EMCIS

13th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2016)

Krakow, Poland, 23-24 June 2016

Online Proceedings of the 13th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS)

www.emcis.eu

GOVERNING INFORMATION SYSTEMS RESILIENCE: A CASE STUDY

Amitrajit Sarkar Department of Computing, Ara Institute of Canterbury, New Zealand, Amitrajit.Sarkar@ara.ac.nz

Dr. Stephen Wingreen Department of Accounting and Information Systems, University of Canterbury, New Zealand, stepehen.wingreen@canterbury.ac.nz

John Ascroft Chief Innovation Officer, Jade Software Corporation, New Zealand, jascroft@jadeworld.com

Abstract

Organisational resilience has gained increasing attention in recent years. This research focuses on an aspect of organisational resilience, i.e., on Information Systems (IS) resilience. To the best of researchers' knowledge, there is no study focusing on understanding the decision making process of senior executives in context to IS resilience in Large Organisations. The paper presents an in-depth case study of a large New Zealand organisation adapting with the aftermath of crisis, lessons learnt from them and also proposes a model for IS resilience planning based on IT governance framework.

Keywords: IT governance, IS resilience, TMT decision making, decision rights.

1   INTRODUCTION

To a large extent, most organisations are dependent on complex Information Systems (IS) and digital platforms to manage their businesses, which require IS to operate reliably under a variety of crisis situations. IS are considered as the most susceptible components in delivering continuous services. When interruptions affect IS operations, entire organisational ecosystems suffer from the disruption and its pouring effects (Maurer and Lechner, 2014). One crucial aspect of examining organisational resilience is to examine the continuance of stable and reliable IS services. To date, there has been no systematic examination on how IS resilience planning decisions are made. 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 strategic IS planning (Hann and Weber, 1996) and developing high level IT governance model, rather than inspecting previous disruptions and examining finer details of what really happened and how to prevent a recurrence and ensure IS resilience (Kayes, 2015). We see three problems with this prior research in particular. First, it is mainly prescriptive in nature, second, it describes what organizations should be doing with respect to IS planning practices, rather than what decision makers in organizations are actually doing and why they are doing so. Third, IT governance is on the agenda of many organisations but having a high level IT governance model does not ensure that governance is practically working in the organisation. So, more research is needed of the extension of IT governance concepts to IS resilience. To our knowledge there are no empirical validation which addresses these three aforementioned limitations, this will be an important contribution of this research. Moreover, to aid the study and practise of IS resilience, we propose a conceptual IS resilience framework, this will be another important contribution.

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. So, IS resilience encompasses a variety of IT decision types, while some decisions have a clear strategic orientation, others may address strategic, technical and business related objectives and rest may lie somewhere in between. Also, IS resilience plan is unique with respect to other types of plans because an IS resilience plan is intended to be implemented and executed during a time of crisis, when there is a high degree of uncertainty and ambiguity. In theory, IS resilience should be aligned with the overall organizational strategy, and therefore under the wider umbrella of organizational resilience. Increasingly, IT

governance receives a lot of attention with both academic and practitioners as the advantages of IT governance are being recognised (Weill and Ross, 2004; Grover, Henry and Thatcher, 2007). 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 elucidate why decision rights and responsibilities are spread the way they are. 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). It is therefore the goal of this research to develop and validate an IT governance framework in the context of IS resilience and to understand how the decisions are made by senior executives. Therefore, this study aims to examine, how senior executives make decisions to ensure IS resilience? Toward this goal, we have selected the Jade Software Corporation because it is an exemplar of the theoretical concepts we would expect in the context of IS resilience. Specifically, during the course of this study, Jade was enthusiastically involved in the domain of IS resilience planning, prioritization, and alignment in the result of a major crisis, the Christchurch earthquakes of 2011. Because of this, we expect Jade to be deeply engaged with IS resilience, and we should observe a full, rich range of IS resilience planning and decision-making.

