castillo (2005)	“Business Continuity is the ability to retain a revenue stream through a crisis.” (p. 18)
	Herbane, Elliott, & Swartz (2004)	Authors use Sharp's (2002) definition: “business continuity is about anticipating failures and taking planned and rehearsed steps to protect the business and its stakeholders’ interests” (p. 439).
	International Organization for Standardization (2012)	BC is a “capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident” (p. 2).
Organizational means to achieve an end	Arduini & Morabito (2010)	BC is “a framework of disciplines, processes, and techniques aiming to provide continuous operation for “essential business functions” under all circumstances” (p. 122).
	Benyoucef & Forzley (2007)	Authors use Security and Privacy Research Center’s definition: “business continuity determines how a company will keep functioning until its normal facilities are restored after a disruptive event” (p. 16)
	Botha & von Solms (2004)	Authors use the definition of Rubin (1999): “It [business continuity] can be defined as the process of examining an organisation’s critical functions, identifying the possible disaster scenarios and developing procedures to address these concerns” (p. 329).
	Momani (2010)	“Business continuity is a continual improvement process that starts with establishing business continuity policy and ends with recommendations from the management review to keep business continuity plans up to date.” (p. 278)
	Rapaport & Kirschenbaum (2008)	“‘Business continuity” (BC) is not the outcome of a work organisation's coping with an emergency, but is rather a social process leading to survival.” (p. 339)
	Shaw & Harrald (2006)	BC is “the business specific plans and actions that enable an organization to respond to a crisis event in a manner such that business functions, sub-functions and processes are recovered and resumed according to a predetermined plan, prioritized by their criticality to the economic viability of the business. Business continuity includes the functions of business resumption and business (disaster) recovery.”.
	Swartz et al. (2003)	Authors use Herbane et al.'s (1997) definition: “business continuity is defined as a management process that identifies an organisation's exposure to internal and external threats, and which synthesises hard and soft assets to provide effective prevention and recovery whilst enabling competitive advantage and value system integrity” (p. 66).
An organizational state to continue operations	Speight (2011)	“Business continuity is a management process that identifies potential factors that threaten an organization and provides a framework for building resilience and the capability for an effective response.” (p. 529)
	Basel Committee on Banking Supervision (2006)	BC is “[a] state of continued, uninterrupted operation of a business”.
	Roitz & Jackson (2006)	BC is about “ensuring uninterrupted operations even after a disastrous event” (p. 7).
	Hecht (2002)	BC “is about ensuring that the critical business functions can continue” (p. 446).

3 Methodology

In this paper, I use a narrative review with some descriptive elements (King & He, 2005). King and He view narrative and descriptive reviews along a continuum of different types of approaches to analyzing past research. The narrative approaches present “verbal descriptions of past studies” that are “of great heuristic value, and serve to postulate and advance new theories and models…and direct further development in a research domain” (p. 667). The descriptive approaches:

> *introduce some quantification” and “often involves a systematic search of as many relevant papers in an investigated area, and codes each selected paper on certain characteristics, such as publication time, research methodology, main approach, grounded theory, and symbolic research outcomes (e.g., positive, negative, or non-significant) (p. 667).*

I chose the narrative approach because I sought to integrate past contributions to an IS continuity framework and direct further developments of the topic (King & He, 2005). Thus, I present the paper’s contributions (see Section 4) and the elements of the integrative framework (see Section 5) in a more elaborate fashion (in narrative-like format) than is typical for descriptive reviews. Accordingly, I illustrate the previous studies’ main themes and the related elements of the integrative framework with interesting examples instead of systematically listing all studies under each result category. Further, to present the distribution of research approaches in the IS continuity literature, to present the distribution of papers per theme, and to indicate where and when the most research efforts have been made, I include quantifications that are typical for descriptive studies.

3.1 Finding and Choosing the Papers

I found 83 academic peer-reviewed papers published across a wide range of disciplines that fitted my scope (see Appendix C for a complete list of reviewed papers). The scope included papers written in English, that were published between 2000-2012, that study BC in organizational context, and that provide contributions that cover socio-technical aspects of BC (i.e., IS continuity). I chose the 2000-2012 period because BC shifted from planning approaches to management approaches during this period (Herbane, 2010). In addition, the period length is well over the average time span in similar papers (Siponen & Willison, 2007).

More specifically, following Webster and Watson (2002), I first reviewed the two top IS journals *(i.e., MIS Quarterly and Information Systems Research).* I discovered only one paper that discusses BC (i.e., Butler & Gray, 2006) instead of just briefly mentioning the concept (e.g., Backhouse, Hsu, & Silva, 2006; Gordon, Loeb, & Sohail, 2010; Smith, Winchester, Bunker, & Jamieson, 2010). Next, I searched for peer-reviewed papers using the term “business continuity” in well-known search engines (Google Scholar, ACM Digital Library, ProQuest, AIS Digital Library, and EBSCO). After uncovering the first set of the literature, I used the snowballing technique to uncover rest of the papers (Webster & Watson, 2002). As such, I was able to collect a comprehensive selection of interdisciplinary academic literature on BC.

To narrow the uncovered literature to fit my scope, I reviewed all potential papers at the topic level to determine whether they covered BC in an organizational context, after which I analyzed their abstracts. I included all papers on organizational BC published in IS outlets. I read and analyzed other potentially suitable papers to identify whether they covered the topic from an IS perspective. I give IS here a wide interpretation. Rather than viewing IS as synonymous for IT artifact, I use IS in a socio-technical sense to cover both social aspects (e.g., attitudes, skills, values, the relationships between people and authority structures) and technical aspects (processes, tasks, and technology) and their correlative interactions (cf. Bostrom & Heinen, 1977). This interpretation would likely fail to meet the expectations of those who advocate (returning to) an IT artifact-centered view on IS (e.g., Benbasat & Zmud, 2003) but is likely to resonate for those advocating a wider interdisciplinary view on IS (e.g., Galliers, 2003; Desanctis, 2003) and work system view (Alter, 2003). Therefore, IS continuity represents the part of the business continuity literature that is concerned with the continuity (i.e., preparing for and responding to) of a socio-technical assemblage (i.e., the IS).

I could discard some papers easily; some I could not do so easily. For example, I deemed Conseil et al. (2008) and Hassanain and Al-Mudhei (2006) to not cover IS continuity. When there was uncertainty, I further discussed the paper in question with another scholar to verify whether it reflected her understanding of an IS contribution. When there was disagreement or uncertainty, I included than excluded the paper. The resulting collection of papers forms the basis for IS continuity.

Figure 1 illustrates the distribution of papers per year[1] and the number of papers published across disciplines (see Appendix A for a full list of journals and categorization of journals to disciplines).

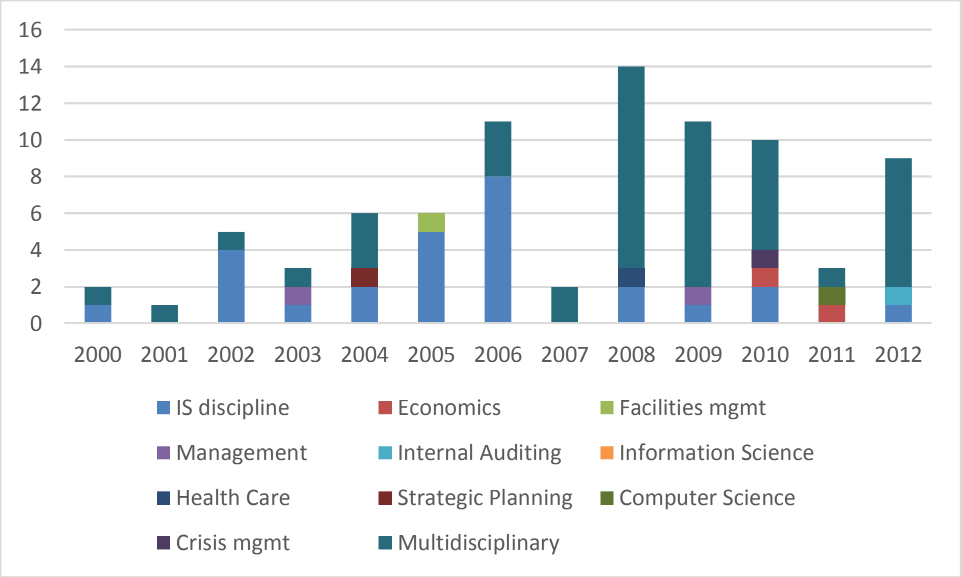

Figure 1: Distribution of IS Continuity Papers Per Year

3.2 Analyzing and Categorizing the Literature

To thematize the papers, I classified the contributions into themes to identify the most common themes across contributions, which I did by avoiding predefined categories. Instead, the themes emerged from the papers themselves (Bacon & Fitzgerald, 2001). Allowing the themes to emerge was necessary because no predefined categories existed due to the topic's multidisciplinary nature. Instead, the themes resulted from an iterative literature analysis in the spirit of hermeneutic analysis (Myers, 2004; Boell & Cecez-Kecmanovic 2014).

The fundamental tenet of hermeneutic analysis is that correct understanding emerges from the interplay between the parts and the whole (Klein & Myers, 1999). The "whole" refers here to the understanding that one gains through reading and analyzing the papers; that is, the "parts". The interdisciplinary focus of the research further supported using hermeneutics because "(i)nterdisciplinary integration brings interdependent parts of knowledge into harmonious relationships through strategies such as relating part and whole or the particular and the general" (Stember, 1991, p. 4). To understand the whole, I read each paper through and wrote notes down about it. Subsequently, I coded each paper by using qualitative coding techniques (Miles & Huberman, 1994). The notes included emerging categories and other notes that I felt were important for the research (e.g., interesting findings, representative papers for each category). For example, the codes included "methodologies", "frameworks", "lifecycle" that, I assimilated after several iterations of hermeneutic interpretation and qualitative coding into a single category. Section 4 presents the emerged categories, their definitions, and their respective content.

Before moving to discuss the results of the review in more detail, I note other research that has embarked to review some aspects of BC literature that I uncovered during the review process. Herbane (2010) provides a detailed trajectory of BC by following its development from the 70s' "disaster-recovery" approaches to developing an approach coined as business continuity management (BCM). Adkins, Thornton, and Blake (2009) conducted a content analysis on business continuity planning literature: they collected 2500 publications (academic, trade publications, media articles, and government/legal publications) published between 1997-2007. They used random sampling to choose 75 papers from each

[1] Interestingly, the quantity of published research between 2008-2010 is equal with the quantity of published research during the rest of the analyzed period. In a yearly survey of key issues for IT executives, BC was ranked relatively highly (ranks 3,6,4) between the same period (Luftman & Ben-Zvi, 2010). The authors suggest that "[t]he likely reason for its [BCs] high ranking during the recession is the inherent risks due to the reduced investment during the recession" (p. 10). The popularity of the topic among IT executives might also explain the high number of research during the 2008-2010. Unfortunately, no comparison data was available for the rest of the review period (2011-2012) that could be used to correlate whether current recession has had similar effects on BC popularity among IT executives. However, at least the number of published studies seems to be lower than during the earlier recession.

category (N = 300), after which they used random sampling to select 28 papers for intercoder reliability. Their findings suggest business continuity planning is mostly used for natural disasters, electronic disasters, and terrorism/warfare events. Unfortunately, the authors do not disclose the categories' details, so it is only possible to speculate whether they categorized all the IT- and technology-related publications as "electronic disasters".

4 Results

In Section 3, I describe the review process I used to uncover, analyze, and classify the IS continuity literature. In this chapter, I present the results of the review process. First, I discuss the reviewed papers' research approaches and their theoretical basis. These two parts provide a more generic view on methodologies and theoretical orientations that IS continuity scholars have found particularly fruitful. Last, I discuss the thematized IS continuity contributions in detail.

4.1 IS Continuity Research Approaches

To assess and categorize the research approaches used in the IS continuity literature, I used the following categorization scheme:

- Cases: research that studies single or several sites over a period of time to provide a detailed and particular account of some interesting organizational change or development process.
- Conceptual: research that is argumentative and makes no or little reference to empirical data to back up its arguments.
- Experiment: research that studies one or more controlled groups. The studies may take place in a laboratory or in a real-world setting.
- Interview: research that collects data only through any type of qualitative interviews.
- Survey: research that collects data through questionnaires.

