# Understanding the Stakeholder Roles in Business Continuity Management Practices – A Study in Public Sector

Jonna Järveläinen
Turku School of Economics, University of Turku
jonna.jarvelainen@utu.fi

## Abstract

*Natural disasters, power cuts and fires do not discriminate, but they happen to both private and public organizations. Prior literature has agreed that business continuity management (BCM) requires commitment from all levels of an organization. However, the roles of different internal and external stakeholders in BCM practices has not been discussed in prior literature. This study focuses on BCM stakeholders in continuity practices in the public sector. We report the results of a qualitative case study with 16 interviews. The support from senior management was wanted, IT experts were valued, the role of users was not deemed important, and external service providers were trusted partners but also considered "the biggest headaches" by the interviewed managers.*

## 1. Introduction

*"Since we do not have large interruptions, the [department heads] just assume that [continuity] is an issue someone else manages, and it works, so why should they [care]. Just like water comes from the tap, it just does."* - Interviewee

Engaging employees and managers in business continuity is probably as hard as motivating people to see the importance of information security; unless some incident happens, they do not care. Serious disruptions in IT services tend to catch the attention of senior management, since disruptions might lead to substantial reputational damage and have business impacts [21, 30]. Therefore, many companies nowadays consider business continuity a critical IT issue along with information security issues [18].

Business impacts of risks are used in prioritizing critical systems and processes, and based on those analyses, the business continuity management (BCM) proactively prepares and aims to avoid possible incidents in organizations [15] Also public sector uses BCM to avoid operational interruptions [17, 35].

Prior research has concluded that embedding BCM into organizations requires engagement from internal and external stakeholders [15, 16]. In private companies, we have seen that continuity culture of an organization improves the embeddedness of BCM [29] and we know that technical experts create the continuity of digital infrastructures [24]. Thus, it would be interesting to understand the role of different stakeholders in BCM of IT services also in the public sector.

Managers responsible for BCM have a central view to the BCM area and can encourage the involvement of stakeholders. Understanding their perspective could thus lead us to see how BCM could be embedded in the whole organization. Hence, this paper extends the prior literature by focusing on *how managers responsible for BCM see the roles of different stakeholders in BCM practices in the public sector?*

This paper reports the findings from interviews of 16 public sector organizations in Finland. We identify five different stakeholder groups, top and middle management, IT experts, users and external service providers, which have varied roles in BCM practices.

## 2. Business continuity management

Prior research in information security (ISsec) and information systems has recognized that one of its aims is to ensure business continuity [8, 11]. There are a number of risks related to information systems and information communications and technology (ICT), and business impact analysis of critical processes and IT resources can help to prevent interruptions [28]. Operational interruptions may occur due to many reasons: natural disasters [19], epidemic diseases affecting human resources [33], ISsec incidents [9], technical break downs etc.

BCM aims to proactively avoid operational interruptions in critical business processes with socio-technical solutions [15]. Disaster recovery and business continuity planning studies have presented several

URI: https://hdl.handle.net/10125/63980
978-0-9981331-3-3

ways to technically avoid or mitigate interruptions [6, 14]. Back-ups, infrastructure and facility redundancy have been found important [34] while disaster identification, preparedness and an organizational recovery team further ensure operational recovery [31]. Several business continuity planning methods emphasize business impact analysis, planning, testing, training employees and the cyclic nature of planning to improve organizational resilience [22].

Since the aim is to ensure the continuity of business operations, the business focus and organization-wide perspective of BCM is significant, in contrast to mere IS perspective [3]. Therefore, it is essential that senior management takes responsibility of BCM [9, 17]. Butler and Gray [5] have emphasized that reliable IS requires routines and mindful behavior on operational and management levels as well as in system design. Embedded processes and practicing of continuity are central along with traditional technical solutions [23].

Business continuity has been recognized valuable for organizations also in other disciplines; resilience, robustness and disruption management have been studied e.g. in supply chain management [27] societal safety [13], economic resilience of areas [4]. The survival of private and public organizations after natural and man-made crises has been discussed also in the crisis and emergency management field [2, 7].

Prior literature has reported BCM problems in public sector [1], and earlier some concerns have been raised for public sector BCM such as senior management not implementing appropriate continuity risk analyses [35], not having sufficient continuity controls for ICT [20] or not creating business continuity plans [32]. After major natural disasters, the interest in continuity issues seems to increase in the public sector [26]. Yet, the prior research on public sector BCM has not discussed the role of different stakeholders in BCM to the best of our knowledge.

