Bouncing Back after a Crisis: Lessons from Senior Management Team to Drive IS Resilience

Amitrajit Sarkar
University of Canterbury, NZ
Amit.Sarkar@ara.ac.nz

Stephen Wingreen
University of Canterbury, NZ
stephen.wingreen@canterbury.ac.nz

John Ascroft
Jade Software Corporation, NZ
jascroft@jadeworld.com

Ravishankar Sharma
University of Canterbury, NZ
ravishankar.sharma@canterbury.ac.nz

Abstract

In this paper, we adopt Agency Theory and Weill and Ross's IT Governance framework to examine the decision priorities of senior executives and board of directors in the context of IS resilience planning, which falls under the broader umbrella of IT governance. As identified in our earlier research, although research was conducted on the topics of organizational resilience, and IT governance, there is a gap in the extant literature on IS resilience. In this study we also expand the basic assumptions of Agency theory. We present a case study of the Jade Software Corporation, in which we use Q-methodology to develop a typology of decision priorities for IS resilience planning. Our analysis revealed two types of decision-makers, each representing a unique perspective of IS resilience. These types are discussed, along with implications of findings, a theoretical framework for IS resilience, and suggestions for future research.

1. Introduction

Global warming is increasing the risk of extreme weather conditions and disasters. With Hurricane Katrina in 2005, the Great East Japan earthquake of 2011, Christchurch earthquakes in 2010 and 2011, and more recently floods in Mozambique and the COVID-19 pandemic the regular occurrences of disasters are evident. To survive after a disaster and subsequently to bounce back is a significant source of sustainable competitive advantage for most organizations. Organizations increasingly rely on complex Information Systems (IS) and digital platforms to manage their businesses, which require IS to operate reliably under a variety of adverse circumstances. Previous research has addressed disaster recovery, continuity planning, crisis planning, and other pertinent issues. Organizational research has involved all of these issues in the concept of "organizational resilience", which is commonly defined as the organization's ability to operate dependably in a variety of adverse circumstances, but the concept of IS resilience has yet to be developed. However, when examining the crisis resilience of organizations, one crucial aspect is to examine the continuance of stable and reliable IS services [4]. In theory, IS resilience should be aligned with the overall organizational strategy, and therefore under the wider umbrella of organizational resilience.

Apart from our seminal research, we were able to find only a few papers ([6]; [10]) on the topic of IS resilience. To our knowledge, apart from our research work there has been no systematic examination on how IS resilience planning decisions are made or the role of IS resilience in firm governance. Rather than inspecting previous collapses and reveal finer details of what happened and how to prevent a recurrence [8], prior research has addressed disaster recovery (DR), business continuity planning (BCP) and other related issues and mostly focused on strategic IS planning, particularly developing best practice for it [5]. Therefore, this study aims to examine, ***how top management in a large organization prioritizes decisions to ensure IS resilience?***

Agency theory has confirmed substantial predictive power concerning the decision-making of the board of directors (BoDs) and executives by its proposition of the principal-agent relationship dynamics [2][7][9]. Specifically, Agency Theory proposes that the misalignment of interests between the principals (BoDs) of a firm and the agents (executives) is a source of costs and losses to the firm [2][7]. When there are conflicting interests between principals and agents, it is referred to as "principal-agent conflict", which is solved by various types of contractual agreements that distribute risk among decision-makers. However, Agency Theory does not deal directly with IT-related decision-making or risk distribution. Also, IS projects are typically the key building blocks of large-scale, multiyear digital transformation journey[15]. in the digital era, the organizations have changed and therefore it is worth questioning that the agency theory which is based on the understanding of organizations that dates back to the 1970s may limit our ability to better understand organizations and advise managers at present.

URI: https://hdl.handle.net/10125/71426
978-0-9981331-4-0

On the other hand, Weill's and Ross's IT governance framework explains how decision rights and responsibilities are distributed within the IS function in organizations, by his definitions of IT archetypes, and IT domains, but it does not explain why decision rights and responsibilities are spread the way they are. Agency Theory and Weill are compatible with both decision rights and decision responsibilities, since Weill's definition of an IT archetype encompasses the type of person who has decision rights, and the IT domain includes the decision responsibilities of each IT functional area [14]. Weill explicitly assumes that there should be an alignment of decision-makers' interests with the strategic interests of the firm, as it is with Agency Theory.

Increasingly, the advantages of the decision-making authority of information technology (IT) governance are being recognized. However, more scrutiny is needed for the extension of governance concepts to information systems (IS) resilience. Weill and Ross (2004) treat business continuity planning simply as a cluster in "IT infrastructure services" and did not mention IS Resilience. This reflects the traditional view of information system resilience as a mere technical issue. While some resilience decisions have a clear technological orientation, others are more strategic and business-oriented and rest lie somewhere in between. Thus, fresh considerations of IS resilience call for a more fine-grained treatment of governance of resilience decisions.