I adopted the above categorization scheme from Chen and Hirscheim (2004) and adjusted it. Chen and Hirscheim categorize research approaches to six categories: 1) survey, 2) case study, 3) laboratory experiment, 4) field experiment, 5) action research, and 6) others. The adjustments were necessary due to the nature of IS continuity literature. The categorization I used does not distinguish between laboratory and field experiments due to the low number of experiment studies (only one field experiment; i.e., van de Walle & Rutkowski (2006)). The case studies, in addition to academic case studies (cf. Yin, 2003), include practitioner-oriented case studies that Orlikowski and Baroudi (1991) call descriptive work: ”the researchers attempted no theoretical grounding or interpretation of the phenomena; rather, they presented what they believed to be straightforward 'objective', 'factual', accounts of events to illustrate some issue of interest to the information systems community" (p. 5) (see Thornton, 2008, for example). Further, I categorized conceptual studies that make no or little references to empirical material as conceptual instead of "other" as Chen and Hirscheim (2004) categorize them. Lastly, I added studies that relied purely on qualitative interviews as a separate research approach (interview) because they did not fit to any of Chen and Hircscheim's (2004) categories. Where possible, I categorized the papers in line with their authors own assessment of their research approach.

Because many papers omit explicit discussion on the adopted research approach, I had to infer their approaches. My analysis suggests that the most popular research approach IS continuity studies have adopted is conceptual that makes no or little references to empirical data. Appendix B provides the details of the analysis. Further, because most papers do not discuss data collection and analysis, I do not discuss these aspects here.

4.2 IS Continuity Use of Theories

Theory use in IS continuity can be mostly characterized as "loose" (Walsham, 2006) or even as "no theory" (Siponen & Willison, 2007). Exceptions are Butler and Gray (2006), who draw on mindfulness; Van de Walle and Rutkowski (2006), who draw on fuzzy set theory; Pheng, Ying, and Kumaraswamy (2010), who draw on rational choice theory, normative theory, and cultural-cognitive theory; and Lindström, Harnesk, Laaksonen, and Niemimaa (2010b), who draw on soft-systems methodology (SSM). Other studies review the prior literature on business continuity to define conceptual relations. The extent of connection to past literature varies across the papers. Indeed, the business continuity niche journal's *(i.e.,* *Journal of Business Continuity & Emergency Planning)* policy explicitly states that papers"need not display in-depth knowledge of previous academic work in the field" (Henry Stewart Publications, 2013). Clearly, there is no common core theory or set of core theories in IS continuity.

4.3 IS Continuity Contributions

The literature on IS continuity broadly deals with ways to improve the continuity of organizational IS. I discuss the four themes that emerged from the data for rest of the paper: 1) social aspects as IS continuity enabler, 2) technology as IS continuity enabler, 3) salience of IS continuity, and 4) models that improve IS continuity.

I categorized each paper to a single theme. While some papers fit unambiguously under a certain theme, some are more ambiguous to categorize. For instance, Rapaport and Kirschembaum (2008) clearly emphasize that social processes lead to BC, and Bajgoric (2006, 2010) clearly emphasize that technology enables BC. Thus, they exemplify the first two emerged themes, respectively. However, those categorized as models (theme 4) include studies that advocate certain steps that organizations should take, which might include both social and technological aspects. More specifically, these steps included choosing a suitable technology to mitigate continuity problems or arranging training for personnel to prepare them to act in a preplanned manner during an incident. As such, the models would connect with the two categories of social and technology, but, in lieu of extensively discussing either aspect, the discussion is held at a superficial level and as a single part of a larger set of steps. Lastly, while each of the reviewed papers discuss the salience (e.g., why the continuity practices are important and why organizations should engage with those practices) of their study topic, the papers in theme 3 ("salience of IS continuity") mainly emphasize the importance of organizational continuity preparations. These interrelations and interdependencies suggest possibilities exist for integrating the themes.

In lieu of exhaustively listing every paper and their respective contribution, I discuss certain papers' contributions that illustrate the themes in line with the paper's narrative approach. As such, I focus on describing the themes rather than on describing individual papers (Webster & Watson, 2002).

4.3.1 Social Aspects as IS Continuity Enabler (11 Papers, 13.3%)

Despite advancements in the literature emphasizing BC's socio-technical nature (Herbane et al., 2004), according to Smith (2003), social aspects have been under represented in the literature. Even though technologies have a central role in contemporary organizations (Orlikowski & Scott, 2008), "it is people who actually deal with business continuity and crisis" (Smith, 2003, p. 28). Past research suggests that the social aspects influence incident preparations at the individual and collective levels but also that response for an incident is contingent on social aspects. In this section, I elaborate on the individual-level social aspects and the collective-level social aspects. I then discuss the contingencies between social aspects and incident response.

Influencing the central organizational actors is viewed crucial for IS continuity. Top management that is reluctant and disinterested about IS continuity may significantly impede preparations (Seow, 2009). As such, scholars have repeatedly emphasized the importance of organizational leaders' commitment to BC (e.g., Gibb & Buchanan, 2006; Kite & Zucca, 2007; Lindström et al., 2010a; Seow, 2009; Stanton, 2005). Inducing fear on the executives by describing the consequences of not adequately preparing may act as motivator. Indicating sanctions that result from non-compliance to regulatory (continuity) requirements, showing management ignorance to good management practices, indicating gaps to competitors' practices, showing lost customer opportunities, and appealing to executives personal motivators (and fears) may all motivate executives to sponsor IS continuity projects (Seow, 2009).

Preparing for incidents requires that many organizational roles participate in the implementation project (Kendall, Kendall, & Lee, 2005). Walch and Merante (2008) examine the appropriate staff size to manage continuity projects and explain how to calculate it. They conclude that organizations should consider their industry, their number of critical systems and applications, the complexity of their IT infrastructure, and the quantity of their data centers and their geographical locations when deciding the staffing. However, past studies suggest that not only the quantity of the social actors but also their individual-level qualitative differences affect how well an organization is prepared for an incident. The social traits and skills of the person responsible for managing the IS continuity implementation have been found central for success (i.e., Shaw & Harrald, 2006; Wong, 2009). Wong (2009), building on his own experiences as practitioner, identifies the strategic skills IS continuity managers need. He emphasizes the importance for proactive leadership that “enables organisations to anticipate the threats to corporate objectives and competitiveness, and develop responses in relation to the long-term implications of a crisis” (p. 67).

In addition to the individual, studies also emphasize the collective social aspects’ importance. The prevailing (collective) culture of the social setting in which the preparations to an incident are embedded influences an organization’s preparations. King (2003) sees that a “correct” collective continuity-aware culture ensures that continuity plans and guidelines are maintained Thus, an organization that has a continuity-aware culture acts in a “correct” and BC-aware way, whereas an organization without such a culture “buries its head in the sand” (McConnell & Drennan, 2006, p. 69). Thus, collective behavior becomes inscribed in the culture in such a way that actions that support organization’s preparedness for incidents follows; in other words, culture is an enabler. However, Sawalha and Anchor (2012) and Sawalha and Meaton (2012) view culture differently: that is, as an inhibitor. The authors argue that societal culture can significantly inhibit whether an organization adopts organizational BC. Further, past research on collective social aspects suggests an organization’s social conditions fostered during “normal” times not only influence its preparations but are projected into the moment of incidents. Butler and Gray (2006) argue that organizations should foster conditions of collective mindfulness in lieu of focusing on detailed plans and guidelines. Thus, collective mindfulness implies a change from implementing detailed plans and guidelines that should govern employees' response actions during an incident (i.e., mindless response) to preparing high-level instructions for responding and focusing on enhancing organization's overall ability to perceive early cues of incidents, interpret them, and respond appropriately (i.e., collective mindfulness) (Butler & Gray, 2006). Lastly, Rapaport and Kirschenbaum (2008) argue that “Business Continuity (BC) is not the outcome of a work organisation's coping with an emergency, but is rather a social process leading to survival” (p. 339). They suggest that an organization’s ability to respond to an incident lies in the social process influenced by such social aspects as social ties and social networks that influence employees’ adaptability to incidents and positively contribute to organizational survival.

4.3.2 Technology as IS Continuity Enabler (16 Papers, 19.3%)

Reflecting the roots of business continuity, many organizations still perceive continuity as a technical issue (Cerullo & Cerullo, 2004). However, past research suggests that technology, in respect to continuity, has a dual role. First, technologies themselves are to reduce or remove incidents altogether. From this view, technologies themselves are the preparations for incidents. Second, technologies are to enhance or enable preparations and responses to an incident. From this view, technology mediates and enhances preparations and responses to an incident. I elaborate on both of these views in this section.

Some scholars have viewed improving organizational technology through more-advanced technological solutions as a way to prepare for incidents. Bajgoric (2006) argues that “information technologies (IT) have been recognized as business continuity enablers” (p. 451). Hence, Bajgoric (2006) argues that, to enable business continuity, organizations should invest in continuous computing infrastructure. Continuous computing infrastructure builds on “always-on” computing that uses several technological advancements, such as on 64-bit computer architecture instead of 32-bit architecture (Bajgoric, 2006). In a similar manner, Ceballos, DiPasquale, and Feldman (2012) suggest organizations should use advanced networking technology called dense wave division multiplexing (DWDM) to help them ‘address current datacenter challenges specific to business continuity and security in light of the potential for equipment failure, fiber cuts, floods, fire, or massive power grid blackouts, as well as denial of service and terrorist attacks’ (p. 147). However, organizations cannot focus on IT without accounting for technology’s dependency on other resources. Asgary and Mousavi-Jahromi (2011) found, based on a survey (n = 482) conducted in the Greater Toronto Area in Canada, that power outages are a major threat for organizations, and especially for those dependent on IT. Even though their results show that many respondents had not implemented measures to mitigate power outages, organizations are willing to pay for mitigation efforts, but they prefer options that are less costly, environmentally friendly, and take little (physical) space. Power supply technology called uninterrupted power supply (UPS) may help organizations to prepare for and mitigate the impact of power outages (Asgary & Mousavi-Jahromi, 2011). Thus, using (advanced/additional) technology may serve as an effective way to prepare for and avert certain incidents altogether.

Past research suggests technology may also support preparation. To support business continuity planners to make preparations, van de Walle and Rutkowski (2006) developed a decision support system with which planners can individually assess the likelihood and impact of incidents and compare their assessment to those made by other organizational continuity planners. Based on a field experiment, the authors conclude that the planners they studied were more satisfied with the decision process and showed more agreement with the group decision when they used the decision support system than when they did not. In addition, their data shows that the planners' assessments were less extreme than without the system's aid. Husband (2007) describes an IT system that John Lewis Partnership developed to consolidate 200 separate business continuity plans into a single system which supported the preparation process by ensuring information stored in the system was accurate and up-to-date. In addition, other studies exist that highlight the supportive role IT plays in preparation. However, these studies depict the development of the IT as a straightforward and do not pay attention to the details of the implementation/adoption and/or mention the IT as part of other steps the organizations took to prepare for incidents: Alesi (2008) describes the use of a Web-based intranet solution at Lehman Brothers "to create customised incident response and planning tools that connect in real-time to authoritative, up-to-date sources of data, using the same look and feel familiar to users" (p. 218); Thornton (2008) the use of IT "that provides a consistent and rapid risk assessment capability" (p. 51) at the Australian Customs Service and Australian Quarantine and Inspection Service; and Moyer and Novick (2012) the use of an IT "toolbox" ("a detailed guidance document that supports a utility seeking to develop a BCP [business Continuity Plan], a word processing template, and a series of online training modules for additional guidance in working through each BCP development step" (p. 38)) to help managers plan for water and wastewater system business continuity. As such, technologies are effective in mediating and enhancing organizational preparations for incidents.

Lastly, past research suggest that technologies are not only effective in preparing for incidents, but also significant in responding to incidents. Heng, Hooi, Liang, Othma, and San (2012) and Roitz and Jackson (2006) describe two different but interrelated cases in which an IT-enabled telecommuting work contributed to BC. Heng et al. (2012) designed and implemented a telecommuting system and evaluated (post implementation) the system's influence on organizations' preparedness for incidents. Based on the results, 64.1 percent of the informants strongly agreed that the telecommuting positively affected the organizational preparedness. Roitz and Jackson (2006) describe telecommuting at AT&T and argue that telecommuting is an important contribution to BC. AT&T's IT-based telecommuting enabled the company's employees to access its IT systems and enabled the formation of virtual teams during hurricane Katrina while the normal office premises were unreachable. While these improvements on organizational incident response are positive side effects of telecommuting, Sapateiro, Baloian, Antunes, and Zurita (2011) developed an IT system, a mobile collaboration platform, solely to enhance incident response. They designed the system to increase a team's "capability to assess, make decisions and act upon disruptive situations through better communication, data sharing and coordination' (p. 166). Still, even though scholars have embarked to find technologies that support the response, in general, "further research should be conducted to validate the tool(s) during actual disruptive situations" (Sapateiro et al., 2011, p. 179).