It has been noticed that when IT management initiates organizational BCM, the commitment of other stakeholders is not guaranteed [25]. The embeddedness of BCM practices and their impact seem to be connected and the senior management commitment drives the BCM implementation in organizations [17]. In fact, if senior management is not aware and controlling BCM, then the consequences for instance in hacking situations may be severe [9]. Embeddedness and continuity culture can be created with BCM practices [29], but how are different stakeholder groups involved in these practices has not been studied in the public sector. A comprehensive stakeholder perspective is also missing from private sector although scattered results focusing on the part of senior and IT management in BCM as well as service providers exist [15, 16, 36].

## 3. Research approach and context

In order to study stakeholders and BCM practices in the public sector, we decided to take a qualitative case study approach. We decided to aim for maximum variation in sampling [10] and find diverse public sector organizations from the state, provincial and local level in Finland. We sought the web sites of different organizations for contact details of IT managers, who might be knowledgeable in BCM. All interviewees were approached with personalized emails including high-level interview themes by two researchers.

**Table 1. Interviewees and their organizations.**

| | Organisation type | Personnel in whole organisation | IT-staff | Interviewee |
|---|---|---|---|---|
| A | Governmental organisation | 200 | 7 | CIO |
| B | Governmental organisation | 520 | N/A | Leading expert |
| C | Governmental organisation | 5500 | 150 | ISsec manager |
| D | Governmental organisation | 6000 | 500 | CIO |
| E | Municipality | 500 | 4 | IT manager |
| F | Municipality | 900 | 6 | IT operations manager |
| G | Municipality | 950 | 4 | IT manager |
| H | Municipality | 1500 | 10 | CIO |
| I | Higher education institution | 520 * | 16 | CIO |
| J | Higher education institution | 1200 * | 30 + | CIO and system maintenance manager |
| K | Higher education institution | 3000 * | 250 | ISsec manager |
| L | Higher education institution | 3500 * | 75 | ISsec manager |
| M | Service organisation | 330 | N/A | ISsec manager |
| N | Service organisation | 7000 | N/A | CIO |
| O | Research organisation | 560 | N/A | IT manager |
| P | Research organisation | 750 | N/A | Group manager |

* including staff, but excluding students

From the state level, we chose different governmental, state-funded research and service organizations. From the provincial level, we chose different universities or polytechnics representing higher education institutions and from the local level, we targeted municipalities. We were able to get 16 interviews, one with two interviewees (see details in Table 1).

The variation of BCM practices was wide in the data set. There were three organizations, which had very mature BCM practices with 24/7 operations, data centers in several locations, highly interested top management, regularly updated continuity and recovery plans for all systems and regular testing schedules. Other organizations had almost all quite robust technical BCM approaches and crisis communication, but the interviewees reported either lack of BCM awareness among top or middle management or partial or non-existent continuity plans or testing practices.

Table 2 presents the data structure and coding scheme created based on the analysis. The analysis began by reading the transcripts thoroughly, but open mindedly, to get a sense of the complete set. Some narratives started to catch the reader's attention, a general recurring theme seemed to be an awareness or cognition of some ideal state of continuity, which had not been achieved by most organizations, but to which many interviewees still compared their organization. First, the author started to color code the texts into "issues that had not been done" (compared with the ideal state) and "issues that were well done". Another recurring theme was actor related issues and situation descriptions. All of these were carefully marked to a visual mindmap tool (XMind), and then reorganized into some themes and more detailed concepts behind aggregated categories of "Not done", "Well done", "Descriptions". However, after initial analysis, similar themes emerged on both sides (Not/well done) and the original categorization was reorganized.

After combining the "not done" and "well done" categories, it started to become clear that interviewees were concerned not only with several stakeholders, and practices, but also technical issues and legal issues (which are now out of the scope of this paper). Therefore, the author focused on finding the passages and codes related to stakeholders and practices from the analysis mindmap. The codes were then reorganized to five different stakeholder groups, and three practices, which emerged from the data.

