International Journal of Information Management 33 (2013) 583–590

Contents lists available at SciVerse ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

IT incidents and business impacts: Validating a framework for continuity management in information systems

Jonna Järveläinen*

Information Systems Science, Turku School of Economics, University of Turku, Rehtorinpellonkatu 3, FI-20014 University of Turku, Finland

ARTICLE INFO

Article history:
Available online 22 March 2013

Keywords:
Information system continuity management
Framework validation
Embeddedness
Management support

ABSTRACT

Information technology (IT) incidents that make data inaccessible may cause businesses to lose customers, reputation and market position. Previous studies on information management have identified data availability as a key priority, and the literature on disaster recovery and business continuity describes ways of preparing for and avoiding IT incidents. However, no frameworks for information system continuity management (ISCM) have yet been validated. This research draws on a framework for business continuity management, and extends it to the context of information systems. The framework is validated in a survey of IT managers and chief information officers in large private and public organisations operating in Finland. The results suggest that the embeddedness of continuity practices in an organisation has perceived business impacts whereas, in contradiction of previous theory, there is no such direct relation in the case of organisational alertness and preparedness. The theoretical contribution is to validate the ISCM framework statistically. On the practical level, social factors such as committed managers and employees are influential in decreasing negative business impacts. Further research on the embeddedness of continuity practices is called for.

1. Introduction

> Initial public offering of Facebook fails, due to "technical error" in Nasdaq trading system, which did not have enough capacity to handle all the trades. Thousands of unsatisfied traders, initial market price of the stock set too high, law suits pending (Pepitone, 2012).
>
> A million customers use the new ticketing system of a railway company overnight. The system crashes. Thousands of frustrated customers, the company is in the headlines for a week. It gets the lowest possible ranking in the national reputation survey the next year (Heiskanen, 2012).

Information technology (IT) and information system (IS) incidents affect business operations and, as many examples show, may also have severe business impacts. Organisations recognise IS continuity as a key information management issue (Luftman & Zadeh, 2011). The reliability of the technology and the systems is the primary objective of information management, although extremely complex systems do not always deliver perfectly (Butler & Gray, 2006; Mithas, Ramasubbu, & Sambamurthy, 2011). Ensuring continuous IT and IS operations is among the responsibilities of a firm's information security management (Fink, 1994; Gerber & Von Solms, 2005), although operations may be disrupted for non-security related reasons, too. One traditional approach to ensuring IT and IS continuity is through disaster recovery planning (DRP). Businesses have become convinced that they should make contingency plans for coping with IT and IS incidents, and ensure that backup copies are stored in a safe location (Chow & Ha, 2009; Turetken, 2008). Are these measures sufficient? Is it possible to avoid incidents?

This research draws on the proactive business continuity management framework developed by Herbane, Elliott, and Swartz (2004), and extends it to the context of information systems (for the sake of simplicity the term IS also includes the IT infrastructure and communications technology). Business continuity management has evolved from the notion of disaster recovery planning, combining practices from risk, crisis and supply chain management (Herbane et al., 2004). The focus in disaster recovery is on surviving IT incidents. This is broadened in business continuity management to include the identification and avoidance of potentially damaging incidents that would have a severe business impact (Herbane et al., 2004). It also offers useful tools for engaging top management in the discussion concerning the business implications of various operational incidents that are not necessarily security-related. The scope of continuity management spreads to all business operations, but it is argued here that its proactive application in the IS area could foster its evolution and increase the robustness of IT services.

The purpose of this research is to explore how organisations attempt to ensure IS continuity and thus minimise the possible

* Tel.: +358 2 333 9413; fax: +358 2 333 9800.
E-mail address: jonna.jarvelainen@utu.fi

0268-4012/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijinfomgt.2013.03.001

business impact of negative incidents. The literature refers to the exploitation of technical and social factors to minimise such impacts. Technical factors include plans and alternative arrangements that enhance organisational alertness and preparedness. Embedding continuity practices in the organisation refers to social factors such as the commitment of the personnel. However, despite findings in commercial and academic studies suggesting their crucial importance for chief information officers, no frameworks for business or IS continuity management have been validated academically (Ernst & Young, 2011; Luftman & Zadeh, 2011).

Thus, the research question addressed here is this. How do organisational alertness and preparedness, and the embedding of continuity practices affect the perceived business impacts of information systems continuity management (ISCM)? A survey of large companies operating in Finland was conducted in 2012 to validate a theoretical ISCM framework. The survey was sent to CIOs and IT managers responsible for ISCM in all organisations employing more than 250 persons. Given the low response rate (13.6%), further research is called for.