Therefore, we adopt a grounded theory method to develop an initial model of the domain of IS resilience planning. Case study approach is appropriate for situations where research is in their early, formative stages and not supported by a strong theoretical base. Case studies are suitable for research objectives of an explanatory nature, which attempt to answer why and how questions that focus on contemporary events (Yin, 2004). Using semi-structured interviews, direct observation, and archival data, we construct causal map of the IS resilience planning and decision-making domain. The resulting causal map is derived from the in-depth interviews of a single case. This approach provided a means of obtaining the insights of practicing managers to understand the issues related to IS resilience planning in large organisation.

This paper is structured as follows. First, the literature on IS resilience, IT governance, IS resilience planning and IT governance framework is reviewed. The paper then describes the research methodology, in which the case study method is employed to determine how senior executives at Jade manifest their decision making and implement in order to ensure IS resilience. Detailed analysis of interviews with the executive management team has been documented to enrich our interpretation of the case study. The paper concludes with the discussion of necessary components of IS resilience planning framework. 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 LITERATURE REVIEW

2.1 IS Resilience

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 such as ecology, psychology or engineering, and different research contexts and topics, it is not surprising that the concept lacks an accepted common definition across disciplines (Muller, Koslowski and Accorsi, 2013). After an extensive literature review we have not been able to find a definition of IS resilience. However, organisational resilience has been studied extensively by researchers (Vargo and Seville, 2011; Hatton, Seville, and Vargo, 2012). In order to define IS resilience we have utilised six attributes as identified by McManus (2008), namely overall situation awareness, decreased vulnerabilities and increased adaptability, risk intelligence, flexibility and agility. These terms are defined in Table 1.

Set of Attributes	Definition
Situation awareness	It is the ability to identify and understand changes in the environment.
Management of Vulnerabilities	It is the capability to deal with the major vulnerabilities.
Adaptive Capacity	It is the capability to respond to and adapt to the changing environment.

Risk Intelligence	It is the ability to identify and anticipate risks.
Flexible	It is the ability to change.
Agile	It is the ability to produce timely responses to changing environment and conditions.

Table 1.   Attributes of IS Resilience

A definition of Information Systems 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 organisation'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.*

Traditionally the definition of resilience focuses on an event based approach that focuses on identifying potential risks and preparing response measures for each of them, whereas, our definition of IS resilience includes a process based approach to build sustainable business model. The process based approach embeds the resilience thinking in the culture of an organisation, which differentiates it from simply suggesting a corrective measure for a particular event (Vargo and Seville, 2011).

2.2   IS Resilience Planning

IS planning plays a crucial role in today's complex, connected, unpredictable and dynamic corporate world. IT is fused into all aspects of business operations and the need for strategic IS planning is of great importance in achieving success. It is defined as the process of strategic thinking that identifies the most required IS on which the organisation can implement and impose its long-term IS activities and policies. Earl (1993) stated that IS planning is a mixture of formal activities and informal behaviour. It can either be a special effort or part of overall organisational planning. However, very few organisations has successfully adapt to the demands of constant change by strategic use of IS. Prior 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)recognising organisational opportunities and problems where IS might be used successfully; (2)identifying resources required to allow IS to be applied successfully these problems and opportunities; and (3) developing strategies and processes to allow IS to be applied successfully to these opportunities and problems (Hann and Weber, 1996). Thus, IS planning process is recognized as an exercise to improve organisations' strategic alignment with business-IT objectives; to meet short-term and long-term organisational needs; and to provide the ability of creating impact on competitive advantages. The goals of IS planning include improving systems' architecture; infrastructure capability and reliability from IS/IT investments; managing information resources effectively; and securing user satisfaction. However, 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. Moreover, 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. IS resilience shares some commonality with crisis management. Crisis management is the process by which an organisation deals with any major unpredictable event threatening to harm the organisation, its stakeholders, and its customers and suppliers. Vargo and Seville (2011) stated, three elements are common to most descriptions of crisis: (a) a threat to the organisation, (b) the element of surprise, and (c) a short decision time. Crisis planning is about building to capability to identify looming threats to the organisation and designing a plan for addressing those threats. It is clear that IS resilience planning and crisis planning overlap considerably:

- they both deal with the future;
- they both deal with the weaknesses (vulnerabilities) and threats (risks)
- they both involve creating a plan
- they both involve organisational structures and resources to carry out the plan

However these two planning processes are typically carried out in isolation from one another, if they are carried out at all (Vargo and Seville, 2011).