**Table 2. Coding scheme of the data set.**

| Coding sample | Codes | Themes | Interesting issues |
|---|---|---|---|
| "… we have monthly [reporting]. We have an internal ISsec forum, where we have the related key persons from management. [To] top management, now it goes via IT manager. So those issues, s/he sees necessary to bring to awareness of top management, s/he does [present in senior management group]." [C, p.10] | Support | Top management | Stakeholders |
| "continuity and ISsec related [return on investment] calculations are really difficult to do [for top management]." [E, p.10] | Problems | | |
| "We have the [IT] production steering group once a week, so big ones and small ones, one could say that all interruptions are [discussed] there."[M, p.10] | Task force | Middle management | |
| "Since we do not have large interruptions, the [department heads] just assume that [continuity] is an issue someone else manages, and it works, so why should they [care]." [C, p.11] | Lack of awareness | | |
| "On-call duty team […] has a quite high skill requirement to be accepted in, since one has to be able to absorb new information." [L, p.12] | Teams | Experts | |
| "Since we have a small and established team, so we haven't even done, and there isn't any […] detailed plan, but everybody knows what has to be done." [J, p.7] | Instead of detailed plans | | |
| "There must be countless number of services of which we probably do not know – and those are used by a smaller group, who have organized the services for themselves ... users just use whatever they like." [J, p.3] | Awareness | Users | |
| "When the e-prescription project started, it [e-training] was obligatory for all in the social and healthcare sector to pass before they could use the system." [F, p.11] | Training | | |

| | | | |
|---|---|---|---|
| “We have taken this farthest with this certain service provider, we have practiced it with more than a decade, so once every four years we ask for new tenders and we always improve [the continuity requirements in the contract] and the process.” [I, p.4] | Contracts | External service providers | |
| “We cannot afford a server expert, since there would not be enough tasks for him all the time, only when there is a fault.” [G, p.5] | Reasons to use | | |
| “When we have several providers, and everyone informs us that they have checked their area and there was not any problems there. And the situation still is that somewhere is a problem. So that is the biggest headache of a service integrator, how to handle that.” [C, p.8] | Problems | | |
| “No, about information [systems]. But we have, have done a risk analysis on the organizational level. But related to information management.” [G, p.9] | Risk analyses | Planning | Practices |
| “[Service] provider most often is this [governmental office] and then we have those commercial providers. They do the plans, which system owner then approves.” [A, p.4] | Continuity plans | | |
| “Every year we agree on certain objects to be checked, and this back-up process has been one, not annually, but once in a while we have tested it, and certain other components we have went through.” [O, p.5] | Partial testing | Testing | |
| “Not in that sense, we have not tested them, like we would turn the big handle in the data center - without any warning power would be cut off from one data center and then we would see how it turns out. Well, once in a disruption situation when a UPS broke in a room.”[P, p. 5] | Full testing | | |
| “Actually, Facebook once used with this, since Our Communications [department] uses Facebook, because they informed that [service provider]’s data center had an incident. It was of course a little bit poor message in Facebook, since the [provider] did not necessary want to be mentioned.” [K, p.9] | In disruption situations | Communi-cation | |

## 4. Findings and discussion

### 4.1 Stakeholders

In prior literature, managers are considered important for BCM [9, 17]. In our study, IT management also discussed the role of top and middle management, experts, users and external service providers. After all, many organizations had outsourced fully or partially their IT services.

Commitment of top management was valuable for IT managers. This was apparent in the interviews, when top managers required regular BCM reporting and the reports were actually not only a formality, but studied too.

*“[The reports] are not just for reading, but s/he actually reads them and asks questions [about them].”* [M, p.15]

If top management did not require regular reporting or continuity planning, then interviewees wondered whether management understood the importance of IT service continuity.

*“It is obvious that in this kind of a hierarchical organization where there is a general director, and then departmental directors […] that of course those issues, the general director sees as important and current, those issues s/he will delegate to her/his subordinates.”* [C, p.11]

The support from top management was therefore considered vital for organizational commitment, and “selling” of this BCM agenda was sometimes necessary in order to gain the support.

Another stakeholder group was the middle management. Sometimes regular reporting was targeted for a special IT or ISsec task force consisting of middle management, and top management was informed only when the chairperson of the task force considered it meaningful. This kind of discussion forum supporting decision-making seemed essential for IT managers, since if some organization lacked a task force, the manager had to make decisions and fight the organizational windmills single-handedly for resources.

The middle managers sometimes were not aware of the significance of BCM. Some interviewee had noticed that department heads had the notion that continuity was the responsibility of “someone else”, since the systems seemed to be working and in disruption situations, IT department carried out the operational recovery. Another interviewee had even tried to create SLAs with other departments, which did not want to take responsibility for prioritizing systems based on criticality or costs of continuous IT operations.