2. Theoretical background: ensuring continuity in information systems

The reliable delivery of data and information is indicative of the information management capability of an organisation (Mithas et al., 2011). However, according to Butler and Gray (2006), IS research often assumes the "best-case scenario", in other words that systems are reliable, although the reality is different. As earlier research has shown, ensuring the availability of information, in other words the continuity of information systems, is the responsibility of those responsible for information security (Von Solms & Von Solms, 2004), although IS incidents might also occur for reasons not related to security. Studies on IS risk management have focused on IS investments (Benaroch, Lichtenstein, & Robinson, 2006), projects (Barki, Rivard, & Talbot, 2001), outsourcing (Bahli & Rivard, 2003) and security (Straub & Welke, 1998), for example. Risk management studies recognise that technology might crash (Sherer & Alter, 2004), but the details are discussed elsewhere. Availability incidents were common in the early days of business computing, and disaster recovery planning (DRP) was developed to address that (Herbane, 2010a). According to Ernst & Young's Global Information Security Survey (Ernst & Young, 2011), organisations perceived business continuity management, or DRP, as the most probable information security investment area. The International Organisation for Standardisation and other bodies have developed several risk-management, business-continuity and information-security standards, but they have been criticised as too general for companies with specific business needs (Siponen & Willison, 2009). A more comprehensive approach than disaster recovery planning is needed. Given that post-disaster recovery may not be sufficient to avoid severe damage, there is a need for disaster prevention. It is not surprising, therefore, that business continuity management and IS reliability remain key issues in IS management (Luftman & Ben-Zvi, 2011; Luftman & Zadeh, 2011).

Business continuity management (BCM) is a socio-technical approach, the aim of which is to identify and prevent operational risks (Herbane et al., 2004). The concept stems from disaster recovery planning, and has evolved to include the management of all kinds of business incidents, such as supplier problems in manufacturing and major pandemics affecting operations (Herbane et al., 2004). As in risk and information security management, the first step in BCM is to identify assets, and threats and their probabilities, but the perspective covers not only information security and technical aspects, but also business issues (Gibb & Buchanan, 2006). Recognising and focusing on critical systems and IS resources is therefore crucial, although other systems are not to be ignored.

The emphasis in this study is on how organisations try to ensure continuity in their information systems. The aim is to test a business continuity framework based on crisis management in the IS context. Herbane et al. (2004) developed a framework, which has not been validated. They argue that recovery speed, resilience, the embeddedness of BCM practices and external obligations serve the organisation in terms of preserving its value. If a firm is able to recover from an IS incident more quickly than its competitors, it gains competitive advantage (Herbane et al., 2004). The framework is expanded here through the addition of management support.

Crises such as oil spills interrupt business operations, affect reputations and reduce the firm's market value (Coombs, 2007; Smith, Smith, & Kun, 2010). Similarly, when an IS incident occurs and continuity is disrupted, the operational work in part of the organisation stalls and the impact on the business is negative. If the incident affects customer service, for instance, it may also cause reputational damage. It has been found that service disruptions have significant negative effects on customer loyalty: one Nordic bank lost 30,000 customers because of a long-drawn-out incident during an IS merger (Luoma-aho & Paloviita, 2010; Wang, Wu, Lin, & Wang, 2010). Therefore the premise on which the paper builds is that IS incidents have a negative effect on the business.

In order to weaken the negative impact of IS incidents, organisations should prepare for them. In many countries, finance and health-care sectors are required to ensure continuity in IS operations according to governmental regulations (Elliott, Swartz, & Herbane, 2010). However, customers nowadays do not expect the delivery of products and services to be interrupted for any reason. They will soon use another web store if web pages do not load within a reasonable time, for instance (Parasuraman, Zeithaml, & Malhotra, 2005). Business-to-business customers in particular are very dependent on their suppliers, and therefore require assurances on matters such as compliance with continuity standards and audit reports before engaging in long-term strategic relationships (Choudhuri, Maguire, & Ojiako, 2009). External requirements imposed by government authorities and customers also motivate management to improve the continuity of information systems and technology (Herbane et al., 2004). Given that top management is ultimately responsible for IS continuity, it is in its interest to comply with external requirements that support the organisation in making improvements. It is therefore proposed that:

Hypothesis 1a. External requirements have a positive effect on management support.

The embeddedness of continuity practices facilitates the effective implementation of IS continuity management and requires stability and a clear organisational structure (Elliott et al., 2010). One way of embedding continuity in an organisation is to follow an international standard or framework that comprehensively integrates it into the processes. However, external requirements for continuity among customers and authorities tend to be based on international standards and frameworks (e.g., Information Technology Infrastructure Library, ITIL) or to closely resemble them (Järveläinen, 2012). In order to comply with a standard or framework organisations have to go through audits or analyses, which also makes continuity issues more visible to employees (Bernard, 2007; Gibb & Buchanan, 2006). Alesi (2008) calls for a resilient culture and continuity to be built into processes and everyday operations, thereby becoming part of everyone's work. Other useful techniques for strengthening employee commitment include reward systems, training, exercises and tailored communication (Alesi, 2008; Herbane et al., 2004; Puhakainen, 2006). External requirements integrate continuity into organisations in a more comprehensive way, hence the following hypothesis:

Hypothesis 1b. External requirements have a positive effect on the embeddedness of continuity practices.

Recovery speed after an incident depends on how quickly the organisation identifies the incident and how well it is prepared (Herbane et al., 2004). Organisational alertness and preparedness are easily improved if managers allocate resources and decide to implement back-up plans and form crisis teams, for example (Herbane et al., 2004). It is also essential that top management takes responsibility for and requires regular reports on continuity issues (Ivancevich, Hermanson, & Smith, 1998; Seow, 2009; Wong, Monaco, & Sellaro, 1994). However, if top management assigns responsibility to the IT department, chief information officers (CIOs) may not sufficiently emphasise organisational alertness or preparedness. It is therefore proposed that:

Hypothesis 2a. Management support has a positive effect on organisational alertness and preparedness.