To aid the study and practice of IS resilience, we propose a conceptual IS resilience governance framework (figure 1). It specifically deals with IS resilience decision rights and is based on the synthesis of several principles and taxonomies: (a) Agency Theory; (b) Weill and Ross's taxonomy of IT decision types; (c) the principle of aligning accountability with correct decision authority and (d) the principle of giving decision authority to the organizational unit with the best information for the decision.

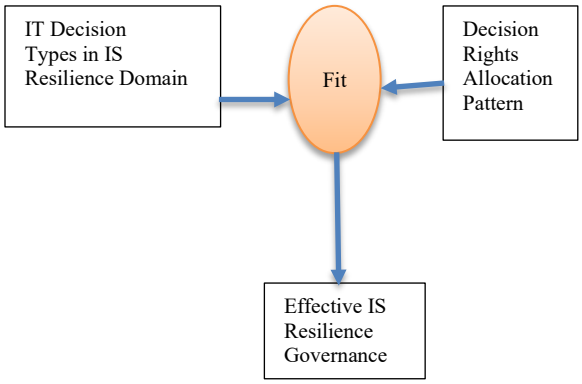

Fig.1 IS Resilience Governance Conceptual Model

It is therefore the goal of this research to develop and validate an IT governance framework in the context of IS resilience. Toward this goal, we have selected Jade Software Corporation, a large organization whose head office is in New Zealand, because it is an exemplar of the theoretical concepts, we would expect in the context of IS resilience. Specifically, firstly, there is a strict separation of ownership and control between Jade's board of directors and their executive management team, as the key decision-makers do not bear a major share of the wealth effects of their decisions. Secondly, during this investigation, Jade was actively involved in the domain of IS resilience planning, prioritization, and alignment in the aftermath of a major crisis, the Christchurch earthquakes of 2011. In this setting, we expect to witness all the richness of IS resilience decision priorities that our theory might predict.

This paper presents the findings of an investigation of the IS resilience decision priorities of the top management team at Jade, which consists of all the c-suite executives and the board of directors (BoD). First, we have reviewed the literature on organizational resilience, IT governance, IS planning and agency theory. The paper then describes the research methodology, in which we employed the Q-methodology to determine how the top management team at Jade manifest their decision priorities and preferences to ensure IS resilience. Further, we conducted interviews with the top management team to enrich our interpretation of the case study. The paper concludes with the discussion of a theoretically founded typology of IS resilience planning priorities and lessons learnt during this process. We also discuss the relevance of this research for both practitioners and academics and we propose some recommendations for further research in the area of IS resilience.

2. Theoretical background

2.1. IS Resilience Planning

The concept of resilience has been a prominent and emerging topic in various scientific fields, however, as resilience research encompasses a wide range of disciplines, it is not surprising that the concept lacks an accepted common definition across disciplines [10]. For our study IS resilience is defined as:

"Information Systems resilience is a function of an organization's overall situation awareness related to Information Systems, management of Information Systems vulnerabilities, and adaptive capacity, risk intelligence, flexibility and agility of Information Systems in a complex, dynamic, and interconnected

environment."

The traditional approach to define resilience focuses on an event-based approach that deals with identifying potential risks and preparing response measures for them, whereas, our definition of IS resilience incorporates a process-based approach to build a sustainable business model. The process-based approach embeds the resilience thinking in the culture of an organization, which distinguishes it from just suggesting a corrective measure for a particular event [12].

Empirical studies of IS planning practices in organizations indicate that varied differences exist. Organizations differ in terms of how much IS planning they do, the IS planning methodologies they use, the employees involved in IS planning, the alignment between IT and business, the focus of IS plans, and how IS plans are implemented [5]. IS planning is used to accomplish three major objectives: (1) establishing a basis for monitoring and bonding IS managers so their actions are more likely to be consistent with the goals of the organization; (2) resolving how the gains and losses from unforeseen circumstances will be distributed among principals and agents; and (3) determining the level of decision rights to be deputized to the agents[5]. IS resilience planning is unique with respect to other types of plans because an IS resilience plan is intended to be implemented during a time of crisis or adverse circumstances when there is a high degree of uncertainty.