The role of middle management was varied in organizations. Based on the data set, other IT managers considered the middle managers as valuable companions in the taskforces. Others had to survive by themselves and give equal service to all departments since the middle management did not care for continuity issues.

Another important group was the experts, who were considered being “*top-of-the-line professionals*” [L, p.7] and sometimes were used as auditors for external suppliers, since many had auditor qualifications (CISA etc.). When the experts had long experience from the same organization, they were so reliable that some even considered continuity plans unnecessary, because the expert team knew their job so well. They were also committed, one interviewee told about an incident when the air conditioning of a data center broke down and the spare parts came from Denmark with some delay. During the delay, they organized operations manually, requiring manual labor every morning and evening during the weekend. Although the IT team normally operated 8 hours on weekdays, the team still came every morning and evening to help their manager to ensure IT operations for those 5 days.

However, since some organizations were in the middle of an outsourcing process, they had some concerns about whether the same kind of service quality could be maintained after their experts had been moved to the service provider.

*“It has been based on that the people really well know what they are doing. On their expertise. But in the future, the maintaining people might not know [the systems] in a similar way [for example] that one cannot pull that cord.”* [O, p.9]

A knowledgeable IT team was valuable and the reliability of the external service provider was questionable at least, since this organization was just in the middle of outsourcing their IT services. To summarize, expertise was respected and it seemed that all interviewees trusted their IT teams, and they took the personnel risk so seriously that they had “stuntmen and women” for key people, so the operations would not be disrupted because of holidays or illnesses.

Users were mentioned as the fourth stakeholder group. Since many of the interviewees were also responsible for ISsec, the familiar “user is the weakest link” argument was used. A normal user probably had no idea of continuity management, if they had not been involved in BCM planning, but “*the others are perhaps somehow aware of the [continuity] issue, it is like any other issue, which is not part of my tasks.*” [C, p.10]

Most organizations had conducted ISsec training online or otherwise, and they required staff to sign ISsec policies and sometimes their supervisors even tested their ISsec knowledge. However, apart from the top three organizations, the organizations struggled with how basic users should be trained in BCM issues. In the less mature organizations, interviewees were certain that their technical monitoring of devices (by service providers or by themselves) was sufficient for continuity management and no particular training to increase continuity awareness was required.

The “top” organizations had a clear incident reporting system for normal users in place *“[They report] to their supervisor or his/her supervisor, […] or use centralized reporting, which goes automatically to our ISsec team.”* [D, p.11]. In the other organizations, the helpdesk treated the user reported incidents or transferred them to experts. One organization provided a 40-50 page online document for all users to explain all alternative processes and systems for service failure situations. Another organization also monitored the network traffic constantly and every year caught an employee doing some forbidden activity. This kind of monitoring was not possible for instance in higher education institutions, where staff had versatile research areas and required access everywhere.

Users as a stakeholder group were discussed in rather indifferent tone; they were not really important to be informed about continuity and technical equipment alarmed experts when needed even without user reports. This is contradictory to prior research, which encourages general awareness and embeddedness of continuity issues throughout the organization [29].

External service providers, the fifth stakeholder group, were a central concern of almost all interviews, more so than any other group, probably because the organizations had either fully or partially outsourced their IT services. Reason for outsourcing was related to lack of expertise and resources in their own organization: “*When the old environment was at the end of its lifecycle, […] we got an offer from [local public service provider], […] they would provide the service, build the environment and had pricing options for smaller to large organizations. […] The price was so [low] that we had to look at it twice to believe it*

*[…] and they would provide service 24/7.”* [G, p.4] Many public organizations operate with limited funding and when people have retired, they have not hired replacements. In this kind of scenario, it is a sound decision to outsource IT services, if it is possible to get expertise with a minimal cost from a specialized service provider.

Many smaller organizations accepted standard contract terms for outsourcing since they did not have more power to gain better terms. If they asked for sanctions for service level agreement (SLA) breaches, the prices would increase significantly, so most organizations did not ask for them. One interviewee told about a major storm that affected power distribution in the whole southern Finland. The interviewee worked in a small organization and had bought in advance some extra maintenance hours (guaranteed fixing of a problem in 8 hours) from a network operator as a precaution and decided to use those hours for the storm damages. However, the operator would not allow using those hours, since they had to ensure network services for larger organizations first: *“They didn’t care for [the contract] at all. They just would not fix it. […] Even if they hadn’t prepared for [the storm] and their resources were not enough, so they thought ‘ok, there will be some yelling later, but do we want some yelling from Hospital X or the Small organization’. So of course they think that the small organization does not matter.*”[E, p.7] After this incident, the smaller organization decided to start network cooperation with a larger organization in the same area, so together they would have better bargaining power with the network operator.

