Top Management Team Decision Priorities to Drive IS Resilience: Lessons from Jade Software Corporation

Indicate Submission Type: Full Papers

Amitrajit Sarkar
Ara Institute of Canterbury, NZ
Amitrajit.Sarkar@ara.ac.nz

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

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

Abstract

In this paper, we adopt Agency Theory and Weill's IT Governance framework to investigate the decision priorities of senior executives in the context of IS resilience planning, which falls under the broader umbrella of IT governance. Although research has been undertaken on the topics of organizational resilience, and IT governance, there is a gap in the literature with respect to IS resilience. We report 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. 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.

Keywords

IS resilience, IT governance, IS resilience planning, top management team, decision priorities.

Introduction

Organisations 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 relevant issues. Organizational research has included all of these issues in the concept of "organizational resilience", which is generally defined as the organization's ability to operate reliably in a variety of adverse circumstances, but the concept of IS resilience has yet to be developed. However, when examining the crisis resilience of organisations, one crucial aspect is to examine the continuance of stable and reliable IS services (Gibb and Buchanan 2006). In theory, IS resilience should be aligned with the overall organizational strategy, and therefore under the wider umbrella of organizational resilience.

Unfortunately, to best of the authors' knowledge, no research has been undertaken on how IS resilience planning decisions are made. Rather than inspecting previous collapses and reveal finer details of what really happened and how to prevent a recurrence (Kayes, 2015), most research focuses on the IS planning agenda, and developing best practice for IS planning and priorities. For example, prior literature has discussed why IS planning should be undertaken, how IS plans can mitigate risks and how IS plans can be better connected to business strategy. We see two problems with this prior research. First, it is primarily prescriptive in nature and second, it describes what organizations ought to be doing with respect to IS planning practices, rather than what decision makers in organizations are actually doing.

Agency theory has demonstrated significant predictive power with respect to the decision-making of owners and managers by its proposition of the principal-agent relationship dynamics (Jensen and Meckling, 1992; Eisenhardt, 1989; Lee and Wingreen, 2010). Specifically, Agency Theory proposes that the misalignment of interests between the principals (owners) of a firm and the agents (managers) is a source of costs and losses to the firm (Jensen and Meckling, 1992; Eisenhardt, 1989). 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.

Peter Weill'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 distributed the way they are. Agency Theory and Weill are compatible with regard to 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 (Weill and Ross, 2004). Weill explicitly assumes that there should be alignment of decision makers' interests with the strategic interests of the firm, as it is with Agency Theory.

IS resilience is comprised of a complex structure and process of decision making which include alignment between IT and business strategies, better focus on IT investment on strategic priorities, avoiding potential business risks, and capitalising on current business opportunities. For example, an IBM study reported how organizations are increasingly adopting integrated business resilience strategies in an uncertain environment and large organisations lead the way in business and IS resilience (IBM 2011). 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 because it is an exemplar of the theoretical concepts we would expect in the context of IS resilience. Specifically, first of all, 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 the course of 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 environment, we expect to observe all the richness of IS resilience decision priorities that our theory might predict. Therefore, this study aims to examine, *how top management prioritise decisions to ensure IS resilience?*

This paper presents the initial findings of an investigation of the IS resilience decision priorities of the executive management team at Jade. First, the literature on organisational resilience, IT governance, IS planning and agency theory is reviewed. The paper then describes the research methodology, in which the Q-methodology is employed to determine how senior executives at Jade manifest their decision priorities and preferences in order to ensure IS resilience. Further, we conducted interviews with the executive 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. 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.

Literature Review

IS Resilience and 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 (Muller, Koslowski and Accorsi, 2013). A definition of IS resilience is introduced based on these characteristics for the purpose of our study, it 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 each of them, whereas, our definition of IS resilience incorporates a process based approach to build sustainable business model. The process based approach embeds the resilience thinking in the culture of an organisation, which distinguishes it from merely suggesting a corrective measure for a particular event (Vargo and Seville, 2011).

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 the ways in which IS plans are implemented (Hann and Weber, 1996). IS planning has been 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 their superiors; (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 delegated to the agents (Hann and Weber, 1996). 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.