2.2. Agency Theory and Decision Making

Agency Theory rejects the classical view of the firm as a unified profit-maximizing identity and proposes an alternative view of a firm. Agency Theory is essentially a theory of decision-making, where the principal and the agent are theorized to be in a contractual agreement that serves the best interests of the principal [2][7]. The key idea behind the Principal-Agent model is that the principal is too busy to do a given job and so hires the agent but being too busy also implies that the principal cannot monitor the agent easily. As a result, when decision-making authority is delegated to agents, it cannot be assured that the decisions will be aligned with the interest of the principal. However, when the principal has adequate information to verify agent behaviour, the agent is more likely to behave in favour of the principal (Eisenhardt, 1989). It predicts that higher levels of uncertainty will be associated with higher levels of delegation of decision rights to the agent. However, if decision rights are not delegated in the presence of high uncertainty, organizations cannot respond quickly enough to the IS prospects and problems they meet. From an Agency theory viewpoint, a plan should be devised in such a way that they become a better monitoring and bonding device and reflects organization goals and objectives rather than the senior executives' goals and objectives. Similarly, an IS plan can be a form of an implicit contract between the principals (Directors) and their agents (Sr. Executives), and between senior executives and employees at other levels of the firm. An IS plan is thus a vehicle to distribute risk across all levels of the firm. Agents should have the power proportional to their responsibilities, including the proper decision rights to search for and take actions that benefit the organization. Proper allocation of decision rights also improves decision quality. Different organizational units are the natural sub-divisions for different decision types depending on the contexts of the decision rights.

2.3. Weill and Ross IT governance archetypes

IT governance, the term defined as "specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT" [14] constitutes the most universal and systematic approach helping to solve the problems connected with supporting business with IT in the organizational context. According to Weill, IT governance is not about specific decisions about IT but about who makes what decisions, who has input and how the decision makers are held accountable for the decisions. IT governance encompasses five major decision domains. IT principles comprise the high-level decisions about the strategic role of IT in the business. IT architecture includes an integrated set of technical choices to guide the organization in satisfying business needs. IT infrastructure consists of the centrally coordinated, shared IT services that provide the foundation for the enterprise's IT capability and were typically created before precise usage needs were known. Business application needs are the business requirements for purchased or internally developed IT applications. Last, prioritization and investment decisions determine how much and where to invest in IT. There are six archetypal approaches to IT decision making, ranging from highly centralized to highly decentralized. Most companies employ a variety of them, using different approaches for different decisions [14]. In this research, focus is on who, what and how decisions are prioritized to ensure IS resilience. To our knowledge there are no empirical validation of Weill's IT governance framework in context to IS resilience planning, this will be a vital contribution of this research.

Table 1. Weill and Ross's IT governance archetypes

Archetype	Decision Rights Allocation Mechanisms
Business Monarchy	Senior business focused executives make IT decisions for the whole organization. The IT focused executives are considered as one voice in the decision making.
IT Monarchy	IT focused executives make the IT decisions.
Feudal	Business Unit management makes IT decisions.
Federal	Both the enterprise and business IT function leaders are involved in making IT decisions.
IT Duopoly	Decisions are made by the duo of IT-focused executives and either the enterprise business executives or business unit leaders.
Anarchy	No IT Governance

3. Case Organization

Jade Software Corporation Limited was founded in 1978 and is headquartered in Christchurch, New Zealand. Jade works with leading companies around the world to solve complex business problems through the design and delivery of innovative software solutions. It is a large organization with 45 major partners, and offices in the United States, the United Kingdom, the Middle East, the Netherlands, Indonesia, New Zealand and Australia. The company operates three main lines of business: Jade Solutions: custom software development and support; Jade Technologies: JADE programming language and database platform; Jade Logistics – Terminal Operating System for mixed cargo shipping ports.

Jade experienced several challenges as a result of the Christchurch earthquakes, mosque attack and COVID-19 pandemic. Jade had in place a robust and rehearsed business continuity and disaster recovery plan, had set up special control rooms, as well as establishing a task list and contact tree for emergencies and had established a resilience culture. Therefore, Jade was prepared when the COVID 19 pandemic struck. Even though Jade was well-prepared, the scale of the disaster still took them by surprise. But, as they were well prepared, they quickly adapted to the changing environment and successfully met all contractual requirements throughout the crisis. As mentioned earlier, we have selected Jade because they are the exemplar to study the effects of senior executives' decision priorities in context to IS resilience. They are already committed to IS resilience and have multiple decision-makers in the IS resilience committee. One of the most important aspects to understand resilience is to know how people learn to adapt and what happens when they stop learning from experiences [8]. However, in this context, what is absent is empirical research that shows how learning is sustained during crises and how lessons learned after a crisis actually make a difference later. As all the key decision-makers at Jade have already experienced a crisis scenario, this issue will be addressed and will add realism to this study.