2.3   IT Governance

IT governance has become an important issue in the organisations. While there are many definitions of IT governance exist but following two definitions are widely used in IS research.

> *IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives (IT governance Institute, 2001).*

> *IT governance is the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT (Van Grembergen, 2002).*

These definitions emphasise on the same aspects: alignment of business and IT, and the primary responsibility of the board and senior executives. Van Grembergen's definition also specifies that IT management must participate in the IT governance processes. It is important to note that there is a clear distinction between IT management and IT governance. IT management is engrossed on the effective management of IT operations and supply of IT resources, whereas, IT governance is much larger concept and focusses on performance and transformation of IT to meet present and future demands of the business and its customers.

IT governance describes a firm's overall process for sharing IS decision rights and monitoring the performance of IT investments (Weill and Ross, 2004). IT need to be governed to ensure corporate governance and it is evident from the definitions that IT governance is an essential part of enterprise governance and has a strong relationship with IS resilience. This relationship can be further established by translating the IT governance questions into specific IS resilience questions (refer to table 2).

IT Governance	IS Resilience
How does top management get the CIO and IT organisation to return some business value to it?	How does board get the senior executives to ensure IS resilience?
How does top management make sure that the CIO and IT organisations do not steal the capital it supplies or invest it in bad projects?	How does board monitor that the senior executives will prioritise and invest in the projects which will ensure IS resilience?
How does top management control the CIO and IT organisation?	How does board control the senior executives' decision priorities to ensure IS resilience?

Table 2.   IT governance questions are adopted from "IT Governance and Its Mechanisms" (Haes and Van Grembergen, 2004)

2.4   IT Governance Framework

Peter Weill's IT governance framework describes how decision rights and responsibilities are spread within the IT function in organizations, by his definitions of IT archetypes, and IT domains, but it does not elucidate why decision rights and responsibilities are distributed the way they are or how the decision makers make decisions. Weill's definition of an IT archetype involves the type of professional who has decision rights, and the IT domain comprises the decision responsibilities of each IT functional area (Weill and Ross, 2004). Decision rights indicate 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 essentially 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). Weill explicitly assumes that there should be alignment of decision makers' interests with the strategic interests of the firm. According to Weill, IT governance is not about explicit decisions about IT but about who makes what decisions, who has input and how the

decision makers are held accountable for those decisions. IT governance encompasses five major decision domains. First, IT principles comprise the high-level decisions about the strategic role of IT in the business. Second, IT architecture includes an integrated set of technical choices to guide the organization in satisfying business needs. Third, IT infrastructure consists of the centrally coordinated, shared IT services that provide the foundation for the enterprise's IT capability and fourth, business application needs are the business necessities for purchased or internally developed IT applications. Last, prioritization and investment decisions determine how much and where to invest in IT. Also, there are six archetypal approaches to IT decision making, ranging from highly centralise to highly decentralise. According to Weill most enterprises employ a variety of them, using different approaches for different decisions (Weill and Ross, 2004).