Organizations often had requirements for continuity in SLAs and ISsec requirements were considered critical by some organizations. However, one interviewee pointed out that all of their contracts had force major terms, so 100% reliability was not a possibility. Some organizations did not have any exit plans, for possible problems with the service provider, some had two providers for most critical services. They did audits for the service providers or at least had started to make them and aimed to do them always for new providers. Many providers automatically monitored their clients’ services and fixed them before any problems were visible at the client end. Still, some interviewees indicated that their role as an IT service integrator was difficult when many components of certain systems were outsourced to various providers. During service interruptions, it often happened that all service providers were confident that their services were running correctly, but the problem still persisted. Then interviewees had to organize all the providers into the same negotiation table to solve the situation, which was time-consuming.

From continuity perspective, the organizations had good service from their service providers, but not so much negotiation power, which then affected major incident management. But service providers seemed trustworthy partners based on their experiences. The general tone of voice regarding service provider activities was mostly neutral or even positive in the interviews.

## 4.2 Stakeholder roles in continuity practices

Interviewees discussed five stakeholder groups: top and middle management, IT experts, users and external service providers. We identified several BCM practices: risk analyzing, continuity planning, testing, training, reporting and communicating in crisis situations.

Continuity planning was discussed extensively during interviews and first phase of planning in BCM is business impact analysis or risk analysis [12]. In some organizations, IT department had done risk analyses by themselves and some not so systematically or at all, for example, if a general risk assessment had been done on the organizational level. *“Yes, [in the document template] if I remember right, is some kind of heading for risks, but it has not been for example done with any particular risk method.”* [L, p.9]. Organizational input to risk analysis was rarely mentioned in the interviews. So it seems that the only stakeholders interested in BCM risk analysis were the IT experts themselves.

There was a lot of variation in continuity plans and planning. Some lacked BCM plans, since they had a good IT team, or used their current resources in some other project like mapping of the enterprise architecture. Several interviewees stated that they had disaster recovery plans or legally required preparedness plans instead of continuity plans. Some had extensive system documentation otherwise, which was maintained regularly and covered continuity and recovery issues, so they did not need separate plans. In this case, the system owner was responsible for updating of the documentation also after incidents, so there was an incentive to keep it up to date, otherwise, people would call the system owner whenever there was a problem.

IT team or department, sometimes in cooperation with middle (departmental) managers, often did the plans themselves. The continuity plans made by departments were not perfect in the beginning: *“It is worth being a realist, and this is organizational learning. Just like in any other learning, such as when small schoolchildren do their first crafts project, it is rarely good. That is not the point; the point is just to do one. Then you do a second [one], and another and* *your skills improve all the time. So I think this same analogy applies to risk analysis and continuity plans."* [C, p.6]

The role of top management was vital for planning. If they had not required planning, plans were not written. If the management was interested in continuity, then the maintenance of the plans would be regular. One interviewee from the healthcare sector told that since the organization discussed and reported all medical incidents and near-misses into software for organizational learning purposes. Recently, they had acquired an extension to the system to report also ISsec related incidents and near-misses. The idea was not to blame anyone, but discussion in order to learn and improve processes. Incident-centered reporting was common in other organizations too, but not all organizations required regular reporting for top management.

Although IT department and experts carried the major workload of continuity planning and risk analysis, top management support was influential and middle management occasionally participated in creating the plans. In prior literature, planning was an important opportunity to create BCM awareness and commitment among employees and managers [25, 29]. Thus, the embeddedness of BCM practices was not probably improved in these organizations, since other stakeholder groups had minimal part in the planning phase.

Since many organizations had outsourced their IT services partially or fully, sometimes all IT team could do was to communicate situation to users via the intranet, emails and text messages. Quick communication and guidance of users to check common information sources when they noticed problems ensured that *"the investigating experts have a peaceful working situation. They are working feverishly and most often there are more than one party [investigating]: there might be network operators, software developer companies, [office]'s people and experts from the [system] owner."* [A, p.6] Communication between organization and external service providers was, as already mentioned, sometimes a "headache", since all parties avoided responsibility.