Agency Theory Effects in Decision Making

Agency Theory rejects the classical view of the firm as a unified profit-maximizing identity and proposes an alternative model of a firm. Agency Theory is essentially a theory of decision-making, where the principal and the agent are theorised to be in a contractual agreement that serves the best interests of the principal (Jensen and Meckling, 1992; Eisenhardt, 1989). Conflict between the principal and the agent occurs when the agent pursues his or her own best interests rather than those of the principal, and the principal finds it difficult and costly to verify what the agent is actually doing; as a result, the firm becomes less efficient, and this situation is referred to as the "agency problem." The central notion 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 effortlessly. When decision-making authority is delegated to agents, it cannot be guaranteed 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. Generally speaking, Agency Theory also predicts that risk would be transferred away from lower levels of the firm, to be borne by senior executives and managers. Although IS plans are usually about funding, functional activities (Hann and Weber, 1996), or IS processes, in the case of monitoring unobservable behaviours, the principal may use IS plans as a cost-effective means of monitoring and bonding agents (senior executives and managers) because they provide information about the agent's efforts to manage risk. Senior management may seek to exert more influence on the form of the IS plan via their control over the planning process if it can be used for monitoring and bonding purposes. From their viewpoint, the plan will be a better monitoring and bonding device if it reflects their goals and objectives rather than the IS manager's goals and objectives. In the context of Agency Theory, an IS plan is a form of 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.

IT Governance and Decision Making

Decision rights imply a decision-maker with knowledge needed to make those decisions, since a decision right specifies who in a firm has the authority to make what decisions. Decision rights must be moved to the department where the relevant knowledge resides ("delegation" solution), or the relevant knowledge must be moved to the locus of decision rights ("transmission" solution) (Jensen and Meckling 1992). IT governance, the term defined as "specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT" (Weill and Ross 2004) constitutes the most universal and systematic approach helping to solve the problems connected with supporting business with IT in the organizational context. There is a distinction between IT governance and IT management. Weill is speaking primarily of IS when he develops his IT governance framework, it does not focus on the technological solutions to business problems rather it focuses on principles of technologies as it relates to corporate businesses. "IS" is a term used primarily by academics, while "IT" is the term used in practice to speak of IS. 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, in this case, IT governance includes IS. 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 centralised to highly decentralised. Most companies employ a variety of them, using different approaches for different decisions (Weill and Ross, 2004). In this research focus is on who, what and how decisions are prioritised 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 an important contribution of this research.

Research Method

An exploratory case study methodology was adopted to support the development and preliminary validation of an initial theoretical framework about information systems resilience. Since there are no existing theoretical foundations for IS resilience, the procedure focused on discovering decision-makers' priorities with regard to IS resilience planning, with the goal of using the priorities as a foundation for a theoretical framework. In this case, decision priorities are considered to be a de-facto statement of the decision-makers' beliefs about IS resilience and all its various aspects, and how it is related to other issues of interest, such as risk management, disaster recovery, and contingency planning. Agency Theory and Weill's IT governance framework are the nearest theoretical kindred to IS resilience planning, and therefore were used as a loose principle by which to guide the investigation.

Q-methodology and its associated q-sort procedure were chosen to operationalize the theoretical concepts of interest, gather and analyse data, and interpret the results. First of all, 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. Decision makers perform the q-sorts, which are then factor analysed 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 categorised all statements into one of Weill's five IT decision domains. There was 100% inter-rater agreement between the senior executives and the researchers (refer to table 2). 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 decision and planning priorities. In this manner, the Q-methodology was employed to guide the study and to collect and analyse 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 (Brown, 1980; Stephenson, 1986; Watts and Stenner, 2012). 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 for the purposes of testing the statistical properties of the Q-sort set and also evaluated the Q-Sort instrument. Seven (7) senior executives at Jade, who belong to the IS resilience committee were then approached to provide their own q-sorts, and data gathered was analysed using the PQ-method software that is commonly used in Q-methodology research.

A Brief Introduction to Jade

Jade Software Corporation Limited was founded in 1978 and is head quartered 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. Jade 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 a number of challenges as a result of the Christchurch earthquakes. At the time of the disasters, the communications network and electricity cuts were problematic, with personal employee

issues following in the days after the earthquakes. Jade had in place a robust and rehearsed IS resilience plan, had set up special control rooms, as well as establishing a task list and contact tree for emergencies. Therefore, Jade was prepared when the disaster struck. Jade's primary business operations are located within the disaster zone of 2010 and 2011 Christchurch earthquakes and as a result, suffered a perturbing blow to business operations. But, as they were well prepared, they quickly adapted to the changed environment and successfully met all contractual requirements throughout the crisis. One of most important aspects to understand resilience is to know how people learn to adapt and what happens when they stop learning from experiences (Kayes, 2015). 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.

Research Findings and Discussion

This section presents the research findings that were reached through analysis of Q-sort data. The Q-sort data was analysed using a centroid factor analysis, as suggested by prior research (Watts and Stenner, 2012). 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 seven (7) senior executives can be distributed into two types and their respective positions in the organisation have also been outlined. The "Role" column reports how senior executives classified their roles as either technical or strategic, based on their position in the organisation. There was 100% inter-rater agreement between the senior executives and the researchers for this classification.