Currently, there is a plethora of IT management frameworks and standards, each catering to a narrow silo. A general lack of clarity still exists, when it comes to what constitutes an overarching IT governance framework focused specifically on the senior management's role. 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. IT governance can be deployed using a mixture of various structures, processes and relational mechanisms. A mixture of various structures, processes and relational mechanisms are deployed in organisations. IT governance structures include organisational units and their roles and responsibilities for making IT decisions. This can be proposed as an outline of how the IT governance framework will be structurally organised in an organisation. Further, IT governance processes refers to the formalisation of strategic IT decision making, IT monitoring and IT performance management procedures. Processes are important to ensure that daily practices are consistent with policies and provide a feedback to decisions. Finally, relational mechanisms are about active support and participation of senior executives, IT management and business management. Relational mechanism include education, training and empowerment of employees. An example of these structures, processes and relational mechanisms are provided in figure 1.
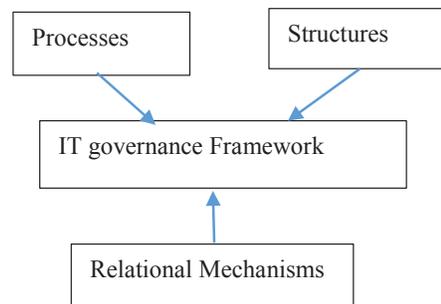
Figure 1.   IT governance framework

To complement the IT governance framework Control Objectives for Information and related Technology (COBIT) provides for 34 identified IT processes and their corresponding high-level control objectives and management guidelines for IT decision makers. Control objectives can help support IT governance within an organisation. COBIT's management guidelines also includes the maturity models for each of the 34 IT processes (Haes and Van Grembergen, 2004). The first process identified by COBIT is "define a strategic information technology plan." This process is vital to ensure strategic alignment. Different maturity levels are prescribed, for example, maturity level 1 requires that the need for IT strategic planning is known by IT management but there is no structured decision making process. Whereas, to achieve highest maturity level 5, IT strategic planning should be a documented and living process, continuously considered in business goal setting and resulting in discernible business value through investments in IT. High level control objectives can be implemented through the use of the IT infrastructure library (ITIL). Thus, COBIT's control objectives tell the senior executives what to do while ITIL explains how to do it. But it is important to remember that having a high-level IT governance model does not automatically imply that IT governance is working in reality in the organisation. In this

research focus is on who, what and how decisions are made 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.

3   A BRIEF INTRODUCTION TO JADE

The goal of this study is to develop and validate an IT governance framework in the context of IS resilience and to understand how the decisions are made by senior executives. The focus is on theory building rather than theory testing. Toward this goal, we have selected the Jade Software Corporation because it is an exemplar of the theoretical concepts we would expect in the context of IS resilience. 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. Jade's primary business operations are located within the disaster zone of 2010 and 2011 Christchurch earthquakes and as a result, suffered an unsettling blow to business operations. At the time of the adversities, the communications network and electricity cuts were challenging, with personal employee problems resulting in the days after the earthquakes. Jade had in place a full-bodied and prepared 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. As they were well organised, they quickly adapted to the changed environment and successfully met all contractual requirements throughout the crisis. As all the members of Top Management Team (TMT) at Jade have already experienced a crisis scenario, we expect to observe a full, rich range of IS resilience planning and decision making. Also, we will be able to learn from their experience how people learn to adopt and how lessons learnt during the crisis can make a difference later.

TMT is described as the link between the board of directors of a firm and the managers entrusted with the day-to-day functioning of the firm. Consistent with the description, Fama and Jensen (1983) have described them as the "apex of the firm's decision control system". Thus, TMT is an elite workgroup with a crucial role in firm's decision making and face complex, multifaceted tasks that involve both strategic and technical issues. TMTs are responsible for not only decision making but also for implementing and administering those decisions (Fama and Jensen, 1983). Jade has a committee that is responsible for risk management and IS resilience planning. The committee consists mostly of members of the 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. TMT's direct involvement and decision making before, during and after the crisis will add realism to this study. As mentioned previously in the definition of IT governance, it is crucial to have the roles and responsibilities defined unambiguously for an effective IT governance framework. Figure 2 implies that different committees has different memberships and authorities at Jade.