This kind of inter-organizational investigation required efficient communication processes. Interviewees often had clear communication plans for IT incident situations, but since they were in the public sector and had legal requirements also for large crises, the experiences from exercises had shown that sometimes they might need megaphones or other analog means for communicating. *"We had a simulated situation that a train carrying gas had exploded […] and there was a power cut […] and then we tried to figure out how to communicate, since you could not use any electric equipment and we thought where can we get megaphones and generators."* [E, p.5]

Escalating risks made top management interested, since then a possibility of reputation damage increased. When larger crises were imaginable, IT managers informed top management and were ready to contact communications department to manage the external communication to the media. Department heads and other middle management were contacted if affected, for example, when dependencies between different systems were noticed. Therefore, it seems that communication processes were quite effective and if some problems had been experienced before, they had learned their lessons and improved their processes. Communicating to all possible stakeholder groups was the responsibility of IT experts, but in crisis situations top management would be facing the cameras.

As already mentioned above, training was focused on ISsec and not on continuity management. This was provided for users, but in these interviews the systematic training of middle or senior management was not mentioned. However, we can consider the previous example of involving department managers yearly in improving continuity plans as some kind of training. Perhaps interviewees also believed that reporting of continuity issues educates the senior management in such extent that more training is not necessary.

Testing was mainly a task for IT experts, occasionally in co-operation with external service providers. A recurring theme when discussing testing of IT services was that interviewees seemed to quickly admit that they have not done a full testing, when asked about the testing of continuity plans. *"The recovery tests have been done before new systems are implemented [in production environment]. […] But such catastrophe tests, to suddenly pull the [power] plug out from some datacenter, we haven't had the courage yet [for that]."* [P, p.11] This same answer was repeated so often that we started to wonder how had they got an idea for full testing being the norm, since it was clearly not.

One interviewee explained that they had an external audit for their own continuity management system that declared multiple small improvement areas. Only then they understood that a full testing in their data center would be beneficial. The external audit company was responsible also for planning the test due later that year. They used regular partial tests for certain processes and were able to switch to their second data center without any client-facing problems for a long time. This narrative led us to conclude that external auditors recommended these full tests. However, based on this data set, we cannot know whether all clients are encouraged to do a full test, since the scope of testing is dependent on organizational environment and their expected service quality.

We also discussed the testing of back-up recovery. Since recovery from back-ups was rather frequent activity, many interviewees did not see the point of further testing. Back-up recovery however did create awareness of this basic BCM practice, back-ups, at all levels of the organization.

Testing is also a BCM practice that could be used for creating awareness and commitment for BCM in all stakeholder groups [29]. This opportunity is missed in the studied organizations, but back-up recovery, which was discussed in the same context during interviews, could have similar effect on users.

The reporting of continuity issues, as already mentioned, was incident-centered in most organizations and involved top and middle management internally. IT management regularly received reports from service providers. Therefore, reporting involved all the necessary stakeholder groups.

## 5. Conclusions

This paper set out to understand *how managers responsible for BCM see the roles of different stakeholders in BCM practices in public sector*. We extended the prior literature by finding the stakeholders and BCM practices from the interviews of managers responsible of BCM of IT services in 16 organizations. A comprehensive study on all relevant stakeholder groups according to managers responsible of BCM has not been published before to best of our knowledge [see also 22]. We identified five different stakeholder groups, which had some kind of central role in BCM practices (see table 3). In addition to these, the interviewees from public sector also discussed legal requirements and laws, but since the laws were specific to Finland, we decided not to discuss them in more detail. Since the interviewees were mostly from IT department, the role of IT experts as actors is emphasized in the results. Also the role of external service providers was evident, since most of the represented organizations had either partially or fully outsourced their IT services, including development and maintenance. The role of internal stakeholders was not so significant as actors, but their assistance was sometimes needed, support was welcomed and occasionally, in interruptions, they had to be informed.

Contrary to prior literature [29], the IT managers did not emphasize continuity culture or general BCM awareness among users, which leads us to rethink users as a significant stakeholder group. In the age of information overload it seems perhaps an utopian dream that end-users would be concerned about continuity. As long as the IT services work, users do regular back-ups and they know who to contact in disruption situations and understand the impact of information security policy compliance, the need for raising awareness of continuity issues for all users might be unnecessary.