4. Research Method

Q-methodology and its associated q-sort procedure were chosen to operationalize the theoretical concepts of interest, gather and analyze data, and interpret the results. Firstly, a representative set of q-statements are derived directly from the domain of interest, in this case, organizational resilience, IS resilience planning and decision-making. Q-methodology supports the inclusion of theoretical categories in a set of "structured" q-statements, and therefore statements representing aspects of Agency Theory and Weill's IT governance framework were included. The complete list of q-statements may be found in the Appendix. Decision-makers perform the q-sorts, which are then factor analyzed to produce a typology based on the priorities expressed in their q-sorts. Furthermore, the "IT Decision Domain" column represents how both senior executives and the researchers categorized all statements into one of Weill's five IT decision domains. There was 100% inter-rater agreement between the senior executives and the researchers. Since the set of q-statements includes information from the entire domain of IS resilience planning, the interpretation of the factors or types reveals the full richness of the decision process and its associated priorities. The resulting typology may be used as the basis for a theoretical foundation since each type represents a set of correlated decisions and planning priorities. In this manner, the Q-methodology was employed to guide the study and to collect and analyze data gathered from senior executives on Jade's IS resilience planning committee.

The Q-sort instrumentation, a set of 37 Q-sort statements, was developed according to the guidelines outlined by previous research [1][11][13]. The statements were partly derived directly from the living discourse of business executives who were actively involved in IS resilience planning, and partly from the literature, domain experts, interviews, and other referential material. After several iterations of testing and revision, the evaluators confirmed that the instrument is ready and should function as intended.

We then pilot tested the instrument with seven CEO owner-managers of local SMEs, who provided their own Q-sorts to test the statistical properties of the Q-sort set and also evaluated the Q-Sort instrument. Four (4) board of directors along with seven (7) senior executives at Jade, were then approached to provide their q-sorts, and data gathered was analyzed using the PQ-method software that is commonly used in Q-methodology research. Seven (7) senior executives belong to the IS resilience committee.

4. Findings and Discussion

4.1. Findings

This section presents the research findings that were reached through the analysis of Q-sort data. The Q-sort data was analyzed using a centroid factor analysis, as suggested by prior research [13]. Two and three-factor solutions were examined at first, however, since the three-factor solution converged to a two-factor solution, there was no need to continue, and a two-factor solution was adopted. Table 1 reports that four (4) board of directors and seven (7) senior executives can be distributed into two types and their respective positions in the organization have also been outlined.

4.2. Type 1: Technical Focused Tactical

Table 2.Q-Factor Matrix of 2 Factor Solution

TMT Members	Type 1	Type 2	Positions
TMT1	-0.0550	**0.8491**	*Strategic*
TMT2	**0.6310**	0.5936	*Technical*
TMT3	**0.7518**	0.3584	*Technical*
TMT4	**0.7618**	0.1141	*Technical*
TMT5	**0.6521**	0.4261	*Technical*
TMT6	0.3156	**0.6531**	*Strategic*
TMT7	**0.8356**	0.0773	*Technical*
DIR1	0.4807	**0.5553**	*Strategic*
DIR2	0.4650	**0.5871**	*Strategic*
DIR3	0.1694	**0.7498**	*Strategic*
DIR4	**0.7632**	0.1613	*Technical*

Decision Makers

Type 1 can be characterized as technical focused tactical decision-makers. According to Weill they are IT monarchs and are comfortable in IT architecture, and IT infrastructure strategy types of decision making. They are involved in the implementation of high-level views and are responsible for implementing IS resilience and ensuring day to day operation of the organization. This group clearly preferred technical priorities over strategic priorities, as exemplified by the high ranking they assigned to, "Select suppliers with robust resilience plan" (rank 6), which falls under both the IT infrastructure and IT principles categories, but received a low ranking from Type 1 (rank 27). When probed Type 2 decision-makers said, "we [strategic team] understand that in [regard to] hardware and infrastructure, if we do not get replacements on time, then we will end up with problems. It is critical for us". On the other hand, Type 1 says that as with the data, all critical applications are now on the cloud, and cloud infrastructure is highly reliable and always available, so the supplier resilience is important but not critical. Another interesting finding for Type 2 is related to, "Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning" (rank 5), which falls under both the IT infrastructure and IT Investment and Prioritization categories. According to Weill both type 1 and type 2 should consider the statement to be important. Surprisingly, Type 1 ranked it 31 while Type 2 ranked it 3. When probed we found that according to Type 1, top-level technical type decision-makers', "IT changes too fast thus there is hardly any value in making a long term [IS] resilience plan". On the other hand according to Type 2 strategy-oriented decision-makers, "technology changes fast but from a strategic perspective we see a pattern and what we do not know exactly is the detail of implementation but [we] can certainly do long term planning". This justifies why the Type 1 decision-makers rated it low whereas the Type 2 decision-makers rated it high, which could not be predicted by Weill's IT governance framework. Aligning Information Systems (IS) strategies with the strategic plan of the organization" (rank 10) and "Adapting technology to strategic change" (rank 16). The first two statements fall under Weill's IT infrastructure category while the last two falls under the IT architecture category, and hence are more technical than strategic. Lastly, Weill's framework fails to predict statement number 22, which falls under both IT Principles and IT Infrastructure Strategies category. When probed Type 2 explained that, "It is about connectedness", as illuminated by them, "we do not work in isolation; we are intermediaries between suppliers and our customers. It is crucial to ensure that we are connected hence it is important for us." On the other hand, Type 1 again estimates the independence of the firm to ensure resilience.