Another technique is to embed IS continuity in organisational practices, and to make sure that employees and management in other departments understand its importance (Alesi, 2008; Morwood, 1998). Instead of giving the sales director responsibility for every information system in the IT department, it might be more beneficial to make him or her responsible for the customer relationship management system and its continuity. Awareness of and responsibility for IS continuity would therefore extend beyond the IT department (Herbane et al., 2004). If top management supports the embedding of IS continuity practices throughout a company, heightened awareness and commitment would become part of the organisational culture for everyone (Alesi, 2008). Hence the following hypothesis:

Hypothesis 2b. Management support has a positive effect on the embeddedness of continuity practices.

Continuity depends to a great extent on the ability of an organisation to avoid and quickly recover from incidents. A firm that is able to quickly recognise potential risks and notify the crisis team is said to be high in organisational alertness (Herbane et al., 2004). Preparedness refers to familiarity with various recovery methods and the avoidance of risks, such as having continuity plans, forming crisis teams and building in key-person redundancy (Ahmad, Hadgkiss, & Ruighaver, 2012; Chow & Ha, 2009; Lindström, Samuelsson, & Hägerfors, 2010). The plans should be regularly tested and updated, even after major incidents (Gibb & Buchanan, 2006). Preparedness is strengthened if critical systems can be recovered by one of several persons (Conlon & Smith, 2010). An essential element is recognising the critical systems with the help of business impact analysis, identifying the dependencies between internal and external systems, and requiring IS service suppliers to follow continuity practices (Blos, Hui-Ming, & Yang, 2010; Herbane et al., 2004). Plans, analyses and continuity processes involve employees other than IT experts, and thus preparedness will affect the embeddedness of the practices (Herbane et al., 2004). It is therefore proposed that:

Hypothesis 3a. Organisational alertness and preparedness have a positive effect on the embeddedness of continuity practices.

As Herbane et al. (2004) suggest, organisational alertness and preparedness have business impacts. There are a number of examples in the areas of supply chain management and information systems, for instance, of incidents that have had significant impacts (Luoma-aho & Paloviita, 2010; Sheffi & Rice, 2005; Starr, Newfrock, & Delurey, 2003). It is therefore proposed that:

Hypothesis 3b. Organisational alertness and preparedness have a positive effect on perceived business impacts.

When an organisation is prepared and practices are included in processes – and employees, business units as well as managers are fully committed – continuity practices are said to be embedded (Herbane et al., 2004). Their embeddedness will have business impacts in that they will make the organisation more robust, and better able to avoid incidents and to recover more quickly than its rivals. It is therefore proposed that:

Hypothesis 4. The embeddedness of continuity practices has a positive effect on perceived business impacts.

The research model to be tested is presented in Fig. 1.

3. Methodology

Given the aim of this study to validate the theoretical framework, a quantitative survey is suitable (Pinsonneault & Kraemer, 1993). The data was collected in February 2012. The variables were operationalised in accordance with the literature (see Appendix A). Most of the survey items were based on Chow and Ha's (2009) paper on disaster recovery planning, and Herbane et al. (2004), although some were developed from a previous qualitative study and worded in line with other items in the construct. Seven academics pretested the questionnaire first, after which six CIOs, who were the target population, did a second test and suggested adding some items. A five-point Likert scale was used for all of the variables (1 = totally agree, 5 = totally disagree): Appendix A also presents the mean values of all the items.

The respondents to the final survey were selected from a database of managers understood to be the highest ranking persons responsible for the IT function (CIOs 26.6%, IT managers 72%), who were employed in large organisations (1,186 organisations employing at least 250 persons, Official Statistics of Finland (2010) definition). Large organisations were assumed to have sufficiently advanced continuity practices compared to the more narrow focus in small companies (Herbane, 2010b). The total number of organisations in the population that had provided contact details for their CIO or similar was 630 (corporations being counted as one organisation).

The covering letter mentioned that the respondent should be the CIO or the person responsible for information systems continuity management on the assumption that this would be the most knowledgeable person on the subject on the managerial level. A web-based survey was sent to them by 11 of the e-mail addresses were no longer in use. After two reminders 84 responses had been received, an effective response rate of 13.6 per cent. This is common for information security surveys (Kotulic & Clark, 2004).

The respondents were mostly IT managers (50%) and CIOs (31%), but there were also some chief (information) security officers (7.2%), a risk manager and technical personnel (e.g., an IT architect and a head of information and communications technology applications). The distribution of respondents correlated with the titles presented in the initial database quite well. On average they spent 8.6 per cent of their time on IS continuity (range 0–90%), and had an average of 7.7 years of experience in that position (range 1–28 years). In order to assess non-response bias the industry sectors, the number of employees and the turnover of the companies in the population were compared with the respondent data: the respondents appeared to be a representative sample and no systematic error was found. Table 1 gives details of the respondent organisations.