Figure 2.   Three layers of IT Governance responsibility at Jade Software Corporation

4   RESEARCH METHOD

We have conducted an in-depth case study with Jade Software Corporation. This case study is based on observations, archival analysis and in-depth interviews with their seven (7) senior executives who are the members of IS resilience committee. In this case study the goal was to understand, how *senior executives make decisions to ensure IS resilience?* Purpose of this research is theory building as oppose to theory testing. A major contribution of this research is to understand how IT governance structures, processes and relational mechanisms are applied by practitioners to ensure IS resilience and equipped with the experience and expertise of practitioners we would propose an IS resilience framework. The rationale for applying case research is based on the thoughts of Yin (2004). Yin (2004) used (1) type of research question; (2) the extent of control an investigator has over actual behavioural event and (3) the degree of focus on contemporary in contrast to historical events. Yin (2004) concluded that when a 'how' or 'why' question is asked about a contemporary set of events over which the researcher has little or no control, then it is appropriate to use case study method. Our research question clearly favours the use of a case study approach. Also, the research is focused on the contemporary issue of an organisation in making decisions to implement IS resilience. It is evident that our focus is not in their past decision making practices but more in current IS resilience priorities and practices. Finally, controlling behavioural events was not possible by the researchers.

5   FINDINGS AND DISCUSSION

Jade's IS resilience committee, which constitutes of seven (7) c-suite executives are distributed in two types of decision makers – (1) business focused strategic decision makers (type 1) and (2) technical focused tactical decision makers (type 2) (refer to table 3). In this study our focus is to develop and validate an IT governance framework in context to IS resilience and to have a deep understanding of how decisions are made by the top management team to ensure IS resilience.

	Type 1	Type 2
Type 1	1.0000	.6018
Type 2	.6018	1.0000

Table 3.   Factor correlation between Type 1 and Type 2 decision makers

5.1   Strategy-Implementation Bicycle

The Top Management Team (TMT) at Jade Software Corporation agree on most of the statements with high degree of correlations between factor scores (.6018). Both types are in nuances rather than in disagreement. So, we can say that they are functioning more like a team rather than individuals. Jade's IS resilience committee is made up of members from both business and technical divisions. Members has clearly defined roles to ensure IS resilience at Jade. Business focused strategists work in a high and

conceptual level predominantly dealing with the IT principles and IT investment and prioritisation type decision makings, whereas, technical focused tactical decision makers deal with the IT architecture and IT infrastructure related decision making and both type play an important role to make decisions related to business application needs. This split between strategy and implementation is very crucial for Jade to make right decisions which can be explained through "*Strategy-Implementation*" bicycle. This bicycle model will be helpful to visualise at a high and conceptual level the split and relationship between the strategy and implementation cycle. As shown in figure 3, the IS resilience committee based on the business/IT strategy drives the definition and application of the IT governance principles and priority rules. Based on the service level agreements (SLAs) they then define the critical services. Committee identifies the critical services and relate them to business need and specifies both service owners and consumers to imposes accountability and ensure smooth and uninterrupted delivery of services. The approved critical services are managed in strategy cycle. After decision has been made, critical services need to be implemented so they become part of implementation cycle. They are implemented and monitored in the implementation cycle. As a result of continuous evaluation, critical services may continue without any changes or may need to be innovated and re-enter the strategy cycle through a new critical service. This helps decision makers at Jade to identify the critical services early, evaluate different options to address them and implement a solution. As illustrated during interviews, "key risks are identified and understood and then we deal with them [risks]." Another executive stated, "we identify the key services first and then walk backwards to facilitate those services. This way a transformation happens from 'passionate drive from individuals' to 'service critical thinking'." The momentum generated due to this bicycle model in decision making shows that IS resilience plans are never parked at Jade but are living documents. This has been described and emphasised eloquently by several committee members; "In time of crisis plans go out of the window, it is important not to park those plans". "Planning is critical but continual review is important." "We had a plan and people knew what to do [during events of crisis]." This strategy-implementation bicycle has been verified with the senior executives at Jade.
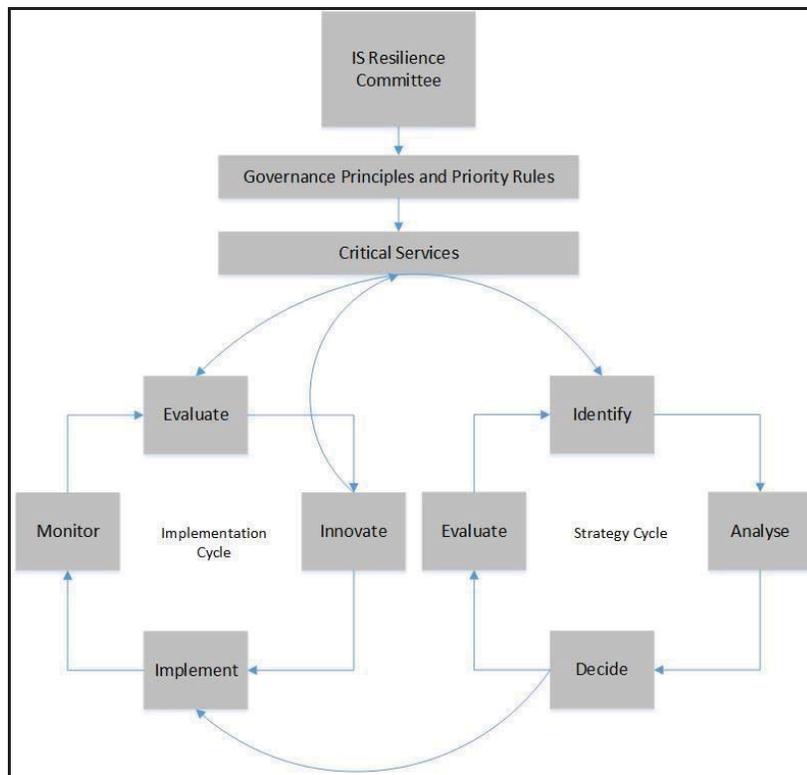
Figure 3: Strategy- Implementation "Bicycle" at Jade Software Corporation