4.3. Type 2: Business Focused Strategic Decision Makers

Type 2 can be characterized as business-focused strategic decision-makers. According to Weill they are business monarchs and are more comfortable with IT principles and IT investment and prioritization types of decision making. They have high-level enterprise-wide views and clearly prioritized more strategic than technical type decisions which can be exemplified by these highly ranked statements: "Organization hazard/risk assessments carried out which provide a comprehensive picture of all major hazards and risks faced by organization (and potential risks)" (rank 1) and "Organizational vulnerability and capacity assessments carried out which provide a comprehensive picture of vulnerabilities and capacities" (rank 5). Both questions fall under Weill's IT investment and priority category; hence, they are more strategic than technical. Type 1 decision-makers want more certainty around risks, as reflected by the statement of one of their executives, "a comprehensive picture is essential to foresee risks to manage them and ensure that correct risks are addressed". When probed on another statement, "Organization IS Continuity plans, developed through participatory processes, put into operation and updated periodically", which was ranked (6) by type 1 whereas ranked (11) by type 2, we found that both types understand that this is important and existing plans need to be regularly audited, exercised and updated, that is consistent with what they do in practice. In another case, both Type 1 and Type 2 mentioned existing IS resilience plan requires to be updated regularly to reflect the changes in technology, business environment and customer priority changes. This statement falls under the IT principles category; hence it would have made perfect sense if Type 2 ranks it high in comparison to Type 1. However, both types think it is very important. Diving deep we understand that this factor is a critical aspect of IS resilience and from the practitioner's perspective; ie those who are involved in mitigation planning need a well captured, live prioritized snapshot of the risk environment.

4.4. Key Lessons on IS Resilience

Neither centralized nor decentralized decision making is always a good thing. Instead, different decisions need to be made in different organization locations (refer to table 3).

A central assumption of Agency Theory is that goal incongruence between principal and agent is typically unavoidable. This assumption reflects a traditional view of organizations with corporate business units in a Principal role and internal IT units in an Agent role, emphasizing bounded roles and work division and conflicting interests and goals across roles. However, the digital revolution has enhanced the importance and changed the role of the organization's IT units, which are now increasingly requested to partner with business units and integrated into cross-functional teams pursuing digital innovation and transformation projects. In the new digital era, business and IT experts share common goals or in other words, the agent motives are aligned with the objectives of the principal and the organization.

Also, agency theory holds the assumption that information asymmetry between principal and agent can lead to opportunistic behaviour, as agents can exploit the principals by using their superior knowledge for individualistic goals. We found in our study that this does not hold. IS resilience decision making is complex, multidimensional and knowledge-intensive and requires specialized inputs from domain experts. IS resilience decision making deals with ill-defined complex problems coupled with uncertainty and requires continuous innovation, rely heavily on diverse and heterogeneous sources of knowledge and domain expertise.

Some very interesting evidence of "cooperative games" has been identified in our study, they are: "[Jade] solve new and existing customer problems which are novel and technologically challenging. Also, we are trusted to deliver insights that support high performing operations and growth." "[Jade] has a strong focus on the power of collective and participatory models that draw the best from staff knowledge and expertise."

Table 3. IS resilience governance at Jade

Decision / Archetypes	IT Principles		IT Architecture		IT Infrastructure		Business Application Needs		IT Investments	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Business Monarchy		√								√
IT Monarchy			√	√	√	√				
Federal	√						√	√	√	
IT Duopoly										

"We are a connected team that provides a consistent experience when anyone engages with us. Our people feel empowered and own what we do and how we do it."

"Our customers see us as one Jade, keeping our commitments and easy to work with. This results in increased loyalty, higher-margin engagements, and future growth. Our growth in revenue and margin is mission-critical."

Consequently, in the current context, we can see that how information asymmetry can add to the expertise and allows IS resilience team members to perform knowledge-intensive works better. In fact, we can conclude that information asymmetry can positively influence information resilience decision making.

Agency theory assumes that the agents will demonstrate extrinsically motivated, profit-maximizing behaviour whereas, we found that knowledge workers tend to value their jobs not only for monetary compensation but also for satisfaction, personal and professional growth opportunities. They are intrinsically motivated and self-actuating professionals who display high levels of commitment and involvement.