4.3.3 Salience of IS Continuity (18 Papers, 21.7%)

"Without business continuity and crisis management, lives are lost" (Power & Forte, 2006, p.17). Although this quotation represents one of the extremes, some reviewed papers focus on emphasizing the salience of business continuity practices for organizations. Prior studies have found that previous incidents, especially those that have had a high impact, and hypothetical incident scenarios can be powerful ways to communicate the BC's importance to other scholars and practitioners. These studies are significant for IS continuity for two reasons. First, they emphasize preparation's importance and complacency's likely/possible consequences. Second, they illustrate the type of harmful events organizations in the past have been able to avert through the a priori preparations and effective response. Although past incidents are likely a bad mirror of the future, they can support the assumption that preparations pay off even if all possible future scenarios cannot be predicted or extrapolated based on the past events. As such, drawing attention to the importance of preparation through examples of disastrous events that have already unfolded or to those that may unfold in the future, the studies serve an important role in motivating other organizations to start making preparations or to improve existing ones.

September 11 in 2001 (i.e., "9/11") represents one of the large-scale, catastrophic events that put significant demands on organizations' incident preparations (or lack thereof). According to Berman (2002), those organizations that had done a priori preparations "fared far, far, far better than those who did not" (p. 30). Although, the event had catastrophic effects on all parts of organizational life for those affected, what is of interest here is the impact on organizational technology. Recovering organizational technology resources after the incident took much longer than most organizations had anticipated (Berman, 2002).

Organizations had to find ways to do business without IT. Many technologies, whether advanced or less advanced, had failed and required alternative ways of working and alternative IT to keep the business running. The organizations' IT that supported business processes had to be mapped to alternative manual procedures until the IT had been replaced (Berman, 2002). Alonso (2001) argue much of the preparations organizations had in place to mitigate an event such as 9/11 could be traced to past incidents. According to him, organizations had already learned from the 1993 World Trade Center Bombing and from Y2K problem; as such, they avoided significant data loss from 9/11. Thus, his arguments suggest that the preparations organizations made in the past helped to mitigate impact of an adverse event that greatly differed from the previous events.

Whereas 9/11 is an example of a high-impact incident, Ernest-Jones (2005) argues that organizations should not only focus on grand-scale incidents and contemplate on the idea that preparations for grand-scale incidents would help them to also cover smaller incidents. Indeed, Ernest-Jones (2005) quotes Ernest & Young's specialist who argues that "it's the middle ground that causes most problems. That's where the least successful enactment of (BC) plans usually is" (p. 8).

Further, past incidents may also serve to prepare organizations for different types of incidents that at first seem unrelated but that share some common aspects. In IS security, Hinde (2005) discusses how Lea & Perrins, a company that produces Worcestershire sauce, experienced severe reputational damage that was caused by their competitor's product recall as illegal dye had gone into the competitor's product that also happened to be a Worcestershire sauce. While Lea & Perrins had not used the illegal dye, "[f]or most consumers Worcester sauce is Lea & Perrins...[s]o any scare story about contaminated Worcester sauce automatically implicated Lea & Perrins in many consumer's minds" (Hinde, 2005, p. 19). Using the product recall as an example of an incident with cascading effects, Hinde (2005) argues for the importance of IS continuity practices, even for preparing for technological incidents. Through continuity practices, organizations should realize and account for the wider context in which they reside; "to assume that you can look at the risks facing the computer center in isolation from the neighboring environment is risky to the point of foolhardiness" (p. 18). In addition, Stanton (2005) suggests incidents in IT are different from other incidents in the nature of impact and risk and are, therefore, changing how organizations should view BC. He argues it takes less than 60 seconds to ruin a company's reputation or to cripple its business in the "digital networked economy". Unfortunately, it is unclear how precisely the digital networked economy differs from other types of environments in this respect.

Lastly, Herbane et al. (2004) studied six U.K.-based financial firms and found initial evidence that organizations can derive strategic value from the capability to continue operations in the event of incident and from the capability to restore from an incident quicker than competitors. As such, their results suggests that it makes sense businesswise to enhance organizations BC—both by making preparations and improving response for incidents.

4.3.4 Models That Improve IS Continuity (38 Papers, 45.8%)

The most common contributions from scholars interested in IS continuity have been various models through which organizations improve IS continuity. As discussed earlier, the BC concept and the models, as means to achieve BC, have become so intermingled that they have become nearly synonymous. Scholars have brought forward models/frameworks that can be categorized roughly into two approaches: 1) business continuity planning (BCP) and 2) business continuity management (BCM). As the name implies, BCP is a planning approach, whereas BCM[2] is a:

> *holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which 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. (International Organization for Standardization, 2012, p. 2)*

Most of the BCP models comprise six phases (Pitt & Goyal, 2004, p. 88; see also Turetken, 2008, p. 376, for similar categorization): 1) project initiation, 2) risk assessment/business impact analysis, 3) design and development of the BCP, 4) creation of the BCP, 5) testing and exercising (ranging from document reviews to realistic exercises (Gibb & Buchanan, 2006)), 6) maintenance and updating (I ask readers to

[2] Although the definition is from British Standard 25999. The definition is widely accepted and used among scholars and practitioners (see, e.g., Bajgoric, 2006; Herbane, 2010; Sawalha & Meaton, 2012).

view the details of each step from the original research papers). Where the risk assessment phase often follows normal risk management practices (Gibb & Buchanan, 2006), the business impact analysis (BIA), used to calculate business impact of unavailability of resources (Messer, 2009), is more BCP specific. The calculation can be divided into two types of measures: 1) recovery time objective (RTO) and 2) recovery point objective (RPO). RTO is the "the desired amount of time it takes to recover", whereas RPO is "the distance in time between the last restoration point (the last full backup typically) to the current point in time" (Cervone, 2006, p. 176). The BCP phases are transitive and should be followed in consecutive order. According to Cerullo and Cerullo (2004), through these phases, three interdependent objectives should be realized: 1) "identifying major risks of business interruption', 2) "develop a plan to mitigate or reduce the impact of identified risks", and 3) "train employees and test the plan to ensure that it is effective" (p. 71). Further, despite that the abstracted phases of BCP are universal, "every organization needs to develop a comprehensive BCP based on its unique situation" (Cerullo & Cerullo, 2004, p. 71).

Botha and von Solms (2004), based on "a study of various existing methodologies and each one's strong and weak points", developed "a seven-phase BCP methodology" (p. 331). Their suggested methodology has four "sub-lifecycles": 1) the backup cycle, 2) the disaster-recovery cycle, 3) the contingency planning cycle, and (4) the continuity planning cycle. Their methodology differs from the above six-step model in that, through the sub-lifecycles, small and medium-sized organizations can adopt and adjust the methodology to their needs and resources. For instance, with resource constraints, their methodology recommends small organizations to focus merely on the backup cycle and to leave the creation of plans to larger organizations with more resources. Thus, the methodology is customizable to fit even the smallest organizations, and it recognizes differences in the needs of different organizations, something that has not been explicitly addressed in most of the other life cycles.

BCM models extend the BCP models and, thus, represent the next generation in the continuity approaches' evolution (Herbane et al., 2004). Although most BCM models also incorporate a part that focuses on planning (Gibb & Buchanan, 2006), BCM emphasizes embeddedness; that is, "BCM is then not merely 'a plan' but constitutes the organisational processes of leadership, commitment to which may be seen operating at individual and group levels" (Herbane et al., 2004, p. 442). BIA can have important role in moving an organization toward embeddedness. As Messer (2009) argues, BIA can be used as a tool to leverage enterprise-level group thinking, which results in viewing BC as part the of the business-as-usual; that is, as embedded. Further, Selden and Perks (2007) argue that a structured BIA may align BC with organizations strategic goals. Thus, the BCM extends the BCP approaches by drawing attention not only to the steps for creating plans, but also to changing social and organizational aspects. Even though the models depict a linear process (see Smith, 2003; Strong, 2010; Gibb & Buchanan, 2006; Tammineedi, 2010), empirical findings suggest the process is "messy, probably two-directional and incremental" (Herbane et al., 2004, p. 77).

Scholars have also focused on some specific aspect of the IS continuity and provided models for those tasks. Kendall et al. (2005) extend continuity models and use a theatre metaphor to illuminate and deepen understanding of the importance of exercises and evaluation; Nosworthy (2000) provides a model for assessing the risks IS continuity should account for; Turetken (2008) provides a multi-criteria model for choosing the most appropriate location for a backup IT infrastructure; Freestone and Lee (2008) provide a model to "survive" a BCM audit by illuminating the process that auditors take when assessing organizational BCM; McLoughlin (2009), building on an international BCM standard, the International Organization for Standardization's (2013) ISO 22301 standard, provides steps to preparing organization's BCM that are in accordance with the standard; Tammineedi (2010) elaborates the steps and requirements of the same ISO 22301 standard; Wan (2009) develops a framework for integrating BC plans and IT service management and argues that "the continuity plan needs to be integrated with ITSM (IT Service Management) if an organisation is going to be able to manage fault realisation and return to normal business operations" (p. 41); and Lindström et al. (2010b) provide a model for learning from past incidents based on systems thinking.

As the above discussion on BCP and BCM suggests, the focus in the past research on models has been on guiding organizations on making preparations for incidents rather than guiding the actual response that organizations take after an incident.

To summarize, the discussion on the contributions of past research point to some disunity and disagreement among scholars on the ways in which organizations should prepare and respond to incidents. While using IT is recognized as being indispensable for contemporary organizations in preparing for and responding to incidents (see Section 4.3.2), technology alone likely does not suffice for cases when the technology fails. Further, scholars have questioned whether planning approaches (see Section 4.3.4) that assume "likely future scenarios can be probabilistically anticipated and that individuals can understand, or at least imagine, their potential impact" (Butler & Gray, 2006, p. 218) are feasible and suggest focusing fostering social aspects that promote adaptability (see Section 4.3.1). However, scholars such as Stucke, Straubm, and Sainsbury (2008) argue that "adaptability is certainly indispensable in a crisis, but that, overall and primarily, organizations should depend on their well-tested plans for recovery and not on ingenuity" (p. 160) (see Section 4.3.4). Halliwell (2008) differs from the binary opposition between plans and social ingenuity and suggests a response is contingent on the incident and that these contingencies require not only different approaches in responding but also in preparing (i.e., that, for some incidents, there is a need to prepare plans, while others can rest on social ingenuity). Interestingly, Berman (2002), even though clearly emphasizing plans' importance, describes how organizations successfully responded to 1993 World Trade Center bombings without pre-made plans with mere social ingenuity. According to him, the success meant organizations became confident they were sufficiently prepared to respond to future incidents as well, only to be proved wrong by 9/11 (see Section 4.3.3). However, rather than accounting for the qualitative differences (and similarities) between the two incidents, he argues, the environmental circumstances during the incidents, such as the weekday of the incident, access to buildings, loss of lives, transportation, and the availability of recovery sites, influenced the response's effectiveness (i.e., the response that was effective in the 1993 bombing event was not (as) effective in 2001). That is, organizations should not sink into a mindset of complacency only because some earlier incident was averted successfully but should sustain a (pro)active attitude toward incidents. Thus, while it is likely that the technologies, the plans, and the social aspects are complementary and contingent on the incident rather than mutually exclusive, any incident preparations require active and ongoing activity to be successful. In Section 5, I focus on integrating the themes and point out certain gaps that need to be addressed to move further toward a unified, integrated view.

5 Discussion and Suggestions for Future Research

I began this paper with the organizational problem of incidents and ask how organizations can prepare for and respond to incidents to guide the review. To address this question, I reviewed multidisciplinary literature on BC in which I focused on topics of interest for IS community. These contributions form the foundations for IS continuity.