Moreover, we have identified that "Strategy- Implementation Bicycle" at Jade is perfectly aligned to the concept of IT governance framework. IT governance has been defined as the accountability framework for IT decisions to enable desirable behaviours (Weill and Ross, 2004) and is viewed as a key responsibility of top management (Van Grembergen, 2002). The design of an organization's IT governance framework is recognized in the literature as involving key trade-off decisions. For example, when IT decision rights are exclusively allocated to an IT unit, there is a considerable risk that the business interests are not adequately considered, resulting in a lack of business/IT alignment (Van Grembergen, 2002). On the other hand, if IT decision rights are allocated to business units, reflections from a technical as well as an enterprise-wide perspective are not sufficiently addressed.

5.2   How senior executives make decision

We will now take a causal perspective to explore the decision making of two different types of decision makers at Jade Software Corporation. The important message here is that the model combines various causal subjective and objective factors derived from careful reflection. In figure 4, we explained how to think rationally of IS resilience in terms of causal model with trigger events, control events, risk events, mitigate events and consequence events. Causal model has been used to explain how the decisions are made and responsibilities are shared by senior executives at Jade. This is a major contribution of our study as it explains the "gut-feel" decisions, which is based on doing all the reasoning "in the head" of the decision makers or relying on intuition. The causal model helps us to explore "*what lies under the bonnet*". The causal model involves:

- The event itself

- At least one consequence event that characterises the impact

- One or more trigger events

- One or more control events which may stop the trigger event from causing the risk event