**Table 3. Stakeholder roles in continuity management practices**

| Practices | Top management | Middle management | IT experts | Users | External service providers |
|---|---|---|---|---|---|
| Risk analyses | | Sometimes discussing in taskforces | Executing | | Sometimes executing |
| Continuity planning and plan maintenance | Support or not | Sometimes executing | Executing | | Sometimes executing |
| Communication in crises | Towards media if larger incident and possible risk to reputation | Informed if effects to their operations | Towards users, management and service providers | Informing about incidents and reading information about them | Towards IT experts |
| Training | | | Executing | Participating | |
| Testing | (Back-up recovery creates awareness) | (Back-up recovery creates awareness) | Executing | (Back-up recovery creates awareness) | Executing and participating in planning |
| BCM Reporting | Reading | In taskforces | Writing and reading | | Writing |

The role of top and middle management has been recognized in prior literature, at least in the private sector [9, 15]. Contrary to prior research [15], middle management was not as involved in BCM planning as they should have been, and some were also not keen to take responsibility of continuity issues at all. IT managers require support also from department heads and other middle management to understand the business impacts of different systems. Taskforces, where continuity incidents and issues are discussed, could be suitable arenas for engaging middle management in BCM. Prior literature has noticed that if IT management initiates the BCM project in an organization, the commitment of others might be hard to gain, at least in the private sector [25]. Although this data set did not reveal this kind of behavior, some commitment issues were observed in middle management.

One interesting finding was also that IT team seemed to have such a meaning for IT managers that they might disregard BCM planning totally. Similar findings have been reported in small, private sector companies [25]. However, this strategy might not be advisable in the public sector, especially if they have legal obligations to public.

Based on our analysis, in addition to top management and IT experts themselves, middle managers and external service providers have a central role in BCM practices. Since external service providers are most often bound by formal contracts and financial arrangements, their interest towards BCM is quite assured. Yet, the commitment problems of middle management in some organizations and the benefits of their involvement in taskforces suggest that more effort in engaging middle managers in BCM is needed.

Second contribution of this paper is that this study represents public sector organizations, which have been rather neglected in the BCM literature, although the crisis, disaster and incident management studies are more common. Laws required preparedness for crises from these public organizations, but the daily operations had also smaller incidents to manage for which many had prepared with different practices.

Third contribution is practical. Involving management to BCM practices, such as planning, testing and training creates awareness of BCM, which has not been the case in these organizations. It can be exhausting task to “sell” BCM without support from other members in the organization, at least until some major disruption happens. Therefore, it is highly recommended to start embedding BCM practices into organizations, since it also affects the perceived business impacts [15, 17, 29].

There were several limitations in this study. First, it was conducted in Finland and thus generalizability of results to other countries require further study. Second, there was only one representative from all but one target organization, and although they were responsible for BCM, their viewpoint is rather limited. Therefore, a study involving several stakeholder groups from each organization would validate these findings. Third, methodologically an interview has its limits, and it can be argued whether the interviewees gave an objective account. In this study, we try to see these interviews as peaking holes into those organizations and interviewees, not take them as facts, which would need more data to be credible.

## 6. References

[1] Abdullah, N., and E. Nuraihan Mior Ibrahim, “Contributing Factor to Business Continuity Management (BCM) Failure - A Case of Malaysia Public Sector”, *Proceedings of the 5 th International Conference on Computing and Informatics, ICOCI 2015 11-12 August, 2015 Istanbul, Turkey.*, (2015).

[2] Alonso, F., J. Boucher, and R.H. Colson, “Business Continuity Plans for Disaster Response”, *CPA Journal 71*(11), 2001, pp. 60.

[3] Arduini, F., and V. Morabito, “Business Continuity and the Banking Industry.”, *Communications of the ACM 53*(3), 2010, pp. 121–125.

[4] Baba, H., T. Watanabe, M. Nagaishi, and H. Matsumoto, “Area Business Continuity Management, a New Opportunity for Building Economic Resilience”, *Procedia Economics and Finance 18*, 2014, pp. 296–303.

[5] Butler, B.S., and P.H. Gray, “Reliability, mindfulness, and information systems”, *MIS Quarterly 30*(2), 2006, pp. 211.

[6] Chow, W.S., and W.O. Ha, “Determinants of the critical success factor of disaster recovery planning for information systems”, *Information Management & Computer Security 17*(3), 2009, pp. 248–275.

[7] Dietch, E.A., and C.M. Corey, “Predicting long-term business recovery four years after Hurricane Katrina”, *Management Research Review 34*(3), 2011, pp. 311–324.

[8] Fink, D., “A Security Framework for Information Systems Outsourcing”, *Information Management & Computer Security 2*(4), 1994, pp. 3–8.