The purpose of the multidisciplinary approach I used here was to cross the boundaries of disciplinary domains in order to increase understanding and to provide new ideas from the IS reference disciplines and beyond. The literature analysis shows that the topic is both an intra-IS disciplinary and a multidisciplinary concern. This research's interdisciplinary nature brings together the multidisciplinary fragmented ideas to enrich IS research on business continuity with ideas from other disciplines (Stember, 1991).

Next, I suggest an integrative framework for IS continuity that brings the multidisciplinary discussions closer. The framework has two purposes: 1) it provides an integrated overview of the literature and how the different areas of interest fit together and 2) it provides a basis for discussing some of the gaps that need to be addressed to move further toward a unified view.

5.1 Integrating the Themes of IS Continuity

Building on and extending the reviewed literature, Figure 2 illustrates the IS continuity integrative framework. I start by clarifying concept definitions related to the framework. I then describe each part of the framework and provide illustrative examples from the past research, which is in line with the narrative approach I have adopted for this study.

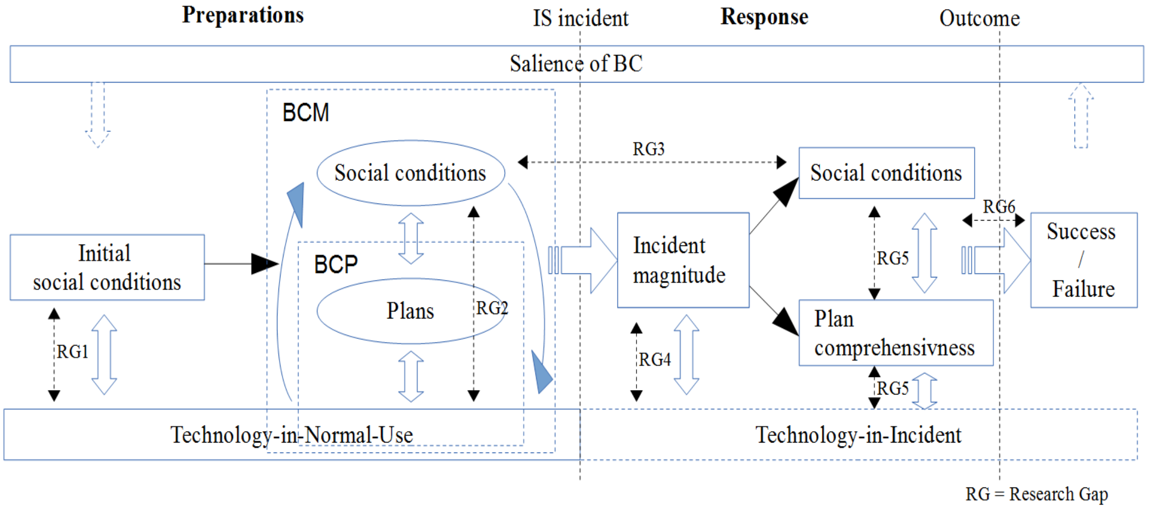

Figure 2. Integrative Framework for IS Continuity

In line with the past definitions (see Table 1), the scope of IS continuity in the integrative framework covers the preparations for and responses to an incident. The wide scope consolidates the views of those authors who limit the scope to preparations and those who extend the scope to also cover the response to an incident. A narrower scope would mean excluding some of the definitions and research from the framework. The preparation phase covers all aspects of preparation—from the initial decision to initiate a project to a point when an event befalls—and the response phase covers all aspects of response—from detecting and initially reacting to the incident to the point when the organization has recovered (or not recovered). Thus, the integrative framework promotes a holistic view of IS continuity rather than isolating the preparations and response to separate domains of interest and research. The holistic view makes sense because the preparations for incidents and how they are enacted in responding to an incident are intimately linked. From this view, there are three “continuity states” instead of a single “continuity state”: 1) the preparations, 2) the response, 3) and the outcome. The continuity capability, then, is an organization’s ability to maintain preparations state (see left side of Figure 2) and to successfully recover from the response state (see right side of Figure 2). In addition, this view differentiates “IS continuity” itself from the models that increase the capability—a separation that has been blurry in past research. To summarize, the framework itself does not pose limits as to whether the IS continuity is an organizational capability, a methodological, means-to-an-end approach, or an organizational state of operations; they fit to different parts of the framework.

In contrast to prior literature, the integrative framework explicitly differentiates between technology-in-normal-use and technology-in-incident (see Section 4.3.2). The technology-in-normal-use refers to the IT technology organizations use to run their routines. The technology-in-normal-use includes those IT technologies the organization has implemented to support and increase the continuity of normal business operations and those designed especially to support the incident preparations. Past IS continuity research has made contributions to both types of technology, such as “always-on computing” (Bajgoric, 2006), DWDM technology (Ceballos et al., 2012), and databases for consolidating all continuity plans (Husband, 2007). The technology-in-incident refers to technology available and in use during an incident. An incident induces changes to organizational technology. For instance, an incident that cripples an organization’s primary IT infrastructure changes the organizational technology in use and simultaneously a need for additional technology not in use before the incident (or using the same technology differently) arises. The organization has to use its secondary IT infrastructure (if the organization has made such preparations) and take into use the technology designed for responding to an incident, such as the mobile collaboration tool (Sapateiro et al., 2011) and other diagnostics and troubleshooting tools, or shift altogether to alternative ways of working, such as telecommuting (Heng et al., 2012; Roitz & Jackson, 2006).

5.1.1 The Preparations

The integrative framework takes a socio-technical process view of continuity that brings closer the social and the technical aspects of continuity (see Sections 4.3.1 and 4.3.2). The process starts from initializing organizational preparations for incidents, which is influenced by organizational social conditions at individual and collective levels, such as top management's state of mind, wider societal culture, and organizational culture. Past research suggests that management needs to be convinced of the salience of proactive preparations (for instance, by using top management's "weak points" or by appealing to past incidents (Seow, 2009)) and that the wider societal culture may inhibit initiating preparations at the organizational level (Sawalha & Meaton, 2012), whereas "correct" organizational culture may promote the initiation (King, 2003). Thus, appealing to descriptions of past incidents and studies that in other ways underline the significance of IS continuity preparations are likely to be a useful source for both the top managers and for those who need to convince the top managers (see Section 4.3.3). Further, an organization's experience of its technology-in-normal-use may influence the initial social conditions in it (indicated as the blue arrow between initial social conditions and technology-in-normal-use in Figure 2). For instance, as a simple and general example, those organizations that perceive their technology-in-normal-use to be unreliable are more open to the idea of initiating measures to reduce the number of incidents and hasten recovery. Similarly, documented cases of past incidents specific to a certain technology (for instance, break downs of certain enterprise resource planning (ERP) software) are likely powerful motivators.

After the preparations have been initiated, the quest is to create/improve plans, technologies, and social conditions (the black arrow in Figure 2 indicates the transition from initiation to improvement). This is the primary domain of BCP/BCM research (see Section 4.3.4) as indicated by the dotted line boxes in Figure 2. I do not claim that BCP research would completely neglect the social conditions but indicate the main thrust of the research. Similarly, I do not claim that BCM would completely neglect the response part but indicate that the main thrust has been in the embeddedness of organizational BC measures as part of organizational social conditions.

The BCP/BCM models provide authoritative guidance to preparations. The models provide guidance to creating plans, choosing technologies, and facilitating "correct" social conditions (such as "correct" culture (King, 2003; Sawalha & Meaton, 2012) and commitment to BC (Herbane et al., 2004)). More-specific models support organizations in more-specific tasks, such as in choosing the appropriate backup IT infrastructure location (Turetken, 2008), "surviving" an audit (Freestone & Lee, 2008), or training and exercising the social actors for incidents (Kendall et al., 2005).

As a means of preparation, organizations seek to employ advanced technologies that potentially move the occurrence of incidents further into the future (see Section 4.3.2). As Messer (2009) argues, continuity planning "is not only planning for what to do when an event occurs, but the preparation, planning and implementation to avoid a crisis in the first place" (p. 13). However, monetary constraints often pose significant challenge because advanced technology may require a large budget. Business impact analysis (BIA), as conducted as part of BCP (Pitt & Goyal, 2004), assists organizations to evaluate the value of their technology and choose appropriate measures thereof (Messer, 2009). The estimation is often based on subjective evaluation of the (monetary) value of the technologies the organization uses, which is likely shaped by the organizational social conditions. Even if the organization is able to invest in the latest advanced technologies, there is always a possibility for an incident in an unpredictable, uncertain, and turbulent environment. Plans complement the technologies and prepare organizations for the time when an incident occurs.

The plans should reflect the technology-in-normal-use, but the contents are created by social actors (although the technology/media used to store and create the plans may impose limitations as to how the plans are created and what they contain). The social actors' individual and collective understanding and experience of the technology-in-normal-use, construction of how technology should be improved, and what should be documented because plans are likely to vary and evolve during the preparation process. The BIA, for instance, shapes the social conditions by changing organizational members' view on continuity as business-as-usual (Messer, 2009) that is likely to promote embeddedness (Herbane et al., 2004).

Further, the various social actors that should participate to the planning process (Kendall et al., 2007) are likely to evaluate the most significant threats to organization differently. Using a decision support system to make evaluations is likely to influence the evaluation (Van de Walle & Rutkowski, 2006) and may change how the social actors view the different technologies that make up the organizational technology-in-normal-use. The implemented decision support system, when adopted by the organization, becomes integrated as a part of its technology-in-normal-use. Once the technology is implemented and adopted, it becomes implicated in and shapes the further cycles of preparations (for instance, by shaping the estimations of the severity of imagined incidents). There is, thus, a cyclic relation (depicted in Figure 2 with the blue, curvy arrows) between the technology-in-normal-use and the social conditions as cycles of reflection and improvement.

5.1.2 The Response

An incident induces a shift from preparation to response (indicated by the blue right-pointing arrow on Figure 2). The incident changes the organizational technology-in-normal-use based on the incident's magnitude. However, the degree of change may vary between very insignificant to very significant (or catastrophic). The more entangled the technology is to organizational processes, the more important the IT system likely is and the more severe organizational damage it can be assumed to inflict. Interestingly, technology that fails may very well be the tool that supports the incident preparations and response and may, thus, become a source of an incident itself. In other words, IT tools and the risk of incident they pose *imbricate*: "the powerful digital 'tools' that enable the more sophisticated representation of risks are at the same time the cause of a potential irruption of the 'incalculable', of not easily representable risks due their man-made character arising from insidious, rare, and undetectable side-effects" (Ciborra, 2006, p. 1341).

Incident magnitude influences what response is suitable. Organizations should first and foremost rely on plans (Stucke et al., 2008). While the plans themselves will not provide any response to an incident per se but need attentive social actors to enact them, a plan's comprehensiveness influences whether it can be used as a basis for response. A plan's comprehensiveness also means that it is accurate because false or inaccurate information is of little use; it is imperative to periodically review the plans. A continuity-aware culture is likely to promote keeping the plans up-to-date (King, 2003), which can be achieved by using supportive IT technology (Husband, 2007). However, if the incident falls beyond that which is planned and documented, organizations have to resort to adaptability and social ingenuity. The possibilities for response are further shaped by the technology-in-incident. For instance, whether the organizational normal communication channels, such as email and instant messaging, are available for use alter the ways in which an organization can reorganize itself (e.g., form virtual teams during an incident (Roitz & Jackson, 2006)) and coordinate the response. Thus, responding to a given incident is likely shaped by the interplay of the social conditions, plan comprehensiveness, and the technology-in-incident.

5.1.3 The Outcome

After an incident, organizations should review and revise their plans and their actions and other current measures taken during the incident. Past incidents can be a valuable source for improvement (Lindström et al., 2010b) and help organizations to survive future incidents (Alonso & Boucher, 2001). The actions and measures taken a prior but also during an incident are likely to influence the outcome. Indeed, it would not make much sense to make preparations unless they influenced the outcome when organizations face an incident. Organizations are then to assess whether the preparations and the enacted response to an incident succeeded or failed, which they may do by evaluating success against the pre-calculated RTO/RPO values. Thus, if an organization fails to meet the calculated objectives, the response is a failure, and when the recovery is in the calculated objectives, it is a success. Naturally, if the a posteriori analysis suggests that the experienced incident was too costly for the organization even if the RTO/RPO was met, the past incident provides a point for readjusting the RTO/RPO values to more realistic calculations. That is, the incident becomes a point of learning for the organization.