- One or more mitigating events which help avoid the consequence event

This is shown in the figure 4. With this causal perspective, our risk event is "compromised IS resilience", this event can be triggered by any form of disaster. The risk event also has a number of possible outcomes or consequences. Multiple controls can be put in place to avoid risk events and in case the risk event takes place then there are multiple mitigants that will reduce the impact of consequences. We found that the ability to decompose a IS resilience issue into chains of interrelated events should make decision making more meaningful, rational, practical and coherent. The causal model clearly shows that the consequences can be divided into two types according to Weill's IT governance framework, hence two types of decision maker in the TMT at Jade would complement each other to ensure IS resilience. As explained in the interview, "*IS resilience committee need wide spread knowledge, it is so complex that no one person understands it. We formed a collaborative team of members with different expertise. We have identified that not only having a plan is critical but execution of the plan is equally important". As a collaborative effort committee first identified key risks. In order to derive those risks we looked at the service level agreements and customer contracts, then we have done a thorough business impact analysis, we have graded customer contracts and SLAs to address various business impacts.*"
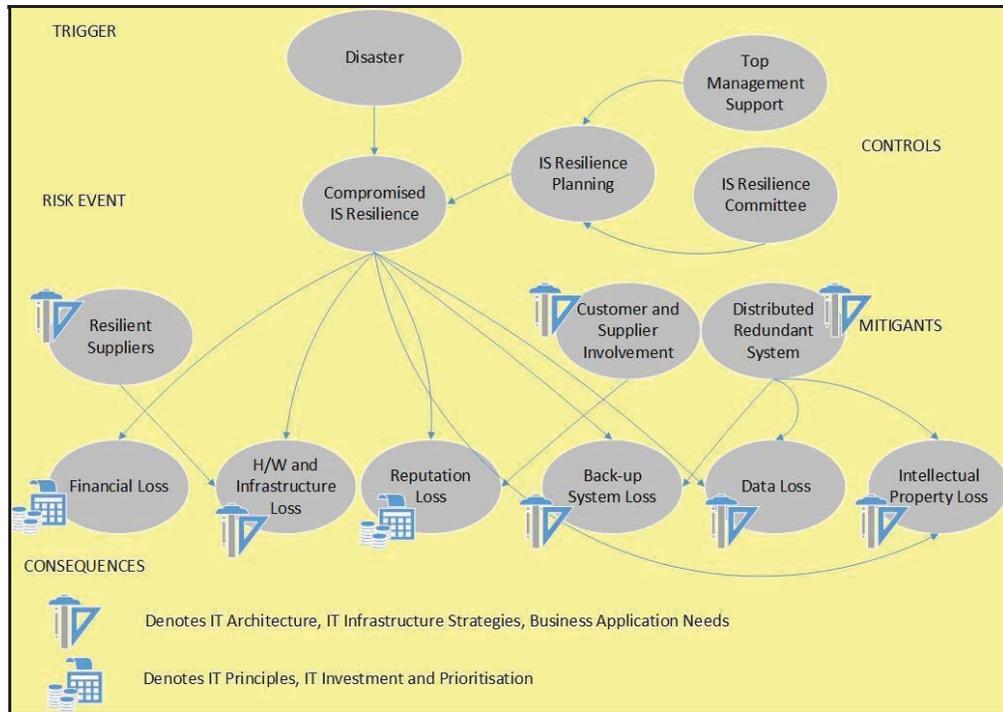
Figure 4: Causal Model for IS Resilience from the Decision Makers' Perspective at Jade Software Corporation

This causal model has been verified with the senior executives at Jade and key lessons learnt from Jade are shared below:

Structures: following quotes will help us to understand the IT governance structures in place at Jade. "We have plans, people knew what to do in time of crisis. Everyone has been trained and they have clearly defined roles and responsibilities." And "we work together as a team. Organisations are dynamic and very complex. No one person understands all. Right people doing the right stuff is critical." These quotes emphasise the importance of clearly defined roles and responsibilities and collective accountability. Delegating job to the right people and empowering staff was identified as critical in the interview. Another important factor was top management support, "it is absolutely critical to have support from the board….top management creates culture." Finally, there is an audit and compliance committee who has the specific responsibility for overseeing IT risks and monitoring IT priorities.

Processes: following quotes will help us to understand the IT governance processes in place at Jade. "We have detailed plans but ability to planning is important than the plan itself" and "it is important not to park those plans." The emphasis is on IS resilience planning process. The senior executives has also mentioned that "continuous review of these plans are critical" and "capability to implement the plan is equally important".