[9] Fischbacher-Smith, D., “When organisational effectiveness fails”, *Journal of Organizational Effectiveness: People and Performance 4*(1), 2017, pp. 89–107.

[10] Flick, U., *An Introduction to Qualitative Research*, SAGE Publications, 2002.

[11] Gerber, M., and R. von Solms, “Management of risk in the information age”, *Computers & Security*

*24*(1), 2005, pp. 16–30.

[12] Gibb, F., and S. Buchanan, “A framework for business continuity management”, *International Journal of Information Management 26*(2), 2006, pp. 128–141.

[13] Hassel, H., and A. Cedergren, “Exploring the Conceptual Foundation of Continuity Management in the Context of Societal Safety”, *Risk Analysis*, 2019.

[14] Herbane, B., “The evolution of business continuity management: A historical review of practices and drivers”, *Business History 52*(6), 2010, pp. 978–1002.

[15] Herbane, B., D. Elliott, and E. Swartz, “Business Continuity Management: time for a strategic role?”, *Long Range Planning 37*(5), 2004, pp. 435–457.

[16] Järveläinen, J., “Information security and business continuity management in interorganizational IT relationships”, *Information Management &amp; Computer Security 20*(5), 2012, pp. 332–349.

[17] Järveläinen, J., “IT incidents and business impacts: Validating a framework for continuity management in information systems”, *International Journal of Information Management 33*(3), 2013, pp. 583–590.

[18] Kappelman, L., R. Torres, E. McLean, C. Maurer, V. Johnson, and K. Kim, “The 2018 SIM IT Issues and Trends Study”, *MIS Quarterly Executive 18*(1), 2019, pp. 51–84.

[19] Kato, M., and T. Charoenrat, “Business continuity management of small and medium sized enterprises: Evidence from Thailand”, *International Journal of Disaster Risk Reduction 27*, 2018, pp. 577–587.

[20] Koen, R., R. Von Solms, and M. Gerber, “ICT Readiness for Business Continuity in local government”, *Proceedings of 2016 IST-Africa Week Conference*, IEEE (2016), 1–11.

[21] Luoma-aho, V., and A. Paloviita, “Actor-networking stakeholder theory for today’s corporate communications”, *Corporate Communications: An International Journal 15*(1), 2010, pp. 49–67.

[22] Niemimaa, M., “Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework”, *Communications of the Association for Information Systems 37*(1), 2015.

[23] Niemimaa, M., “Extending ‘Toolbox’ of Business Continuity Approaches: Towards Practicing Continuity”, *AMCIS 2015 Proceedings*, 2015.

[24] Niemimaa, M., “Entanglement of Infrastructures and Action: Exploring the Material Foundations of Technicians’ Work in Smart Infrastructure Context”, *ICIS 2016 Proceedings*, 2016.

[25] Niemimaa, M., and J. Järveläinen, “IT service continuity: Achieving embeddedness through planning”, *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, (2013), 333–340.

[26] Al Omari, L., P.H. Barnes, and G. Pitman, “Optimising COBIT 5 for IT governance : examples from the public sector”, *Proceedings of the ATISR 2012 : 2nd International Conference on Applied and Theoretical Information Systems Research (2nd. ATISR2012)*, 2012.

[27] Pereira, J. V, “The new supply chain’s frontier: Information management”, *International Journal of Information Management 29*(5), 2009, pp. 372–379.

[28] Salmela, H., “Analysing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach”, *Journal of Information Technology 23*(3), 2008, pp. 185–202.

[29] Sawalha, I.H.S., J.R. Anchor, and J. Meaton, “Continuity Culture: A Key Factor for Building Resilience and Sound Recovery Capabilities”, *International Journal of Disaster Risk Science 6*(4), 2015, pp. 428–437.

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

[31] Shropshire, J., and C. Kadlec, “Developing the IT disaster recovery planning construct”, *Journal of Information Technology Management 20*(4), 2009, pp. 37.

[32] Smith, S., R. Jamieson, and D. Winchester, “An Action Research Program to Improve Information Systems Security Compliance across Government Agencies”, *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, IEEE (2007), 99–99.

[33] Supriadi, L.S.R., and L. Sui Pheng, “Business Continuity Management (BCM)”, In Springer, Singapore, 2018, 41–73.

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

[35] Warren, C.M.J., “The role of public sector asset managers in responding to climate change: Disaster and business continuity planning”, *Property Management 28*(4), 2010, pp. 245–256.

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