Even though the main emphasis of the research on salience of IS continuity (see Section 4.3.3) has been on the significance and positive effects of making preparations for incidents, the research extends from the initial organizational (social) conditions to recovery and post incident outcome. The research on the salience of IS continuity fits to the framework through interrelations to two parts of the framework. First, the research on the salience of IS continuity may contribute to organizations' incident preparations by altering the initial social conditions through motivating descriptions and elaborations, communicated to scholars and practitioners through various publication outlets, on why organizations should make a priori preparations. Second, the a posteriori analyses documents the lessons learned from past incidents for wider audience and, thus, serve as important points of reflection to others. Indeed, such research is beneficial to organizations as a knowledge base of what has and has not worked in the past.

5.2 Recommendations for Future Research

Structuring the past has opened venues not yet taken by scholars interested in IS continuity. The discussion and the future directions here should highlight the need for (and, hopefully, attract) new scholarly contributions to IS continuity (and business continuity in general)—both outside and in the IS discipline's confines. The dotted line arrows in Figure 2 indicate research gaps (RG) in the framework. The RGs are not all-encompassing and reflect the current state of IS continuity (i.e., many other gaps likely await discovery as the research on IS continuity progresses). The identified RGs build on the reviewed literature but focus on BC's socio-technical aspects. Focusing on the socio-technical aspects that are interactional is relational to the integrative and interdisciplinary focus of this research: that is, it brings together rather than separates and keeps apart. While this choice might overlook certain (important) gaps that are not relational to the interactional focus, for the sake of community formation around IS continuity, locating and proposing a research agenda that includes interactional areas is likely beneficial. The interactional areas promote collaboration in such a way that scholars from different disciplines may bring their particular strengths and perspectives to address a mutually shared concern and, thus, colligate scholars across disciplines. Table 2 briefly overviews the identified RGs.

Table 2. Research Gaps (RGs)

RGs	Related research	What is known	Description of RG	Possible ways of researching
RG1	Stanton (2005), Kite & Zucca (2007), Seow (2009), Lindström et al. (2010a)	Top management's attitude and social and organizational culture influences organizational willingness to initiate preparations.	The interaction between technology-in-normal-use and initial social conditions.	Empirical research studying how the type and organizational dependency of technology shapes organizational willingness to initiate incident preparations.
RG2	King (2003), Herbane et al. (2004)	Organizational culture and embeddedness promotes planning. Technology aids the creation and maintenance of plans.	The cyclic interaction between social conditions and technology-in-normal-use.	Empirical research studying how the organizational social conditions influence the social construction of the technology and shape the continuity planning and implementation of continuity (enhancing) technology. Empirical research studying how the process of preparations unfold and evolve in practice.
RG3	Kendall et al. (2005), Butler & Gray (2006), Gibb & Buchanan (2006)	In a broad sense, organizations that have prepared for incidents seem to cope better with incidents. Testing and exercising plans and procedures as part of preparations prepare organizations for real incidents. Social conditions may alter organizations' ability to detect early cues to avoid incidents.	The transition of social conditions between preparations and response.	Empirical research studying how the social conditions between preparations and response shift due to the incident conditions and vary under artificial versus real conditions.
RG4	Berman (2002), Halliwell (2008)	Incidents differ in magnitude. Environmental aspects (e.g., day of the week, access to office premises) influence the magnitude. Magnitude influences response, but the response also influences the magnitude (e.g., activities may hide incidents, incidents may cascade, or response may create more damage).	The interaction between "technology-in-incident" and incident magnitude.	Empirical research studying how the type of incident (in contrast to environmental aspects) is related to the magnitude of incident as experienced by an organization. Empirical research studying how the magnitude of similar type of incidents is shaped by the type and use of organizational technology.

Table 2. Research Gaps (RGs)

RG5	Roitz & Jackson (2006), Sapateiro et al. (2011), Heng et al. (2012), Rapaport & Kirschenbaum (2008)	BC plans provide basis for response action. Technological tools designed for responding to incidents improve coordination and collaboration during them. Technology implemented for other purposes, such as telecommuting, may become enacted as tools for incident response. Social relations and individual background influence response.	The interaction between social conditions, plans and technology-in-incident.	Empirical research studying the occurrence and enactment of responses to an incident to understand how the incident response (which likely combines the social conditions (e.g., social relations, mindfulness), plans, and technology) unfolds during an incident as organizational actors individually and collectively respond to it.
RG6	Cervone (2006), Geelen-Baass & Johnstone (2008), Messer (2009)	Organizations that have been able to return to normal business after an incident in the preplanned timeframe are successful.	The transition from response to evaluating success or failure.	Empirical research on how organizational members individually and collectively construct the meaning of success or failure of responding to an incident. Empirical or conceptual research on how success or failure can be measured by alternative metrics.

5.2.1 The Interaction between Technology-in-Normal-Use and Initial Social Conditions

As Hecht (2002) argue, any organization dependent on IS requires BCM. But how do organizations' understanding of the IS dependency form and what are the individual- and collective-level factors that shape the understanding (RG1)? Organizations are complex, and the technologies they use are many and often interact with each other. Under such conditions, various factors likely shape organizational understanding of the dependency on IS. Prior research focusing on top management support, at least implicitly, acknowledges that the matter is not straightforward. Otherwise, there would be no need to "sell" the BC to top management or to convince them. Technology implementations and already existing technology in use are likely to influence organizational social conditions. For instance, implementing an organizational-wide critical information system will increase an organization's technology dependence and shape how the organization understands its technologies role in relation to organizational BC. However, the relation between technology implementation or technology in use (technology-in-normal-use) to incident preparations should be studied further (RG1, RG2).

5.2.2 The Cyclic Interaction between Social Conditions and Technology-in-Normal-Use

Based on this review, it seems that we know little about the actual process of BC preparations: how the process unfolds and evolves, how the involved actors make sense of the preparations as the process evolves, how their understanding develops, how the actions evolve, and how the social processes and conditions are shaped and reshaped during the process (RG2). Although the prior literature includes accounts of how an implementation has proceeded, they are often descriptive in nature. Instead of straightforward accounts of the implementation, we need studies that convey the complexity and surfaces the meanings and goals (perhaps even conflicting) of the participants.

5.2.3 The Transition of Social Conditions between Preparations and Response

Studies focusing on preparing for an incident largely assume the preparations are, indeed, effective during an incident. However, we lack studies focusing on the transition from normal operating conditions to responding to an incident (i.e., RG3). As organizations integrate more tightly with technology, organizational conditions, both the technological and social, are likely to change abruptly in the awake of an incident. How the actual incident induced shifts in the conditions match a priori expectations of incident conditions has not received the needed attention. Shifts in the conditions may have significance to whether a priori preparations are effective or whether they shatter when an organization truly experience an incident. However, researching such transitions poses difficulties for research due to their relatively rare occurrence and unpredictability (cf. Stallings, 2007), especially as, in an optimal case, the research would have to take place in situ rather than a posteriori for a naturalistic research setting.

5.2.4 The Interaction between Technology-in-Incident and Incident Magnitude

Organizations differ in their technology use and the technological configurations they have are likely to influence the incident magnitude. For instance, robust and highly available technology is more likely to withstand incidents better than other technology as Bajgoric's (2009) “always-on” computing suggests. However, not only the magnitude but also the type of an incident is likely to result in different responses and to differing outcomes (RG4). For instance, technology breakdowns are likely to initiate a different response than a malicious user circumventing a technology's security mechanisms. Understanding how incidents' qualitative differences shape organizations’ experienced magnitude and response to them could potentially contribute not only to more effective responses but also to better explaining the challenges related to preparing for incidents. Understanding the qualitative differences would imply a shift in BC’s underlying assumption to come up with generalized and common processes for preparing for and responding to incidents to appreciate the qualitative differences—the nuances of incidents that matter. Although generic abstractions as methodological steps are certainly indispensable in guiding organizations in their efforts to prepare for and respond to incidents, they largely assume the actual practices of preparations will automatically follow as soon as appropriate and accurate abstractions have been grasped. However, we can expect that, on the micro-level, in the level of actual practices, preparing IS for natural disasters differs from preparing them for man-made ones.

5.2.5 The Interaction between Social Conditions, Plans, and Technology-in-Incident

The role of plans, technology, and social conditions during an incident is largely unsolved in IS continuity literature. To understand how plans are actually effective and used during adverse conditions would improve understanding on the matter. Wider IS literature suggests plans, under normal conditions, are not enacted in practice but rather act as an information source (Suchman, 2005). If such is true also with incidents, how plans are used will likely differ from the BC planners’ intended use. Thus, understanding how plans are enacted under real conditions may provide useful insights for preparing effective plans. Further, technologies’ flexibility and availability during an incident likely shape organizational actions. Such situations are likely to require increased use of different technologies (e.g., diagnostics and troubleshooting technology), well-thought-out pre-planned actions, and social conditions that facilitate ingenuity. How technology, plans, and social actions interconnect during an incident response also requires more attention (RG5).

5.2.6 The Transition from Response to Evaluation of Success or Failure

Knowing when organizational BC is a success or a failure is difficult to assess. The above integrating framework suggests one possible way to assess success or failure is to use the calculated RTO / RPO values. However, these values are calculated as the last point of recovery; that is, as the last possible point from which the recovery is still possible before the organization suffers so much damage that it will very likely perish. However, organizations are likely to benefit from other measures of success / failure than assessing whether it (as a whole) survives from the incident or not. Further, success / failure is likely to be a more complicated construct. Any preparations and response to incidents will likely have certain factors/aspects that have been successful and factors/aspects that have been a failure. Therefore, future research should find ways to assess the success or failure of BC (RG6) in more detail.

5.3 Limitations

This research is subject to limitations. First, it focuses on peer-reviewed journal papers instead of wider practitioner and conference literature. Business continuity is practitioner driven, and many papers in professional publication outlets are likely to also cover some aspects of interest for scholars interested in IS continuity. Thus, the literature review provided here might not present a complete picture of the topic. Nevertheless, the literature review provides a useful reference source for both the practitioners and academics. In addition, the review approach I use is subjective to some degree. I did not cover all papers in the review to the same extent. Instead, I chose to elaborate on papers I deemed as influential, illustrative, or interesting. Needless to say, resulting from the selection process, some authors' voices are more visible than others'. Categorization summaries and quantifications of the reviewed papers balance the limitation to some extent, but do not fully remove it.

6 Conclusion

In this paper, I review the multidisciplinary literature on business continuity (BC) from an IS perspective. The review was guided by the question: “how organizations can prepare for and respond to IS incidents?”. The reviewed literature forms the foundations of IS continuity.

Following Webster and Watson (2002), I thematized the past contributions on IS continuity. To this end, four main themes emerged from the literature: 1) social aspects as IS continuity enabler, 2) technology as IS continuity enabler, 3) salience of IS continuity, and 4) models that improve IS continuity. I also suggest an integrative framework by building on and extending the reviewed literature to progress discussion around BC toward a unified view of IS continuity, and, further, to pinpoint research gaps. The integrative framework promotes a view of BC in which plans, technologies, and social aspects complement and interact with each other.

This research contributes to the literature on BC by structuring the past contributions and identifying possible paths for future research, especially for those interested on the part that IS has for business continuity. At best, interdisciplinary projects such as this one encourage a community’s formation (Stember, 1991). This research contributes to forming a community around IS continuity, which is a shared topic of interest among scholars across disciplines. Further, as Klein and Hirscheim (2008) argue, one can characterize IS as a diverse set of practice communities and knowing among which “[w]e need to choose our particular communities and fully engage with them” (Walsham 2012, p. 3). To this extent, by identifying and structuring the literature under the IS continuity concept, this research enables scholars to identify this particular community of practice and knowing. While this research cannot guarantee that a prosperous and vivid community will evolve around the IS continuity, it will hopefully lower the barrier of joining the already existing, although fragmented, community.

Acknowledgments

I am in debt to John Lindström for his critical and detailed review, Jonna Järveläinen for her feedback on an earlier revision of the research paper, and Elina Laaksonen for her insightful comments, discussions, and support during the whole research process.

References

Adkins, G. L., Thornton, T. J., & Blake K. (2009). A content analysis investigating relationships between communication and business continuity planning. *Journal of Business Communication*, *46*(3), 362-403.