The main drivers for Jade's Business Continuity and Resilience Program are the contractual requirements to provide continuous support for global products and the operation of the managed services providing outsourcing for companies all over the world. In addition, as a software development company, access to collaboration tools, development environments and office support systems is critical. Jade values collaboration and it is purposely led and integrated into the culture of the organization. Jade has a committee that is responsible for risk management and IS resilience planning. The committee consists mostly of members of the c-suite executive management team responsible for the various areas of the company. They work together to ensure that all prospective risks are identified, mitigated, and planned for.

An important aspect of organizational resilience is IS resilience. Thus, agile and successful IS resilience planning requires a subset of organizational capabilities. As learnt from Jade, essential components of successful IS resilience planning can be summarized as:

Sincere Top Management Commitment to Resilience: a vital requirement to IS resilience planning is the commitment at top management level and to reach effective IT governance, two-way communication and a good participation/collaboration relationship between the business and IT people are desirable. Adequate financial support to implement is also very important.

Resilience Strategy: clear strategy aligned to organizational goals and priorities must be formulated which has to be embedded in the organization's culture.

IS Resilience Planning Process and Implementation: rather than a rigid hierarchy of plans derived from an 'event-based' model, it is critical to have a more flexible plan based "service-recovery", which is neither scenario-based nor event specific. Agency Theory would ordinarily predict a less flexible plan, to transfer risk-bearing and decision rights away from employees at lower levels of the firm by creating more certainty about their duties. However, the context in which IS resilience plans are implemented are by definition highly uncertain, ambiguous, laden with risk, and require employees at all levels of the firm to act with greater degrees of autonomy and discretion to remain flexible in adverse circumstances or times of crisis. As highlighted by the senior executives, "In times of crisis plans go out of the window, it is important not to park those plans". In other words, this finding is not immediately obvious from the perspective of Agency Theory but makes good sense in the unique context of IS resilience planning.

Educating and Knowledge Sharing: resilience includes learning and knowledge sharing, adaptation, innovation and staff training. Managers and employees need to be educated regularly to create an organization-wide resilience culture. As identified by Kayes [8], "It is the 'experienced' [person] who knows the limitations of all anticipation, the insecurity of all human plans. Experience teaches the incompleteness of all plans.'' This establishes a deep connection between resilience and learning, and points to a style of learning orientation that is closely aligned with resilience. It is also consistent with the findings about the need for a flexible plan, since training and education are necessary. If employees at all levels of the firm are expected to act with greater degrees of autonomy and discretion in times of crisis. In this case, therefore, training and education become a vehicle for the transference of risk-bearing and decision rights to employees at all levels of the firm.

Table 4.IS Resilience Governance Archetypes

IS Resilience Domain	IT Decision Type	Observed Jade Archetype	Rationale for Observation
Strategy	IT Principles	Business Monarchy and federal	Business-focused strategists have knowledge but interestingly they seek input from technical focused decision makers as detailed technical knowledge required.
Organization (Supplier, Own and Customers)	IT Principles	Business Monarchy	Business focused strategists have knowledge and no detailed technical knowledge required.
Technology (Supplier, Own and Customers)	IT Architecture, IT infrastructure	IT Monarchy	Technical expertise required
Policy	Business Application needs	Federal	Requires ability to analyze technical and strategic implications.
People	Business Application needs	Federal	Mainly enterprise business leader with help from IT professionals develop resilience training
Monitoring	Business Application needs	Federal	Independence is critical, BoD along with business and technical focused executives are responsible collectively.
Finance	IT investment and prioritization	Federal, Business Monarchy	Requires quantitative as well as qualitative evaluation. CFO is the lead but with input from others.

Continuous Testing and Monitoring: conducting dry-run or live test scenarios for testing specific service recovery strategies and regularly re-assessing risks and mitigation strategy. This finding also follows our observation about training and education since it serves a purpose to enable employee preparedness at all levels of the firm.

Regular and Transparent Communication: well-planned communication and change management is essential to effectively adapt to turbulent changes.

Choose Your Partners Wisely: focus on key resilience attributes that really matter while choosing your partners is essential. This is also important while migrating to cloud environment.

Strong Understanding of Value Chain: important message is "connectedness", value chain takes into consideration different types of inter-organizational relationships, such as suppliers, customers, or the government.