TMT Members	Type 1	Type 2	Role
PRILO1	0.4621	**0.7737**	*Technical*
PRILO2	**0.6890**	0.2399	*Strategic*
PRILO3	0.5286	**0.5397**	*Technical*
PRILO4	0.1469	**0.8787**	*Technical*
PRILO5	**0.7222**	0.2998	*Strategic*
PRILO6	**0.7338**	0.3614	*Strategic*
PRILO7	**0.8741**	0.1662	*Strategic*

Table 1: Q-Factor Matrix of 2 Factor Solution

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 organisation's control.	1	IT Architecture	1	1
Organisation Information Systems (IS) Continuity plans, developed through participatory processes, put into operation and updated periodically.	2*	IT Principles	2	1
Organisation's Information Systems (IS) resilience plan shared with all suppliers.	3*	IT Principles	0	-2
Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (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
Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities.	6*	IT Investment and Prioritisation	2	-1

Resilient and accessible critical facilities (e.g. back-up systems, redundancy of data).	**7***	IT Architecture and Infrastructure Strategies	2	3
Top management support and commitment to Information Systems (IS) resilience.	**8**	Critical for effective IT Governance	2	3
Information Systems (IS) resilience can provide an organisation 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	0
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 organisation to make more efficient use of resources.	**13**	IT Principles	-3	-3
Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning.	**14***	IT Infrastructure and IT Investment and Priority	-2	2
Competitor Analysis - Survive disruptions that your competitors cannot.	15	IT Principles	0	-2
Setting up information disaster recovery system (e.g., disk redundancy, backup facility).	**16**	IT Architecture, IT Infrastructure and IT Investment and Priorities	3	2
Study resilience strategies of competitors.	**17**		-1	-1
Select suppliers with robust resilience plan.	**18***	IT Infrastructure Strategies and IT Principles	-1	2
Use Information Systems (IS) network to communicate with the customers.	19	IT Infrastructure Strategies	0	0
Use Information Systems (IS) networks to connect to supplier's databases.	20	IT Infrastructure Strategies	-1	-1
Use cloud computing to back up organisational data.	21	IT Principles and IT Infrastructure Strategies	0	0
The level of customer involvement in preparing resilience, business continuity and disaster management plans.	**22***	IT Principles and IT Infrastructure Strategies	-2	0
The extent of follow-up with customers for feedbacks.	23	IT Principles	-1	0
The level of supplier involvement in preparing resilience, business continuity and disaster management plans.	24	IT Principles	-1	-1
Ensuring data security	**25**	IT Principles and IT Architecture	1	0
Receiving reliable and consistent services from Suppliers	26		-1	-1
Providing reliable and consistent services to customers	**27**	IT Principles and IT Infrastructure	1	2
Capability for disaster recovery	**28**	IT Principles and IT Infrastructure	1	1
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	0	0
Aligning Information Systems (IS) strategies with the strategic plan of the organisation	**31***	IT Architecture	0	1
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	1
Information Systems (IS) resilience plan that is flexible and adaptable	34	IT Principles	0	0
Ability to identify key risks	35	IT Principles and IT Architecture	0	0

Ability to anticipate surprises and crises	36	IT Principles	0	-1
Committed, effective and accountable leadership of Information Systems (IS) resilience planning and implementation.	37	IT Principles	1	0

Table 2. Q-sort statements with their corresponding ranks and z-scores, statement numbers with asterisks (*) denote distinguishing statements between Type 1 and Type 2

Table 2 reports the results of the factor analysis, which reveals two "types" of decision priorities. The factor scores are the factor Q-sort values for how each statement was prioritized on the Q-sort distribution by those who comprise that factor. The "rank" is the average ranking of that statement by those who represent that factor. The highest and lowest rankings are highlighted so as to illustrate the decision priorities that represent each type. Also, the statement numbers with asterisks (*) denote distinguishing statements between two types. With these distinguishing statements we went back to Jade to interview the senior executives and find out the reason behind different priorities. A type is defined by both the high and low priorities as well as distinguishing statements, since both distinguish any given type from others, and therefore the analysis proceeds by interpreting and defining the types based on their respective priorities.

Type 1: Business Focused Strategic Decision Makers

Type 1 can be characterised as business focused strategic decision makers. According to Weill (2004) 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 prioritised more strategic than technical type decisions which can be exemplified by these highly ranked statements: "Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (and potential risks)" (rank 1) and "Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities" (rank 5). Both questions fall under Weill's (2004) 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 in order to manage them and ensure that correct risks are addressed". When probed on another statement, "Organisation ISCP 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 what they do in practice also. Type 2 also mentioned that 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 IT principles category, hence it makes perfect sense that why it is ranked high by Type 1 in compare to Type 2.