Alesi, P. (2008). Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology. *Journal of Business Continuity & Emergency Planning*, *2*(3), 214-220.

Alonso, F., & Boucher, J. (2001). Business continuity plans for disaster response. *The CPA Journal*, *71*(11), 60.

Alter, S. (2003). 18 reasons why IT-reliant work systems should replace "the IT artifact" as the core subject matter of the field. *Communications of the Association for Information Systems*, *12*, 366-395.

Arduini, F., & Morabito, V. (2010). Business continuity and the banking industry. *Communications of the ACM*, *53*(3), 121-125.

Asgary, A., & Mousavi-Jahromi, Y. (2011). Power outage, business continuity and businesses' choices of power outage mitigation measures. *American Journal of Economics and Business Administration*, *3*(2), 312-320.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787-2805.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, *30*(5), 413-438.

Bacon, C. J., & Fitzgerald, B. (2001). A systemic framework for the field of information systems. *ACM SIGMIS Database*, *32*(2), 46-67.

Bajgoric, N. (2006). Information technologies for business continuity: an implementation framework. *Information Management & Computer Security*, *14*(5), 450-466.

Bajgoric, N., & Moon, Y. B. (2009). Enhancing systems integration by incorporating business continuity drivers. *Industrial Management & Data Systems*, *109*(1), 74-97.

Bajgoric, N. (2010). Server operating environment for business continuance: Framework for selection. *International Journal of Business Continuity and Risk Management*, *1*(4), 317-338.

Basel Committee on Banking Supervision (2006). *High-level principles for business continuity*. Retrieved from http://www.bis.org/publ/joint17.pdf

Benbasat, I., & Zmud, R. W. (2003). The identity crisis within the IS discipline: Defining and communicating the discipline's core properties. *MIS Quarterly*, *27*(2), 183-194.

Benyoucef, M., & Forzley, S. (2007). Business continuity planning and supply chain management. *Supply Chain Forum: An International Journal*, *8*(2), 14-22.

Berman, A. (2002). Lessons learned: The aftermath of September 11. *Information Systems Security*, *11*(2), 30-37.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting reviews and literature searches. *Communications of the Association for Information Systems*, *34*, 257-286.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly*, *1*(3), 17-32.

Botha, J., & von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security*, *12*(4), 328-337.

British Standard Institution. (2006). *BS 259999-1:2006 Business continuity management, part 1: Code of practice.* UK: British Standard Institution.

Business Continuity Institute (2013). *Horizon scan 2013: Survey report*. Retrieved from http://www.thebci.org/index.php/download-the-2013-horizon-scan-report

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly*, *30*(2), 211-224.

Castillo, C. (2005). Disaster preparedness and business continuity planning at Boeing: An integrated model. *Journal of Facilities Management*, *3*(1), 8-26.

Ceballos, J., DiPasquale, R., & Feldman R. (2012). Business continuity and security in datacenter interconnection. *Bell Labs Technical Journal*, *17*(3), 147-156.

Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management*, *21*(3), 70-78.

Cervone, F. (2006). Disaster recovery and continuity planning for digital library systems. *OCLC Systems & Services: International Digital Library Perspective*, *22*(3), 173-178.

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, *14*(3), 197-235.

Ciborra, C. (2006). Imbrication of representations: Risk and digital technologies. *Journal of Management Studies*, *43*(6), 1339-1356.

Conseil, A., Mounier-Jack, S., & Coker, R. (2008). Business continuity planning and pandemic influenza in Europe: A thematic analysis of independent sector and national governments' guidance. *Journal of Business Continuity & Emergency Planning*, *3*(1), 75-91.

Copenhaver, J., & Lindstedt, D. (2010). From cacophony to symphony: How to focus the discipline of business continuity. *Journal of Business Continuity & Emergency Planning*, *4*(2), 165-173.

Daily Telegraph. (2013). *Anonymous' hacker who cost Paypal millions escapes jail.* Retrieved from http://www.telegraph.co.uk/technology/internet-security/9842397/Anonymous-hacker-who-cost-Paypal-millions-escapes-jail.html

Desanctis, G. (2003). The social life of information systems research. *Journal of the Association for Information Systems*, *4*(7), 360-376.

Freestone, M., & Lee, M. (2008). Planning for and surviving a BCM audit. *Journal of Business Continuity & Emergency Planning*, 2(2), 138-151.

Galliers, R. D. (2003). Change as crisis or growth? Toward a trans-disciplinary view of information systems as a field of study: A response to Benbasat and Zmud's call for returning to the IT artifact. *Journal of the Association for Information Systems*, *4*(6), 337-351.

Geelen-Baass, B. N., & Johnstone, J. M. (2008). Building resiliency: Ensuring business continuity is on the health care agenda. *Australian Health Review*, *32*(1), 161-173.

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, *26*(2), 128-141.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567-A2.

Haapalainen H. (2012). Sandy-myrsky sotkenut tietojärjestelmiä Suomessakin. *Yle.* Retrieved from http://yle.fi/uutiset/sandy-myrsky_sotkenut_tietojarjestelmia_suomessakin/6358793

Halliwell, P. (2008). How to distinguish between “business as usual” and “significant business disruptions” and plan accordingly. *Journal of Business Continuity & Emergency Planning*, *2*(2), 118-127.

Hassanain, M. A., & Al-Mudhei, A. (2006). Business continuity during facility renovations. *Journal of Corporate Real Estate*, *8*(2), 62-72.

Hecht, J. A. (2002). Business continuity management. C*ommunications of the Association for Information Systems*, *8*, 444-450.

Heng, T., Hooi, S., Liang, Y., Othma, A., & San, O. (2012). Telecommuting for business continuity in a non-profit environment. *Asian Social Science*, *8*(12), 226-237.

Henry Stewart Publications. (2013). *Instructions for authors.* Retrieved from http://www.henrystewartpublications.com/jbcep/instructions

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

Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: Time for a strategic role? *Long Range Planning*, *37*(5), 435-457.

Hinde, S. (2005). From incidents to disasters. *Computer Fraud & Security*, *2005*(4), 17-19.

International Organization for Standardization. (2012). *ISO 22301 Societal security—business continuity management systems—requirements*. Geneva, Switzerland.

International Organization for Standardization. (2011). *ISO/IEC 20000-1:2005 Information technology—service management—part 1: Service management system requirements*. Geneva, Switzerland.

Iyer, R. K., & Bandyopadhyay, K. (2000). Managing technology risks in the healthcare sector: Disaster recovery and business continuity planning. *Disaster Prevention and Management*, *9*(4), 257-270.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*(5), 332-349.

Kadam, A. W. (2010). Personal business continuity planning. *Information Systems Security*, *19*(4), 4-10.

Kendall, K. E., Kendall, J. E., & Lee, K. C. (2005). Understanding disaster recovery planning through a theatre metaphor: Rehearsing for a show that might never open. *Communications of the Association for Information Systems*, *16*, 1001-1012.

King, D. L. (2003). Moving towards a business continuity culture. *Network Security*, *2003*(1), 12-17.

King, W. R., & He, J. (2005). Understanding the role and methods of meta-analysis in IS research. *Communications of the Association for Information Systems*, *16*, 665-686.

Kite, C. S., & Zucca, G. S. (2007). How to access your board/c-suite and make an effective case for business continuity investments. *Journal of Business Continuity & Emergency Planning*, *1*(4), 332-339.

Klein, H. K., & Hirscheim, R. (2008). The structure of the IS discipline reconsidered: Implications and reflections from a community of practice perspective. *Information & Organization*, *18*(4), 280-302.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, *23*(1), 67-93.

Lindstedt, D. (2008). Grounding the discipline of business continuity planning: What needs to be done to take it forward? *Journal of Business Continuity & Emergency Planning*, *2*(2), 197-205.

Lindström, J., Harnesk, D., Laaksonen, E., & Niemimaa, M. (2010b). A methodology for inter-organizational emergency management continuity planning. *International Journal of Information Systems for Crisis Response and Management*, *2*(4), 1-19.

Lindström, J., Samuelsson, S., & Hägerfors, A. (2010a). Business continuity planning methodology. *Disaster Prevention and Management*, *19*(2), 243-255.

Luftman, J., & Ben-Zvi, T. (2010). Key issues for IT executives 2010: Judicious IT investments continue post-recession. *MIS Quarterly Executive*, *9*(4), 263-273.

McConnell, A., & Drennan, L. (2006). Mission impossible? Planning and preparing for crisis. *Journal of Contingencies and Crisis Management*, *14*(2), 59-70.

McLoughlin, R. (2009). What one must know about achieving BS25999-2 certification. *Journal of Business Continuity & Emergency Planning*, *3*(2), 105-111.

Messer, I. (2009). Taking the business continuity programme to a corporate leadership role. *Journal of Business Continuity & Emergency Planning*, *4*(1), 8-13.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Thousand Oaks, CA: Sage.

Momani, N. M. (2010). Business continuity planning: Are we prepared for future disasters. American *Journal of Economics and Business Administration*, *2*(3), 272-279.

Moyer, J., & Novick, K. (2012). Introducing a new resource for water and wastewater system business continuity planning. *American Water Works Association Journal*, *104*(3), 37-39.

Myers, M. D. (2004). Hermeneutics in information systems research. In J. Mingers & L. Willcocks (Eds.), *Social theory and philosophy for information systems* (pp. 104-128). Chichester, UK: John Wiley & Sons.

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *Distribution & Logistics Management*, *34*(5), 434-456.

Nosworthy, J. (2000). A practical risk analysis approach: managing BCM risk. *Computers & Security*, *19*(7), 596-614.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1-28.

Orlikowski, W. J., & Scott, S. V. (2008). Sociomateriality: Challenging the separation of technology, work and organization. *The Academy of Management Annals*, *2*(1), 433-474.

Pearson, C. M., & Clair J. A. (1998). Reframing crisis management. *The Academy of Management Review*, *23*(1), 59-76.

Pheng, L. S., Ying, L. J., & Kumaraswamy, M. (2010). Institutional compliance framework and business continuity management in Mainland China, Hong Kong SAR and Singapore. *Disaster Prevention and Management*, *19*(5), 596-614.

Pitt, M., & Goyal, S. (2004). Business continuity planning as a facilities management tool. *Facilities*, *22*(3/4), 87-99.

Power, R., & Forte, D. (2006). You don't need a weatherman to know which way the wind blows: Business continuity in the 21st century. *Computer Fraud & Security, 2006*(8), 17-19.

Rapaport, C., & Kirschenbaum, A. (2008). Business continuity as an adaptive social process. International *Journal of Emergency Management*, *5*(3/4), 338-347.

Roitz, J., & Jackson, E. (2006). AT&T adds business continuity to the long list of telework's advantages. *Journal of Organizational Excellence*, *25*(2), 3-12.

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.

Sawalha, I. H., & Anchor, J. R. (2012). Business continuity management in emerging markets: The case of Jordan. *Journal of Business Continuity & Emergency Planning*, *5*(4), 327-337.

Sawalha, I. H., & Meaton, J. (2012). The Arabic culture of Jordan and its impacts on a wider Jordanian adoption of business continuity management. *Journal of Business Continuity & Emergency Planning*, *6*(1), 84-95.

Science Publications. (2014). *American journal of economic and business administration—description*. Retrieved from http://thescipub.com/journals/ajeba

Selden, S., & Perks, S. (2007). How a structured BIA aligned business continuity management with Gallaher's strategic objectives. *Journal of Business Continuity & Emergency Planning*, *1*(4), 348-355.

Seow, K. (2009). Gaining senior executive commitment to business continuity: motivators and reinforcers. *Journal of Business Continuity & Emergency Planning*, *3*(3), 201-208.

Shaw, G., & Harrald, J. (2006). The core competencies required of executive level business crisis and continuity managers—the results. *Journal of Homeland Security and Emergency Management*, *3*(1), 1-34.

Shaw, S., & Smith, N. (2010). Mitigating risks by integrating business continuity and security. *Journal of Business Continuity & Emergency Planning*, *4*(4), 329-337.

Sheth, S., McHugh, J., & Jones, F. (2008). A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects. *Journal of Business Continuity & Emergency Planning*, *2*(2), 221-239.

Siponen, M., & Willison, R. (2007). A critical assessment of IS security research between 1990-2004. In *Proceedings of European Conference on Information Systems* (pp. 1551-1559).