All the items are reflective in nature, in that they reflect the phenomenon from different perspectives, share a common theme and do not "cause" the construct (Jarvis, MacKenzie, & Podsakoff, 2003). Furthermore, given the gap in research on continuity management in information systems, it was not feasible to draw up a

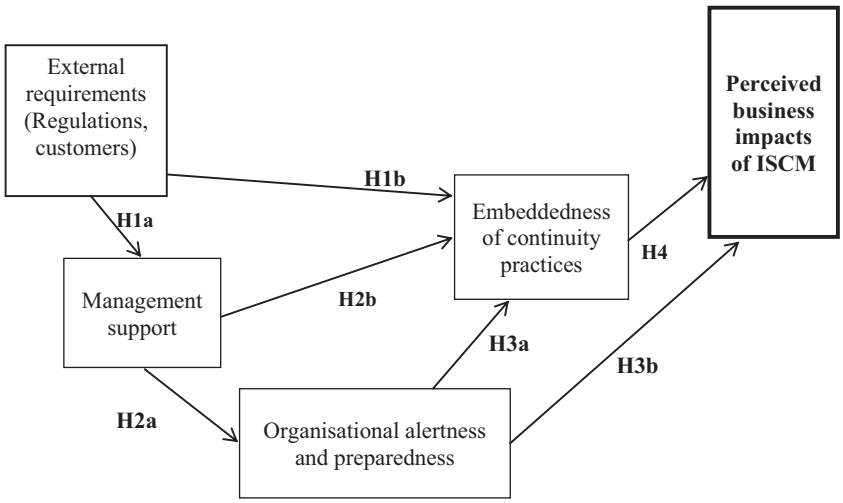

Fig. 1. A framework for information systems continuity management.

comprehensive list of construct items, and in this case a formative construct made sense.

The items with excessively low factor loadings (below 0.7, see Fornell & Larcker, 1981) were not included in the analysis. For instance, almost all the respondents "totally agreed" with the items "Files, databases and servers are backed up regularly" and "Our communication works well in incident situations".

Table 1
Descriptives of the respondent organisations.

Variable	Categories	*N*
Sector (N/A 1)	Public sector	31
	Manufacturing	22
	Services	30
Employees (N/A 2)	≥500	27
	501–1000	23
	1001–6000	23
	≤6001	9
Turnover/public funding (N/A 4)	≥100 M€	30
	101–200 M€	17
	201–700 M€	18
	≤701 M€	15
Employees in the IT department (N/A 1)	≥50	69
	51–500	10
	≤501	4
Outsourced, out of IT (N/A 4)	0–25%	40
	26–50%	13
	51–75%	10
	76–100%	
Outsourced	Infrastructure	59% of companies
	Personal computers, laptops, other equipment	30.1%
	Networks	74.7%
	Critical IS	56.6%
	Other IS	61.4%
	Printing services	31.3%
	Help desk services	38.6%
	IT management, information security and enterprise architecture	16.9%
	Telephone and audio visual services	57.8%
Software as a Service, out of IT (N/A 4)	0	31
	1–10%	39
	11–20%	6
	21–70%	4

As Table 2 shows, the composite reliabilities are all over 0.7 and the average variance extracted (AVE) of each construct is above 0.5 (Hair, Ringle, & Sarstedt, 2011). The Cronbach's alpha of External requirements is somewhat low, being dependent on the number of items (in this case only two). In Table 3, the AVE is greater than any squared correlation with the construct, and the cross loadings are relatively small between the items. Therefore the discriminant validity is also good. The convergent validity of the model is appropriate in that all the t-values of the significant relationships are over 1.96; in fact, most of them are over 2.576 (see Fig. 2). Thus, the reflective constructs express sufficient internal consistency, discriminant and convergent validity.

4. Results and discussion

This paper sets out to answer the research question of how organisational alertness and preparedness, and the embeddedness of continuity practices affect the perceived business impacts of ISC management. The general BCM framework developed by Herbane et al. (2004) is applied in the IS context in order to find an answer.

Because the data set is small and not normally distributed (Gefen, Straub, & Rigdon, 2011) the analysis is based on the partial least squares method, with SmartPLS 2.0 software (Ringle, Wende, & Will, 2005). There were some missing values (1–2/variable), which were replaced by the mean replacement algorithm provided by SmartPLS. Fig. 2 illustrates the tested model.

The model explains 37.1 per cent of the variation in the perceived business impacts of ISCM. It is affected by the embeddedness of the practices, in accordance with the hypothesis. Nearly all the posited relationships (H1a, H2a, H2b, H3a, H4) are supported, with the exception that external requirements (H1b) do not affect the embeddedness of continuity practices. In addition, there is no

Table 2
Composite reliabilities (C.R.), Cronbach's alpha and average variance extracted (AVE) values for the constructs.

Variable	AVE	C.R.	Cronbach's alpha
Perceived business impacts	.6390	.8761	.8159
Management support	.6579	.9199	.8950
Organisational alertness and preparedness	.5808	.9325	.9194
Embeddedness of continuity practices	.6224	.8681	.7968
External requirements	.6530	.7891	.4773

Table 3
Squared latent variable correlations between the constructs: the AVE of each construct is shown in the diagonal from 1 to 5.