Type 2: Technical Focused Tactical Decision Makers

Type 2 can be characterised as technical focused tactical decision makers. According to Weill (2004) they are IT monarchs and are comfortable in IT architecture, and IT infrastructure strategy types of decision making. They are involved in implementation of high-level views and are responsible for implementing IS resilience and ensuring day to day operation of the organisation. 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 [technical 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 overestimates the independence of the firm. 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 Prioritisation categories. According to Weill (2004) both type 1 and type 2 should consider the statement to be important. Surprisingly, Type 1 ranked it 34 while Type 2 ranked it 5. When probed we found that according to Type 1, top level strategic 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 technical oriented decision makers, "technology changes fast but from a technical 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 (2004) IT governance framework. Aligning Information Systems (IS) strategies with the strategic plan of the organisation" (rank 10) and "Adapting technology to strategic change" (rank 16). The first two statements fall under Weill's (2004) IT infrastructure category while the last two fall under the IT architecture category, and hence are more technical than strategic. Lastly, Weill's (2004) 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 over estimates the independence of the firm to ensure resilience.

Consensus between Types 1 and 2

Despite differences it is worth mentioning that there is a high correlation score (0.6018) between two types. This suggests that they are working as a team rather than as individuals. Providing reliable and consistent services to customers, capability for disaster recovery, setting up information disaster recovery system, resilient and accessible critical facilities and top management support and commitment to Information Systems (IS) resilience, which are critical to ensure IS resilience are prioritised highly by both types. The analytical procedure reports a list of "consensus statements", for which both Types 1 and 2 are in agreement. Related to IS resilience planning we found that both types are in favour of both "flexible and adaptable" and "well defined and structured" plans. This was neither predicted by Agency Theory nor by IT governance framework. Moreover, the statements are paradoxical in nature. We probed, and found that Jade uses a hybrid approach when it comes to IS resilience planning. Following the Christchurch earthquakes in 2010 and 2011 the committee has reviewed IS resilience plans and the most significant conclusion drawn from review was that the plans should move from a rigid hierarchy which were focused on recovering from an 'event based' model to a more flexible 'service recovery model', which is neither scenario nor event specific. The service recovery model identifies critical services, relates them to business need and specifies both service owners and consumers. This allows for a greater degree of flexibility in responding to different events and maintaining service-recovery documentation and process and ensures accountability. Some plans are well documented and structured, especially the DR, BC, Continuity of operations and Crisis Communication plans but some documents such as generic BCM Event Response Plan are flexible and adaptable. It outlines the high-level actions and decision making process required in a BCM event. It references more specific procedures contained in the BCM portfolio. The objectives and activities this document describes are to be carried out by senior and line management staff during and immediately following a BCM Event to safeguard the immediate interests of, and minimise damage to, staff and customers.

Theoretical Framework

It is clear that Jade is attempting to balance the contrasts between governance of profitability and governance for revenue growth and innovation. Jade operates on a federal governance design, so they can achieve both the synergies emphasised in centralised models and the autonomy allowed by more decentralised models. Their governing IT principles emphasise sharing and reuse of process, system, technology and data modules.

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	√						√	√	√	

Table 3. IT Governance of IS resilience at Jade Software Corporation

Table 3 shows our view (confirmed by senior management) of Jade's governance of IS resilience, reflecting responsibility for both decisions and input to those decisions. 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 organisational resilience is IS resilience. Thus, agile and successful IS resilience planning requires a subset of organisational capabilities. As learnt from Jade, essential components of successful IS resilience planning can be summarised 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 organisational goals and priorities must be formulated which has to be embedded in the organisation'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, so as 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 so as to remain flexible in adverse circumstances or times of crisis. As highlighted by the senior executives, "In time 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 on a regular basis to create an organisation wide resilience culture. As identified by Kayes (2015), "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 will be 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.

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 finding 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.

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

Conclusion

An important aspect of IT governance and IS research is to describe phenomenon and explain their functions. In this paper 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 emphasised the important distinctions as well as similarities among them and 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 differs from any existing research in that it is rooted in two popular theories, namely, Agency Theory and IT governance framework. To best of our knowledge, this is the first attempt to build the concept of IS resilience separate from the concept of organisational resilience, and it appears to be valid. The types we have identified are complementary to each other and give us a more precisely characterised set of variables and important decision priorities in context to IS resilience framework to work with. This should be useful for academics and practitioners interested in decision priority and successful IS resilience planning.

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, this is usually not considered a weakness by Q-method practitioners. This study is a starting point for further research into the IS resilience in large organisations. Also, the sample was restricted to Jade Software Corporation. There are a number of avenues of future research, including examining a greater range of organisations. Future empirical research should attempt to understand the IS resilience decision priorities and characteristics of resilient organisations, both public and private. Finally, results have implications both for researchers who are looking for theories that explain the importance of IS resilience and business managers and owners who are challenged with decisions about how to design resilient information system framework for their organisation.

REFERENCES

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

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

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

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

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

IBM. (2011). Key trends driving global business resilience and risk. IBM Global Technology Services.

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

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

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.

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.

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

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

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

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.