Smith, D. (2003). Business continuity and crisis management. *Management Quarterly*, 27-33.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly*, *34*(3), 463-486.

Speight, P. (2011). Business continuity. *Journal of Applied Security Research*, *6*(4), 529-554.

Stallings, R. A. (2007). Methodological issues. In H. Rodríguez, E. L. Quarantelli, & R. R. Dynes (Eds.), *Handbook of disaster research* (pp. 55-82). New York, NY: Springer.

Stanton, R. (2005). Beyond disaster recovery: The benefits of business continuity. *Computer Fraud & Security*, *2005*(7), 18-19.

Stember, M. (1991). Advancing the social sciences through the interdisciplinary enterprise. *The Social Science Journal*, *28*(1), 1-14.

Strong, B. (2010). Creating meaningful business continuity management programme metrics. *Journal of Business Continuity & Emergency Planning*, *4*(4), 360-367.

Stucke, C., Straub, D. W., & Sainsbury, R. (2008). Business continuity planning and the protection of informational assets. In D. W. Straub, S. Goodman, & R. L. Baskerville (Eds*.), Information security: Policy, processes and practices* (pp. 152-171). Armonk, NY: M.E. Sharpe.

Suchman, L. A. (2007). *Human-machine reconfigurations: Plans and situated actions*. Lancaster, UK: Cambridge University Press.

Swartz, E., Elliott, D., & Herbane, B. (2003). Greater than the sum of its parts: Business continuity management in the UK finance sector. *Risk Management*, *5*(1), 65-80.

Swedish Civil Contingencies Agency. (2011). *Reflektioner kring samhällets skydd och beredskap vid allvarliga IT-incidenter*. Retrieved from https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Reflektioner-kring-samhallets-skydd-och-beredskap-vid-allvarliga-it-incidenter-/

Talbot, C. (2012a). Hurricane Sandy: How did cloud data centers fare? *Talkin'Cloud*. Retrieved from http://talkincloud.com/cloud-computing-management/hurricane-sandy-how-did-cloud-data-centers-fare

Talbot, C. (2012b). Cloud, disaster recovery lessons learned from Hurricane Sandy*. Talkin'Cloud*. Retrieved from http://talkincloud.com/cloud-virtualization/cloud-disaster-recovery-lessons-learned-hurricane-sandy

Tammineedi, R. L. (2010). Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective*, *19*(1), 36-50.

Thibodeau, P. (2012). Hurricane Sandy leaves wounded servers in its wake. *ComputerWorld.* Retrieved from http://www.computerworld.com/s/article/9233754/Hurricane_Sandy_leaves_wounded_servers_in_its_wake

Thornton, G. (2008). An innovative, flexible and workable business continuity plan: Case study of the Australian customs service cargo BCP. *Journal of Business Continuity & Emergency Planning*, *3*(1), 47-54.

Turetken, O. (2008). Is your back-up IT infrastructure in a safe location? A multi-criteria approach to location analysis for business continuity facilities. *Information Systems Frontier*, *10*(3), 375-383.

Van de Walle, B., & Rutkowski, A. (2006). A fuzzy decision support system for IT service continuity threat assessment. *Decision Support Systems*, *42*(3), 1931-1943.

Walch, D., & Merante, J. (2008). What is the appropriate business continuity management staff size? *Journal of Business Continuity & Emergency Planning*, *2*(2), 240-250.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320-330.

Wan, S. (2009). Service impact analysis using business continuity planning processes. *Campus-Wide Information Systems*, *26*(1), 20-42.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii-xxiii.

Wong, W. N. Z. (2009). The strategic skills of business continuity managers: Putting business continuity management into corporate long-term planning. *Journal of Business Continuity & Emergency Planning*, *4*(1), 62-68.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems*, *31*(2), 35-60.

Zsidisin, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research*, *43*(16), 3401-3420.

Appendix A: List of Journals and Disciplines

Categorization of journals to IS discipline followed that of Siponen and Willison (2007) with some additions. I included *Communications of the ACM, Computer Fraud & Security, IT Pro, IT Now, Network Security, Information Systems Frontier, Review of Business Information Systems and Campus-Wide Information Systems* as IS journals (see Table A1). I categorized non-IS journals to disciplines based on the journal's own assessment. For instance, I categorized the *American Journal of Economics and Business Administration* to the "economics" discipline because it "publishes original, innovative and novel work in various areas representing the intersection of economics as a scientific discipline and the professional practice of business management" (Science Publications, 2014). I categorized journals that target multiple disciplines as "multidisciplinary".

Table A1. List of Journals

IS (27 papers / 32.5%)	Non-IS (56 papers / 67.5%)
Campus-Wide Information Systems (1 / 1.2%)	*American Journal of Economics and Business Administration* (2 / 2.4%) (Economics)
Communications of the ACM (1 / 1.2%)	*American Water Works Association* (1 / 1.2%) (Multidisciplinary)
Communications of the Association for Information Systems (2 / 1.2%)	*Asian Social Science* (1 / 1.2%) (Multidisciplinary)
Computers & Security (1 / 1.2%)	*ASBM Journal of Management* (1 / 1.2%) (Management)
Computer Fraud & Security (4 / 4.8%)	*Australian Health Review* (1 / 1.2%) (Health care)
Decision Support Systems (1 / 1.2%)	*Bell Labs Technical Journal* (2 / 2.4%) (Multidisciplinary)
Information Management & Computer Security (3 / 3.6%)	*CPA Journal* (1 / 1.2%) (Multidisciplinary)
Information Systems Frontier (1 / 1.2%)	*Disaster Prevention & Management* (4 / 4.8%) (Multidisciplinary)
Information Systems Management (1 / 1.2%)	*Facilities* (1 /1.2%) (Multidisciplinary)
Information Security Journal: A Global Perspective (formerly *Information Systems Security*) (2 / 2.4%)	*IBM Systems Journal* (1 / 1.2%) (Information science)
International Journal of Information Management (1 / 1,2%)	*Industrial Management & Data Systems* (1 / 1.2%) (Multidisciplinary)
IT Now (2 / 2.4%)	*International Journal of Business Continuity and Risk Management* (2 / 2.4%) (Multidisciplinary)
IT Pro (1 / 1.2%)	*International Journal of Business and Social Science* (1 / 1.2%) (Multidisciplinary)
Network Security (5 / 6%)	*International Journal of Emergency Management* (1 / 1.2%) (Multidisciplinary
	International Journal of Information Systems for Crisis Response and Management (1 / 1.2%) (Crisis management)
	Internal Auditor (1 / 1.2%) (Internal auditing)
	Journal of Business Continuity & Emergency Planning (22 / 26.5%) (Multidisciplinary)
	Journal of Facilities Management (1 / 1.2%) (Facilities management)
	Journal of GXP Compliance (1 / 1.2%) (Multidisciplinary)
	Journal of Homeland Security and Emergency Management (2 / 2.4%) (Multidisciplinary)
	Journal of Organizational Excellence (1 / 1.2%) (Multidisciplinary)
	Journal of Universal Computer Science (1 / 1.2%) (Computer science)

Table A1. List of Journals

	Long Range Planning (1 / 1.2%) (Strategic management)
	Management Quarterly (1 / 1.2%) (Management)
	OCLC Systems & Services (1 / 1.2%) (Multidisciplinary)
	Risk Management: An International Journal (2 / 2.4%) (Multidisciplinary)
	Work Study (1 / 1.2%) (Multidisciplinary)

Appendix B: Research Approaches and Thematized Contributions

Table B1. Summary of Research Approaches and Themes

Theme	Author(s)	Year	Cases	Concept	Exp.	Interv.	Survey
Models	Iyer & Bandyopadhyay	2000		√			
	Nosworthy	2000		√			
	Lam	2002		√			
	Savage	2002		√			
	Smith	2003		√			
	Swartz et al.	2003	√				
	Botha & von Solms	2004		√			
	Cerullo & Cerullo	2004		√			
	Jrad et al.	2004		√			
	Shaw & Harrald	2004		√			
	Castillo	2005	√				
	Kendall et al.	2005		√			
	Cervone	2006	√				
	Gibb & Buchanan	2006		√			
	Power & Forte	2006		√			
	Alesi	2008	√				
	Dye	2008	√				
	Freestone & Lee	2008	√				
	Geelen-Baass & Johnstone	2008	√				
	Halliwell	2008	√				
	Sheth, McHugh, & Jones	2008		√			
	Thornton	2008	√				
	Turetken	2008		√			
	Vaid	2008		√			
	Alonaizan	2009	√				
	Devlen	2009		√			
	McLouglin	2009	√				
	Nollau	2009		√			
	Paton	2009		√			
	Wan	2009	√				
	Arduini & Morabito	2010		√			
	Lindström et al.	2010a	√				
	Lindström et al.	2010b		√			
	Shaw & Smith	2010		√			
	Tammineedi	2010		√			
	Karim	2011					√
	Järveläinen	2012				√	
	Moyer & Novick	2012		√			
	Sum	**38**	**13**	**23**	**0**	**1**	**1**
Salience	Alonso & Boucher	2001		√			
	Berman	2002	√				

Table B1. Summary of Research Approaches and Themes

	Hecht	2002	√				
	Herbane et al.	2004	√				
	Ernest-Jones	2005	√				
	Hinde	2005		√			
	Stanton	2005		√			
	Brettle	2006		√			
	Walker	2006	√				
	Windsor	2006		√			
	Messer	2009		√			
	Kite & Zucca	2007		√			
	Hunter	2008		√			
	Low et al.	2010					√
	Momami	2010		√			
	Pheng et al.	2010					√
	Streufert	2010	√				
	Baker	2012		√			
	Sum	**18**	**6**	**10**	**0**	**0**	**2**
Social	King	2003		√			
	Pitt & Goyal	2004					√
	Butler & Gray	2006		√			
	Shaw & Harrald	2006					√
	Rapaport & Kirschenbaum	2008					√
	Walch & Merante	2008		√			
	Seow	2009		√			
	Wong	2009		√			
	Sawalha & Anchor	2012		√			
	Sawalha et al.	2012		√			
	Sawalha & Meaton	2012		√			
	Sum	**11**	**0**	**8**	**0**	**0**	**3**
Technology	Ionescu	2002		√			
	Bertrand	2005		√			
	Bajgoric	2006		√			
	Roitz & Jackson	2006	√				
	van de Walle & Rutkowski	2006			√		
	Husband, R.	2007	√				
	Coullahan & Shepherd	2008		√			
	Lumpp et al.	2008		√			
	Bajgoric & Moon	2009		√			
	De Luzuriaga	2009	√				
	Bajgoric	2010		√			
	Asgary & Mousavi-Jahromi	2011					√
	Sapateiro et al.	2011				√	
	Bajgoric, N.	2012		√			

Table B1. Summary of Research Approaches and Themes

	Ceballos et al.	2012		√			
	Heng et al.	2012	√				
	Sum	**16**	**4**	**9**	**1**	**1**	**1**
Total		**83**	**23**	**51**	**1**	**2**	**7**