Relational Mechanisms: following quotes will help us to understand the IT governance relational mechanisms in place at Jade. "Prepare your people so that they can respond", "people should know what to do in crisis", "in time of crisis plans go out of the window…so empower staff so that they can be proactive to the recovery process." Relational mechanisms are very important. It is possible that an organization has all the IT governance structures and processes in place, but it does not work out because business and IT do not understand each other and/or are not working together. Or, it may be that there is little business awareness on the part of IT or little IT appreciation from the business. So, to reach effective IT governance, two-way communication and a good participation/collaboration relationship between the business and IT people are needed. Ensuring ongoing knowledge sharing across departments and organizations is paramount for attaining and sustaining business/IT alignment. It is crucial to facilitate the sharing and the management of knowledge by using mechanisms such as career crossover (IT staff working in the business units and business people working in IT), continuous education, cross-training, etc.

5.3   Necessary Elements of IS Resilience Framework

Our findings suggest that IT governance has significant influence for organisations when making decisions and assigning responsibilities and accountabilities. Though IS resilience framework is consistent with the existing IT governance framework, developed by Peter Weill (cites here) we have identified several unique attributes of IS resilience. This suggests that IS resilience planning is an instance of IT governance, however, it is distinct in several ways, and therefore justifies its own framework. For instance, IS resilience is unique because of high degree of ambiguity and uncertainty.

IT governance suggests that implementation of processes, structures and relational mechanisms that enabled both IT and business managers to execute their roles and responsibilities in support of business-IT alignment will create value from IT-enabled investments, in other words, alignment of business and IT strategies improves business performance of organisation. Figure 5 shows the necessary elements of IS resilience framework as derived from the case study.

Structures
C-suite executives in IS resilience committee, Top management support, Audit and compliance committee, clearly defined roles and responsibilities

Processes
IS resilience planning, Continuous testing and monitoring, SLA, BCP, DR, Service based approach, BIA, Response planning, Data centre plan, financial and legal plan, communications plan.

IS Resilience Framework

Relational Mechanisms
Active collaboration with suppliers and customers, Strategic dialogue, Regular and transparent communication, Education, training, knowledge sharing and empowerment.

Figure 5.   Necessary elements of IS Resilience framework.

6   CONCLUSION

The allocation of information technology (IT) decision rights between IT units and business units remains an important IT governance challenge. Companies that do not design an appropriate accountability framework for IT run the risk of business losses due to poor management decisions and misaligned IT priorities. While more detailed empirical work is necessary to elaborate and confirm the framework, it is believed that a useful starting point has been made. Understanding the decision making by senior executives to ensure IS resilience informed us to develop an IS resilience framework that encompass IT governance structures, processes and relational mechanisms. Effective IS resilience does not happen accidentally, rather requires thoughtful planning. We have described IS resilience planning in light of strategy-implementation bicycle and causal model is used to understand decision makers' perspective to understand decision priorities. 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. 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.This study contributes to the existing literature from both a theoretical viewpoint and a practical viewpoint.

7   REFERENCES

Earl, M. J. 1993. "Experiences in Strategic Information Systems Planning," MIS Quarterly, March: 1-27.

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.

Grover, V., Henry, R.M., and Thatcher, J.B. 2007. "Fix IT-business relationships through better decision rights", Communications of the ACM, 50(12):80-86.

Haes, S. D., and Grembergen, V., W.2004. – "IT governance and its mechanisms", Information Systems Control Journal, 1(1):27-33.

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

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.

Maurer, F., and Lechner, U. 2014. "From Disaster Response Planning to e-Resilience: A Literature Review," BLED 2014 Proceedings. Paper 32.

McManus, S., Seville, E., Vargo, J., and Brunsdon, D. 2008. "Facilitated Process for Improving Organizational Resilience," Natural Hazards Review, 3(4): 81-90.

Muller, G., Koslowski, T., and Accorsi, R. 2013. "Resilience – A New Research Filed in Business Information Systems," ACM Symposium on Business Computing, 55(4):1-12.

Vargo, J., and Seville, E. 2011. "Crisis strategic planning for SMEs: finding the silver lining," International Journal of Production Research, 7(3): 5619-5635.

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.

Yin, R. K. 2004. The Case Study Anthology, Thousand Oaks, CA, Sage.