	1	2	3	4	5
(1) Perceived business impacts	.7993				
(2) Management support	.4677	.8111			
(3) Organisational alertness and preparedness	.4431	.6887	.7621		
(4) Embeddedness of continuity practices	.6091	.6976	.5998	.7889	
(5) External requirements	.4092	.3835	.3174	.4149	.8081

direct relationship between organisational alertness and preparedness (H3b) and perceived business impacts. However, because the model only explains 37.1 per cent of the variation, it seems that other variables might also have an effect.

There is a statistically significant correlation between external requirements (government and customer) and management support, demonstrating that – in industries with such requirements – the respondents believed that their top management provided good continuity support. However, given that external requirements do not correlate statistically significantly with the embeddedness of practices, it is not clear whether or not they affect continuity practices. Examination of the item means to see how organisations try to ensure continuity showed agreement among most of the respondents that top management was committed to ensuring continuity, and supported its development. However, there was seldom any requirement for regular ISCM reports, which might indicate that top management trusts IT managers to manage continuity, that there have been no major incidents, or that continuity is not considered important enough to warrant regular reports (Seow, 2009). The last-mentioned option is the most dangerous, because it could also affect the commitment of employees.

There were significant relationships between management support and both organisational alertness and preparedness as well as the embeddedness of continuity practices. This shows the importance of top-management support for IS continuity management (Alesi, 2008; Herbane et al., 2004; Morwood, 1998). Organisational alertness also turned out to influence embeddedness but, contrary to the findings of Herbane et al. (2004), this was not statistically significant in relation to perceived business impacts. Upon close examination of the item means it seems that organisations prepare well technically. The respondents agreed on the need for regular backing up, and with providing alternatives for critical IS, for example. The mean of almost all items measuring organisational alertness and preparedness is below 3, indicating that most of the respondents agreed with the statements. The exception is that the plans are not tested regularly in all organisations, which could render them impractical and useless (Gibb & Buchanan, 2006).

Finally, the embeddedness of continuity practices correlated statistically significantly with perceived business impacts, indicating that technical preparedness in the IT department is not enough to make an impact. The means of the embeddedness items in the survey varied greatly. Many of them were above three, indicating that most of the respondents did not agree with the statements, and the social aspect of continuity was not emphasised as much as the technical aspects. In particular, offering rewards for improving ISCM and training employees was not popular among the respondent organisations, although the literature recommends these practices (Herbane et al., 2004). However, the respondents believed that all employees knew their responsibilities, and that the business units and departments were committed to continuity. One explanation for this contradiction could be that the organisations have managed to involve employees in continuity planning, for instance, which is therefore a common target and no training or rewards are needed. The respondents also agreed that good ISCM practices had led to a reduction in business interruptions, indicating that measures taken to ensure continuity minimise adverse business impacts.

Several other models were tested, too, such as whether or not external requirements have an effect on perceived business impacts, as Herbane et al. (2004) suggest. However, the only statistically significant relationship was that IS incidents do have perceived business impacts. This confirms the premise of the study, but is not included in the model. Although the finding might seem trivial, it is important to know that IS continuity managers realise that IS incidents should be minimised. Organisational alertness and preparedness were separated in the initial testing to form the variables originally suggested by Herbane et al. (2004), namely recovery speed and resilience. Later on they were combined in a single variable because the covariance between them was so high, and conceptually they were also very close: there were some items referring to plans in both.

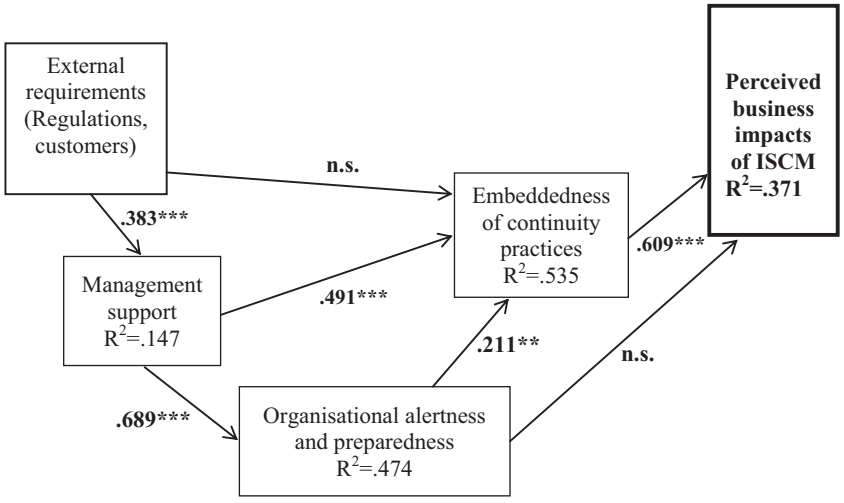

Fig. 2. The test results: $^{**}t > 1.96$, $^{***}t > 2.576$.

5. Conclusions

This paper expands understanding of IS continuity management in validating a framework that shows how organisational alertness and preparedness, and the embeddedness of continuity practices affect the perceived business impacts of ISC management, and that improvement in these areas could minimise the negative impacts. Moreover, top-management support is a key factor. External requirements from customers and government regulations may motivate top management to enhance continuity. Furthermore, the findings of this study indicate that the embeddedness of continuity practices is essential in minimising the impacts, and that a purely technical approach is insufficient because commitment to and awareness of continuity are required on every organisational level.