Appendix C: References of IS Continuity Papers

Table C1. List of Reviewed IS Continuity Papers

A-G	H-O	P-Z
Alesi, P. (2008). Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology. *Journal of Business Continuity & Emergency Planning*, *2*(3), 214-220. Alonaizan, A. (2009). Developing a business continuity programme at Arab National Bank. *Journal of Business Continuity & Emergency Planning,* *3*(3), 216-221. Alonso, F., & Boucher, J. (2001). Business continuity plans for disaster response. *The CPA Journal, 71*(11), 60. Arduini, F., & Morabito, V. (2010). Business continuity and the banking industry. *Communications of the ACM*, *53*(3), 121-125. Asgary, A., & Mousavi-Jahromi, Y. (2011). Power outage, Business Continuity and Businesses' Choices of Power Outage Mitigation Measures. *American Journal of Economics and Business Administration*, *3*(2), 312-320. Bajgoric, N. (2006). Information technologies for business continuity: an implementation framework. *Information Management & Computer Security*, *14*(5), 450-466. Bajgoric, N. (2010). Server operating environment for business continuance: framework for selection. *International Journal of Business Continuity and Risk Management*, *1*(4), 317-338. Bajgoric, N., & Moon, Y. B. (2009). Enhancing systems integration by incorporating business continuity drivers. *Industrial Management & Data Systems*, *109*(1), 74-97. Bajgoric, N. (2012). System administration for business continuity—the case of HP-UX operating system. *International Journal of Business Continuity and Risk Management*, *3*(1), 19-40. Baker, N. (2012). Enterprisewide Business continuity. *Internal Auditor, 69*(3), 36-40.	Halliwell, P. (2008). How to distinguish between" business as usual" and "significant business disruptions" and plan accordingly. *Journal of Business Continuity & Emergency Planning*, *2*(2), 118-127. Hecht, J. A. (2002). Business continuity management. *Communications of the Association for Information Systems*, *8*, 444-450. Heng, T., Hooi, S., Liang, Y., Othma, A., & San, O. (2012). Telecommuting for Business Continuity in a Non-profit Environment. *Asian Social Science, 8*(12), 226-237. Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: Time for a strategic role? *Long Range Planning*, *37*(5), 435-457. Hinde, S. (2005). From incidents to disasters. *Computer Fraud & Security*, *2005*(4), 17-19. Hunter, P. (2008). Eastern Internet outage brings customary boom in business continuity. *Computer Fraud & Security*, *2008*(3), 16-17. Husband, R. (2007). How John Lewis Partnership connected 200 business continuity plans to an emergency notification database. *Journal of Business Continuity & Emergency Planning, 1*(3), 261-270. Iyer, R. K., & Bandyopadhyay, K. (2000). Managing technology risks in the healthcare sector: disaster recovery and business continuity planning. *Disaster Prevention and Management*, *9*(4), 257-270. Ionescu, I. (2002). Secondary data – the Poor Relative of Business Continuity. *Network Security, 5*(31), 9-11. Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*(5), 332-349. Jrad, A., Morawski, T., & Spergel, L.	Paton, D. (2009). Business continuity during and after disaster: Building resilience through continuity planning and management. *ASBM Journal of Management*, *2*(2), 1-16. Pheng, L. S., Ying, L. J., & Kumaraswamy, M. (2010). Institutional compliance framework and business continuity management in mainland China, Hong Kong SAR and Singapore. *Disaster Prevention and Management*, *19*(5), 596-614. Pitt, M., & Goyal, S. (2004). Business continuity planning as a facilities management tool. *Facilities*, *22*(3/4), 87-99. Power, R., & Forte, D. (2006). You don't need a weatherman to know which way the wind blows: business continuity in the 21st century. *Computer Fraud & Security*, *2006*(8), 17-19. Rapaport, C., & Kirschenbaum, A. (2008). Business continuity as an adaptive social process. *International Journal of Emergency Management*, *5*(3/4), 338-347. Roitz, J., & Jackson, E. (2006). AT&T adds business continuity to the long list of telework's advantages. *Journal of Organizational Excellence*, *25*(2), 3-12. 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. Savage, M. (2002). Business continuity planning. *Work Study*, *51*(5), 254-261. Sawalha, I. H., & Anchor, J. R. (2012). Business continuity management in emerging markets: The case of Jordan. *Journal of Business Continuity & Emergency Planning*, *5*(4), 327-337. Sawalha, I. H., & Meaton, J. (2012). The Arabic culture of Jordan and its impacts on a wider Jordanian adoption of business continuity management. *Journal of Business Continuity &*

Table C1. List of Reviewed IS Continuity Papers

A-G	H-O	P-Z
Berman, A. (2002). Lessons learned: The aftermath of September 11. *Information Systems Security*, *11*(2), 30-37. Bertrand, C. (2005). Business continuity and mission critical applications. *Network Security*, *2005*(8), 9-11. Botha, J., & von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security*, *12*(4), 328-337. Brettle, P. (2006). Real world response to business continuity. *IT Now, 48*(2), 8-9. Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly*, *30*(2), 211-224. Castillo, C. (2005). Disaster preparedness and Business Continuity Planning at Boeing: An integrated model. *Journal of Facilities Management*, *3*(1), 8-26. Ceballos, J., DiPasquale, R. & Feldman R. (2012). Business continuity and security in datacenter interconnection. *Bell Labs Technical Journal*, *17*(3), 147-156. Cerullo, V. & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, *21*(3), 70-78. Cervone, F. (2006). Disaster recovery and continuity planning for digital library systems. *OCLC Systems & Services: International digital library perspective, 22*(3), 173-178. Coullahan, R. J., & Shepherd, C. D. (2008). Enhancing enterprise resilience in the commercial facilities sector. *Journal of Business Continuity & Emergency Planning*, *3*(1), 5-18. De Luzuriaga, J. (2009). Ensuring business continuity for business process outsourcing companies. *Journal of Business Continuity & Emergency Planning*, *3*(4), 312-316. Devlen, A. (2009). How to build a comprehensive business continuity programme for a healthcare	(2004). A Model for Quatifying Business Continuity Preparedness Risks for Telecommunications Networks. *Bell Labs Technical Journal, 9*(2), 107-123. Karim, A. J. (2011). Business disaster preparedness: An empirical study for measuring the factors of business continuity to face business disaster. *International Journal of Business and Social Science*, *2*(18), 18. Kendall, K. E., Kendall, J. E., & Lee, K. C. (2005). Understanding disaster recovery planning through a theatre metaphor: Rehearsing for a show that might never open. *Communications of the Association for Information Systems*, *16*, 51. King, D. L. (2003). Moving towards a business continuity culture. *Network Security*, *2003*(1), 12-17. Kite, C. S., & Zucca, G. S. (2007). How to access your Board/C-suite and make an effective case for business continuity investments. *Journal of Business Continuity & Emergency Planning*, *1*(4), 332-339. Lam, W. (2002). Ensuring business continuity. *IT Professional*, *4*(3), 19-25. Lindström, J., Harnesk, D., Laaksonen, E., & Niemimaa, M. (2010a). A methodology for inter-organizational emergency management continuity planning. *International Journal of Information Systems for Crisis Response and Management*, *2*(4), 1-19. Lindström, J., Samuelsson, S., & Hägerfors, A. (2010b). Business continuity planning methodology. *Disaster Prevention and Management*, *19*(2), 243-255. Low, S., Liu, J., & Sio, S. (2010). Business continuity management in large construction companies in Singapore. *Disaster Prevention and Management*, *19*(2), 219-232. Lumpp, Th., Schneider, J., Holtz, J., Mueller, M., Lenz, N., Biazetti, A., & Petersen, D. (2008). From high availability and disaster recovery to business continuity solutions. *IBM*	*Emergency Planning*, *6*(1), 84-95. Sawalha, I., Anchor, J., & Meaton, J. (2012). Business continuity management in Jordanian banks: Some cultural considerations. *Risk Management*, *14*(4), 301-324. Seow, K. (2009). Gaining senior executive commitment to business continuity: Motivators and reinforcers. *Journal of Business Continuity & Emergency Planning*, *3*(3), 201-208. Shaw, G., & Harrald, J. (2006). The core competencies required of executive level business crisis and continuity managers—the results. *Journal of Homeland Security and Emergency Management*, *3*(1), 1-34. Shaw, G. L., & Harrald, J. R. (2004). Identification of the Core Competencies Required of Executive Level Business Crisis and Continuity Managers. *Journal of Homeland Security and Emergency Management*, *1*(1), 1-14. Shaw, S., & Smith, N. (2010). Mitigating risks by integrating business continuity and security. *Journal of Business Continuity & Emergency Planning*, *4*(4), 329-337. Sheth, S., McHugh, J., & Jones, F. (2008). A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects. *Journal of Business Continuity & Emergency Planning*, *2*(2), 221-239. Smith, D. (2003). Business continuity and crisis management. *Management Quarterly*, 27-33. Stanton, R. (2005). Beyond disaster recovery: The benefits of business continuity. *Computer Fraud & Security*, *2005*(7), 18-19. Streufert, J. (2010). Business continuity strategies for cyber defence: Battling time and information overload. *Journal of Business Continuity & Emergency Planning, 4*(4), 303-316. Strong, B. (2010). Creating meaningful business continuity management program metrics. *Journal of Business*

Table C1. List of Reviewed IS Continuity Papers

A-G	H-O	P-Z
organisation. *Journal of Business Continuity & Emergency Planning*, *4*(1), 47-61. Dye, K., & Langsett, M. (2008). A roadmap to measure and achieve enterprise operational resiliency, *Journal of Business Continuity & Emergency Planning*, *3*(1), 38-46. Ernest-Jones, T. (2005). Business continuity strategy—the life line. *Network Security*, *2005*(8), 5-9. Freestone, M., & Lee, M. (2008). Planning for and surviving a BCM audit. *Journal of Business Continuity & Emergency Planning*, *2*(2), 138-151. Geelen-Baass, B. N., & Johnstone, J. M. (2008). Building resiliency: ensuring business continuity is on the health care agenda. *Australian Health Review*, *32*(1), 161-173. Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, *26*(2), 128-141.	*Systems Journal, 47*(4), 605-619. McLoughlin, R. (2009). What one must know about achieving BS25999-2 certification. *Journal of Business Continuity & Emergency Planning*, *3*(2), 105-111. Messer, I. (2009). Taking the business continuity programme to a corporate leadership role. *Journal of Business Continuity & Emergency Planning*, *4*(1), 8-13. Momani, N. M. (2010). Business continuity planning: Are we prepared for future disasters. *American Journal of Economics and Business Administration*, *2*(3), 272. Moyer, J., & Novick, K. (2012). Introducing a new resource for water and wastewater system business continuity planning. *American Water Works Association Journal*, *104*(3), 37-39. Nollau, B. (2009). Disaster recovery and business continuity. *Journal of GXP Compliance*, *13*(3), 51-58. Nosworthy, J. (2000). A practical risk analysis approach: managing BCM risk. *Computers & Security*, *19*(7), 596-614.	*Continuity & Emergency Planning, 4*(4), 360-367. Swartz, E., Elliott, D., & Herbane, B. (2003). Greater than the sum of its parts: Business continuity management in the UK finance Sector. *Risk Management*, *5*(1), 65-80. Tammineedi, R. L. (2010). Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective*, *19*(1), 36-50. Thornton, G. (2008). An innovative, flexible and workable business continuity plan: Case study of the Australian Customs Service Cargo BCP. *Journal of Business Continuity & Emergency Planning*, *3*(1), 47-54. Turetken, O. (2008). Is your back-up IT infrastructure in a safe location?: A multi-criteria approach to location analysis for business continuity facilities. *Information Systems Frontier, 10*(3), 375-383. Vaid, R. (2008). How are operational risk and business continuity coming together as a common risk management spectrum? *Journal of Business Continuity & Emergency Planning*, *2*(4), 330-339. Van de Walle, B., & Rutkowski, A. (2006). A fuzzy decision support system for IT service continuity threat assessment. *Decision support systems*, *42*(3), 1931-1943. Walch, D., & Merante, J. (2008). What is the appropriate business continuity management staff size? *Journal of Business Continuity & Emergency Planning*, *2*(2), 240-250. Walker, A. (2006). Business continuity and outsourcing—moves to take out the risk. *Network Security*, *2006*(5), 15-17. Wan, S. (2009). Service impact analysis using business continuity planning processes. *Campus-Wide Information Systems*, *26*(1), 20-42. Windsor, C. (2006). Business Continuity—is it expensive and hard?. *IT Now, 48*(2), 12-13.

Table C1. List of Reviewed IS Continuity Papers

A-G	H-O	P-Z
		Wong, W. N. Z. (2009). The strategic skills of business continuity managers: Putting business continuity management into corporate long-term planning. *Journal of Business Continuity & Emergency Planning*, *4*(1), 62-68.

About the Authors

Marko Niemimaa is a PhD candidate at the Turku Centre for Computer Sciences and University of Turku, Turku School of Economics in the department of Information Systems. He has started his PhD in 2010 and his main research interests lie in the discipline of IS security where he mainly focuses on business continuity and information security management. His publications have appeared in IS journals and conferences, such as *International Journal of Social and Organizational Dynamics in IT* (IJSODIT), *International Journal of Information Systems for Crisis Response and Management* (IJISCRAM), Hawaii International Conference on Systems Sciences (HICSS), and International Conference on Availability, Reliability and Security (ARES). He holds an MSc degree in information security and a BBA degree in business information systems. Prior to joining the academia, He has worked nearly 10 years in the industry as an information security professional and consultant. During those years he successfully led a team of technical information security professionals and managed various customer projects around the globe in developing and developed countries.