5. Conclusion and Implications

In this study, we have called attention to key descriptive aspects of top management team decision priorities in context to IS resilience and have identified two types of decision priorities within the top management team at Jade. We have emphasized the important distinctions as well as similarities among them and the types of information they convey. This rich, descriptive analysis was set in the functional IT governance framework, which is relevant to governance and decision making in IS and we also viewed top managers' decision-making priorities through the theoretical lens of Agency Theory. Our contribution is novel as it is rooted in two popular theories, namely, Agency Theory and IT governance framework. To the best of our knowledge, this is the first attempt to build the concept of IS resilience separate from the concept of organizational resilience, and it appears to be valid. The types we have identified are complementary to each other and give us a more precisely characterized set of variables and important decision priorities in the context of IS resilience framework to work with. The Q methodology does have some weaknesses. It is a small-sample technique, and the sample of items and participants is usually purposive, and the results lack generalizability. However, since the goals of Q-methodology are interpretive, Q-method practitioners do not usually consider this as a weakness. This study is a starting point for further research into the IS resilience in large organizations. There are several avenues of future research, including examining a greater range of organizations. Future empirical research should try to understand the IS resilience decision priorities and characteristics of resilient organizations, both public and private.

Our study reveals (refer to table 4) that in dealing with knowledge organizations we should be interested in more than simple "superior-subordinate dyads." The simple principal-agent model focuses for convenience

on one principal and one agent, highlighting the determinants of control in dyadic relationships. But such a dyadic relationship is unrealistic. A simple dyadic principal-agent model is incapable of capturing the dynamic interaction between multiple principals and a set of professional agents. Knowledge-driven organizations can be viewed as sets of coalitions rather than single unitary actors.

Treating information (e.g., technical expertise, strategy expertise) as a variable rather than as a constant consists of two variables—the information possessed by the agent and the information possessed by the principal. When these variables are arrayed in two dimensions (see table 5), in a dyadic relationship with one principal and one agent only, the standard form of information asymmetry is only one of four possible situations. From exhibit 1, case A exists when neither principal nor agent possesses a great deal of information, case B exists when Agent possesses the information, case C exists when both possesses a great deal of information, and case D exists when the agent does not possesses a great deal of information but the principal does.

Case B is consistent with the assumptions of the traditional information asymmetry of the principal-agent model. But as can be seen in Table 5, this is only one of four possible outcomes. In our study, we found that Jade is representative of Case C, where both principal and agents possess high level of business and IT expertise.

Table 5.Untangling Information Asymmetry

Principals Information Level	Agents Information Level: **Low**	**High**
Low	Case A	Case B
High	Case D	Case C

Finally, results have implications both for researchers who are looking for theories that explain the importance of IS resilience and business managers and practitioners who are challenged with decisions about how to design resilient information system framework for their organization.

Among the limitations of a case approach is the question of generalizability. We suggest that this study be replicated across organisations, industries and geographies to confirm a more robust theory of IS resilience. Another limitation inherent in longitudinal studies is the absence of control for personnel and other organizational changes. We suggest that the findings be tempered by this observation.

6. References

[1] Brown, S. R. 1980. Political subjectivity: applications of Q Methodology in Political Science, New Haven, CT: Yale University Press.

[2] Eisenhardt, K. M. 1989. "Agency theory: an assessment and review," Academy of Management Review, pp. 57-74.

[3] Fama, E. F., and Jensen, M. C. 1983. "Separation of Ownership and Control," Journal of Law and Economics, pp. 1-30.

[4] Gibb, F., and Buchanan, S. 2006. "A Framework for business continuity management," International Journal of Information Management (26:2), pp.128-141.

[5] Hann, J and Weber, R. 1996. "Information Systems Planning:A Model and Emperical Tests,"Management Science (42: 7), pp. 1043-1064

[6] Heeks, Richard and Ospina, Angelica V. 2018. "Conceptualising the link between information systems and resilience: A developing country field study", Information Systems Journal, published online first 19 January 2018.

[7] Jensen,M.C. and Meckling, W.H. 1992. Foundations of Organisational Strategy, Lars Werin and Hans Wijkander, eds., Blackwell, Oxford.

[8] Kayes, D.C. 2015. Organizational Resilience: How Learning Sustains Organizations in Crisis, Disaster, and Breakdowns, New York: Oxford University Press.

[9] Lee, C.K. and Wingreen, S.C. 2010. "Transferability of knowledge, skills, and abilities along IT career paths: an Agency Theory perspective," Journal of Organizational Computing and Electronic Commerce (20:1), pp. 23 – 44.

[10] Muller, G., Koslowski, T., and Accorsi, R. 2013. "Resilience – A New Research Filed in Business Information Systems," ACM Symposium on Business Computing, pp. 1-12.

[11] Stephenson, W. 1986. Protoconcursus: The concourse theory of communication: I. Operant Subjectivity (9:2), pp. 37-58.

[12] Vargo, J., & Seville, E. 2011. "Crisis strategic planning for SMEs: finding the silver lining," International Journal of Production Research, pp. 5619-5635.