The item means were further examined in order to shed light on how organisations tried to ensure IS continuity and thus to minimise the potential business impacts of IS incidents. The respondent organisations placed special emphasis on technical areas in increasing alertness and preparedness. Given that the planning of recovery from technical disasters, and the benefits thereof, have been familiar to organisations for decades, this is not surprising. However, there was considerable variance in the social aspect – the embeddedness of continuity practices – and most of the respondents did not agree with many of the statements. Most of the items were based on the literature, some of which may still be too advanced for Finnish organisations. Embeddedness should thus be studied further, and longitudinal research is called for.

The theoretical contribution of the paper is the validation of the framework, which connects findings from earlier literature and identifies new insights. According to the original framework, the business impacts come from recovery speed, resilience, the embeddedness of practices and legal obligations. This was extended in terms of separating management support from the embeddedness of continuity practices, combining recovery speed and resilience into one construct, and extending legal obligations to include customer requirements in the construct covering external requirements. The amended framework explained 37.1 per cent of the variation in the data, and nearly all the relationships were supported. In contrast to the findings reported in Herbane et al. (2004), the only construct showing a direct positive relationship with perceived business impacts was the embeddedness of continuity practices, the others showing only indirect relationships.

This paper emphasises the comprehensive approach to IS continuity in showing that it depends on many stakeholders in addition to the IT department. Continuous IS operations require top-management support, committed business units and employees, and organisational alertness and preparedness. In the light of this study it seems that the implementation of purely technically oriented IS continuity would be insufficient. External requirements from customers and regulators also have an essential role in strengthening top-management support, which otherwise might be difficult to achieve despite its importance (Ivancevich et al., 1998; Wong et al., 1994). However, given that external requirements did not correlate significantly with the embeddedness of continuity practices, it seems that the impact is limited and that the requirements might not have an effect in terms of reducing IS incidents, which was impossible to measure in this study. Therefore, the question remains. Are regulations really necessary for improving continuity in organisations, or are customer requirements sufficient?

The most significant practical contribution of this paper is that it highlights the essential role of embeddedness in continuity practices. Organisational alertness and preparedness, in the form of plans, recovery speed and resilient practices are insufficient in terms of influencing business, and it is necessary to incorporate continuity-related practices on all levels and processes. Improvement actions and managerial support increase awareness of continuity matters and help to embed practices into processes, creating a continuity-oriented environment. From the management perspective the organisation can then avoid, or then survive IS incidents, thus the perceived business impacts will be positive. This finding points to the fact that IT and business experts should have a good relationship, and that business managers should understand the value of IS. Furthermore, customer-service employees should be able to communicate with customers when IS incidents occur in a way that does not negatively affect their loyalty.

This is only one framework, but it opens up the discussion on the business impacts of IS incidents and how organisations could prevent them. The full scope of such impacts remains unclear, although this and many other studies suggest that they relate to reputational damage and customer dissatisfaction (e.g. Luoma-aho & Paloviita, 2010; Pepitone, 2012). Mithas et al. (2011), for example, found a direct relationship between information management and both financial as well as human-resource performance. However, the testing was carried out in one country and the response rate was low, thus any statistical generalizability should be cautious: future research is required.

The limitations of the study include the low response rate to the survey, the geographically homogenous group of respondents and common variance bias. It would be useful to carry out further studies and tests comparing different countries, for instance, and to collect information from customers of respondent companies.

Acknowledgement

I would like to thank professor Pia Arenius for her valuable input during the development of the questionnaire and all the pre-testers of the survey for their comments.

Appendix A. Questionnaire items

Variable	Item (5-point Likert scale, unless otherwise indicated)	Source[a]	Mean	S.D.[b]	F.L.[c]
Perceived business impacts of ISCM	**Good ISCM practices have facilitated customer acquisitions**	H	2.79	.86	.80
	We have achieved competitive advantage with the help of good ISCM practices	H	2.73	.83	.81
	We have been able to keep our market position with the help of good ISCM practices.	H	2.62	.87	.67
	Good ISCM practices have contributed to the growth of our company.	Q	2.88	.80	.62
	Good ISCM practices have improved our reputation from the perspective of customers	Q	2.35	.88	.84
	We have been able to survive in the market with the help of good ISCM practices	H	2.59	.89	.75
	Good ISCM practices have decreased business disruptions, which could not have been predicted.	P	1.91	.83	.62