[13] Watts, S and Stenner, P. (2012). Doing Q methodological research: theory, method and interpretation, London: Sage Publications.

[14] Weill, P. and Ross, J.W. 2004. IT governance: How Top Performers Manage IT Decision Rights for Superior Results, Watertown, MA: Harvard Business School Press.

[15] Wiener, M., Mahring, M., Remus, U. Saunders, C., Cram, W.A. 2019. "Moving IS Project Control Research into the Digital Era: The "Why" of control and the Concept of Control Purpose. Information Systems Research, pp. 1-15.

Appendix – Q-sort statements with asterisks (*) denote distinguishing statements between Type 1 and Type 2 Decision-Makers

Resilience Statements	No.	IT Decision Domain (by Peter Weill)	Factor Scores	
			F1	*F2*
Information Systems (IS) Disaster Recovery plans informed by understanding of underlying causes of vulnerability and other factors outside organization's control.	**1**	IT Architecture	1	1
Organization Information Systems (IS) Continuity plans, developed through participatory processes, put into operation and updated periodically.	**2**	IT Principles	2	2
Organization's Information Systems (IS) resilience plan shared with all suppliers.	**3***	IT Principles	0	-2
Organization hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organization (and potential risks).	**4***	IT investments and priorities, IT Infrastructure Strategies	3	-1
On-going monitoring of hazards and risks and updating of plans.	**5***	IT Principles	1	0
Organizational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities.	**6***	IT Investment and Prioritization	2	1
Resilient and accessible critical facilities (e.g. back-up systems, redundancy of data).	**7***	IT Architecture and Infrastructure Strategies	3	1
Top management support and commitment to Information Systems (IS) resilience.	**8***	IT Principles	1	3
Information Systems (IS) resilience can provide an organization with an edge over its competitors.	**9***	IT Principles	0	-2
Our competitors are developing and enhancing their Information Systems (IS) resilience capabilities.	**10***	IT Principles	-2	-3
A sound Information Systems (IS) resilience plan will help us to win more business contracts.	**11***	IT Principles	0	-2
A sound Information Systems (IS) resilience plan will help us to pay lesser insurance premium.	**12**	IT Principles	-3	-3
A sound Information Systems (IS) resilience plan will help our organization to make more efficient use of resources.	**13***	IT Principles	-3	-1
Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning.	**14***	IT Infrastructure and IT Investment and Priority	-1	2
Competitor Analysis - Survive disruptions that your competitors cannot.	**15**	IT Principles	-1	-1
Setting up information disaster recovery system (e.g., disk redundancy, backup facility).	**16***	IT Architecture, IT Infrastructure and IT Investment and Priorities	2	0
Study resilience strategies of competitors.	**17**		-2	-1
Select suppliers with robust resilience plan.	**18***	IT Infrastructure Strategies and IT Principles	0	1
Use Information Systems (IS) network to communicate with the customers.	**19***	IT Infrastructure Strategies	0	1
Use Information Systems (IS) networks to connect to the supplier's databases.	**20**	IT Infrastructure Strategies	-1	-1
Use cloud computing to back up organizational data.	**21***	IT Principles and IT Infrastructure Strategies	0	-2
The level of customer involvement in preparing resilience, business continuity and disaster management plans.	**22***	IT Principles and IT Infrastructure Strategies	-1	0
The extent of follow-up with customers for feedback.	**23**	IT Principles	0	0
The level of supplier involvement in preparing resilience, business continuity and disaster management plans.	**24***	IT Principles	-1	0
Ensuring data security	**25***	IT Principles and IT Architecture	1	0
Receiving reliable and consistent services from Suppliers	**26**		-2	-1
Providing reliable and consistent services to customers	**27**	IT Principles and IT Infrastructure	2	3
Capability for disaster recovery	**28**	IT Principles and IT Infrastructure	1	0
Providing the organizational units with information for 24 hours a day, 7 days a week	**29**	IT Principles	0	0
Understanding the strategic priorities of top management	**30**	IT Principles	-1	0
Aligning Information Systems (IS) strategies with the strategic plan of the organization	**31***	IT Architecture	0	2
Adapting technology to strategic change	**32***	IT Architecture	-2	0
Information Systems (IS) resilience plan that is well defined and structured	**33**	IT Principles	0	0
Information Systems (IS) resilience plan that is flexible and adaptable	**34**	IT Principles	0	1
Ability to identify key risks	**35**	IT Principles and IT Architecture	0	0
Ability to anticipate surprises and crises	**36**	IT Principles	0	0
Committed, effective and accountable leadership of Information Systems (IS) resilience planning and implementation.	**37***	IT Principles	1	2