Variable	Item (5-point Likert scale, unless otherwise indicated)	Source[a]	Mean	S.D.[b]	F.L.[c]
Embeddedness of continuity practices	Responsibility for business continuity planning has been decentralised to the business units.	H	2.82	1.11	.35
	The business units have coordinators for business continuity management (BCM).	H	3.37	1.15	.61
	Our business units are committed to BCM	H	2.62	.85	.82
	Our business units encourage each other to practise good BCM	H	3.08	.95	.76
	Our staff members know the continuity practices related to their own work	H	2.73	.87	.83
	Our staff members are committed to pursuing disruption-free operations.	H	1.94	.89	.58
	We have studied the commitment of our staff to BCM.	P	3.89	1.05	.63
	The relevant personnel are members of the recovery team (IT, business, etc.)	C	2.71	1.22	.75
	Any employee who has improved BCM or ISCM may be rewarded.	H	3.55	1.21	.61
	BCM and ISCM experts are rewarded in accordance with developments.	H	3.93	1.00	.67
	The personnel receive systematic training in BCM and ISCM.	C	3.40	1.17	.69
Organisational alertness and preparedness	We have conducted a thorough risk analysis for IT.	H	2.21	.92	.59
	We have conducted a systematic business-impact analysis for IT	H	2.96	1.26	.70
	We have surveyed sufficiently internal and external dependence between information systems (e.g., how the sales system connects to other systems)	H	2.48	1.02	.80
	We have imposed adequate ISCM and BCM requirements on our suppliers	H	2.24	.95	.77
	Creating a continuity plan is an integral part of developing a new product or service	H	2.43	1.14	.70
	We have alternative systems for critical IT.	C	2.20	1.09	.56
	We have one or more alternative key persons	C	2.43	1.15	.72
	There is an alternative for our critical facilities.	C	2.92	1.14	.54
	There is an alternative for critical business processes in our organisation.	H	2.91	.99	.58
	Our communication works well in incident situations.	H	2.21	.85	.52
	The crisis team can manage recovery from an incident quickly	H	2.31	.99	.76
	Files, databases and servers are backed up regularly.	C	1.10	.33	.21
	We regularly test the recovery of data from backups.	C	2.20	1.04	.48
	We regularly test our ISCM plan by auditing or simulating an incident.	C	3.05	1.20	.75
	Our ISCM and BCM plans are updated regularly.	C	2.60	1.12	.80
	We have documented continuity plans regarding our business processes.	C	3.17	.90	.71
	We have documented continuity plans for our information systems and infrastructure.	C	2.83	1.00	.85
	We have documented DRPs for our information systems and infrastructure.	C	2.76	1.03	.76
	We have documented disaster-recovery principles for our information systems and infrastructure.	C	2.62	1.22	.67
Management support	**Top management provides adequate financial and human-resource support for ISCM.**	C	2.77	.94	.86
	Top management commits to ISCM.	C	2.46	1.02	.73
	Top management supports the development of ISCM.	C	2.56	.95	.78
	Top management assumes ultimate responsibility for ISCM.	C	2.66	1.11	.79
	Top management requires regular ISCM reports.	C	3.27	1.11	.89
	Top management participates in ISCM projects, seminars and training.	C	3.52	1.02	.80
External requirements	We develop ISCM to improve our customer service.	Q	2.48	1.07	.61
	We develop ISCM because of customer requirements.	Q	2.93	1.02	.74
	We develop ISCM because of legal or governmental requirements.	H	2.24	1.01	.87
	We develop ISCM because of corporate HQ requirements.	Q	2.93	1.13	.56
	We develop ISCM to improve our reputation from a customer perspective.	Q	2.33	.95	.65
	We develop ISCM to improve our position in relation to our competitors.	H	2.84	1.11	.61
	We develop ISCM in order to survive in an extremely competitive environment.	H	2.73	1.13	.61

The items in bold were included in the PLS model.

[a] H = (Herbane et al., 2004); C = (Chow & Ha, 2009); Q = (previous qualitative study, not yet published); P = (pre-testing suggestion).

[b] Standard deviation.

[c] Factor loading in PLS.

References

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. http://dx.doi.org/10.1016/j.cose.2012.04.001

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.

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: A transaction cost and agency theory-based perspective. *Journal of Information Technology*, *18*(3), 211–221. http://dx.doi.org/10.1080/0268396032000130214

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems*, *17*(4), 37–69.

Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: An empirical validation of risk-option relationships. *MIS Quarterly*, *30*(4), 827–864.

Bernard, R. (2007). Information lifecycle security risk assessment: A tool for closing security gaps. *Computers & Security*, *26*(1), 26–30. http://dx.doi.org/10.1016/j.cose.2006.12.005

Blos, M. F., Hui-Ming, W., & Yang, J. (2010). Analysing the external supply chain risk driver competitiveness: A risk mitigation framework and business continuity plan. *Journal of Business Continuity & Emergency Planning*, *4*(4), 368–374.

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

Choudhuri, B., Maguire, S., & Ojiako, U. (2009). Revisiting learning outcomes from market led ICT outsourcing. *Business Process Management Journal*, *15*(4), 569–587.

Chow, W. S., & Ha, W. O. (2009). Determinants of the critical success factor of disaster recovery planning for information systems. *Information Management & Computer Security*, *17*(3), 248–275. http://dx.doi.org/10.1108/09685220910978103

Conlon, R., & Smith, R. V. (2010). The role of the board and the CEO in ensuring business continuity. *Financial Executive*, *26*(9), 52–55.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163–176. http://dx.doi.org/10.1057/palgrave.crr.1550049

Elliott, D., Swartz, E., & Herbane, B. (2010). *Business continuity management: A crisis management approach* (2nd ed.). NY, USA: Routledge.

Ernst & Young. (2011). Into the cloud, out of the fog: Ernst & Young's 2011 Global Information Security Survey. Retrieved from http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf

Fink, D. (1994). A security framework for information systems outsourcing. *Information Management & Computer Security*, *2*(4), 3–8. http://dx.doi.org/10.1108/09685229410068235

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Gefen, D., Straub, D., & Rigdon, E. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, *35*(2), iii–xiv.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16–30. http://dx.doi.org/10.1016/j.cose.2004.11.002

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, *26*(2), 128–141. http://dx.doi.org/10.1016/j.ijinfomgt.2005.11.008

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *The Journal of Marketing Theory and Practice*, *19*(2), 139–152. http://dx.doi.org/10.2753/MTP 1069-6679190202

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

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

Herbane, B., Elliott, D., & Swartz, E. (2004). Business continuity management: Time for a strategic role? *Long Range Planning*, *37*(5), 435–457. http://dx.doi.org/10.1016/j.lrp.2004.07.011

Ivancevich, D. M., Hermanson, D. R., & Smith, L. M. (1998). The association of perceived disaster recovery plan strength with organizational characteristics. *Journal of Information Systems*, *12*(1), 31.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*(5), 332–349. http://dx.doi.org/10.1108/09685221211286511

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, *30*(2), 199–218. http://dx.doi.org/10.1086/376806

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597–607, doi:16/j.im.2003.08.001.

Lindström, J., Samuelsson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management*, *19*(2), 243–255. http://dx.doi.org/10.1108/09653561011038039

Luftman, J., & Ben-Zvi, T. (2011). Key issues for IT executives 2011: Cautious optimism in uncertain economic times. *MIS Quarterly Executive*, *10*(4), 203–212.

Luftman, J., & Zadeh, H. S. (2011). Key information technology and management issues 2010–2011: an international study. *Journal of Information Technology*, *26*(3), 193–204. http://dx.doi.org/10.1057/jit.2011.3

Luoma-aho, V., & Paloviita, A. (2010). Actor-networking stakeholder theory for today's corporate communications. *Corporate Communications: An International Journal*, *15*(1), 49–67. http://dx.doi.org/10.1108/13563281011016831

Mithas, S., Ramasubbu, N., & Sambamurthy, V. (2011). How information management capability influences firm performance. *MIS Quarterly*, *35*(1), 137–A15.

Morwood, G. (1998). Business continuity: Awareness and training programmes. *Information Management & Computer Security*, *6*(1) http://dx.doi.org/10.1108/09685229810207425, 28–28–32

Official Statistics of Finland. (2010). Finnish enterprises 2009 (e-publication). Helsinki: Statistics Finland. Retrieved from http://www.tilastokeskus.fi/til/syr/2009/syr_2009_2010-11-26_fi.pdf

Parasuraman, A., Zeithaml, V. A., & Malhotra, A. (2005). E-S-QUAL: A multiple-item scale for assessing electronic service quality. *Journal of Service Research*, *7*(3), 213–233. http://dx.doi.org/10.1177/1094670504271156

Pepitone, J. (2012). Facebook: IPO debacle was Nasdaq's fault. CNNMoney. Retrieved from http://money.cnn.com/2012/06/15/technology/facebook-ipo-lawsuit/index.htm

Pinsonneault, A., & Kraemer, K. L. (1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems*, *10*(2), 75–105.

Puhakainen, P. (2006). *A design theory for information security awareness, Doctoral dissertation*. Acta Universitatis Ouluensis. Series A, Scientiae rerum naturalium.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS 2.0 (beta). Hamburg, Germany: SmartPLS. Retrieved from http://www.smartpls.de

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

Sheffi, Y., & Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, *47*(1), 41–48.

Sherer, S. A., & Alter, S. (2004). Information Systems Risks and Risk Factors: Are They Mostly About Information Systems? Communications of the Association for Information Systems, 14(1). Retrieved from http://aisel.aisnet.org/cais/vol14/iss1/2

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270, doi:16/j.im.2008.12.007

Smith, K. T., Smith, M., & Kun, Wang. (2010). Does brand management of corporate reputation translate into higher market value? *Journal of Strategic Marketing*, *18*(3), 201–221. http://dx.doi.org/10.1080/09652540903537030

Starr, R., Newfrock, J., & Delurey, M. (2003). Enterprise resilience: managing risk in the networked economy. *Strategy and Business*, *30*(Spring), 70L 79.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. http://dx.doi.org/10.2307/249551

Turetken, O. (2008). Is your back-up IT infrastructure in a safe location? *Information Systems Frontiers*, *10*(3), 375–383.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376, doi:16/j.cose.2004.05.002.

Wang, Y. S., Wu, S. C., Lin, H. H., & Wang, Y. Y. (2010). The relationship of service failure severity, service recovery justice and perceived switching costs with customer loyalty in the context of e-tailing. *International Journal of Information Management*, *31*(4), 350–359.

Wong, B. K., Monaco, J. A., & Sellaro, C. L. (1994). Disaster recovery planning: Suggestions to top management and information systems managers. *Journal of Systems Management*, *45*(5), 28.

Jonna Järveläinen is a Senior Research Fellow in Information Systems Science, Turku School of Economics at University of Turku. She defended her thesis on e-business in 2004, and has since studied e-government, mobile technology adoption and implementation. Currently she is researching business continuity management research. She has published in for example in *Information Management & Computer Security*, *Journal of Organisational Computing and Electronic Commerce*, *International Journal of Electronic Government Research and Electronic Markets* and many conference proceedings.