Sustainability **2015**, *7*, 6149-6188; doi:10.3390/su7056149

OPEN ACCESS

sustainability

ISSN 2071-1050

www.mdpi.com/journal/sustainability

Article

Key Determinant Derivations for Information Technology Disaster Recovery Site Selection by the Multi-Criterion Decision Making Method

Chia-Lee Yang [1,2], Benjamin J. C. Yuan [1,3] and Chi-Yo Huang [4,*]

[1] Institute of Management of Technology, National Chiao-Tung University, Hsinchu 300, Taiwan; E-Mails: joy.yang@nchc.narl.org.tw (C.-L.Y.); benjamin@faculty.nctu.edu.tw (B.J.C.Y.)

[2] National Center for High-Performance Computing, Hsinchu 300, Taiwan

[3] Institute of Industrial Economics, Jinan University, Guangzhou 510632, China

[4] Department of Industrial Education, National Taiwan Normal University, Taipei 106, Taiwan

* Author to whom correspondence should be addressed; E-Mail: georgeh168@gmail.com; Tel.: +886-2-7734-3357.

Academic Editor: Rachel J. C. Chen

Received: 4 January 2015 / Accepted: 29 April 2015 / Published: 20 May 2015

Abstract: Disaster recovery sites are an important mechanism in continuous IT system operations. Such mechanisms can sustain IT availability and reduce business losses during natural or human-made disasters. Concerning the cost and risk aspects, the IT disaster-recovery site selection problems are multi-criterion decision making (MCDM) problems in nature. For such problems, the decision aspects include the availability of the service, recovery time requirements, service performance, and more. The importance and complexities of IT disaster recovery sites increases with advances in IT and the categories of possible disasters. The modern IT disaster recovery site selection process requires further investigation. However, very few researchers tried to study related issues during past years based on the authors' extremely limited knowledge. Thus, this paper aims to derive the aspects and criteria for evaluating and selecting a modern IT disaster recovery site. A hybrid MCDM framework consisting of the Decision Making Trial and Evaluation Laboratory (DEMATEL) and the Analytic Network Process (ANP) will be proposed to construct the complex influence relations between aspects as well as criteria and further, derive weight associated with each aspect and criteria. The criteria with higher weight can be used for evaluating and selecting the most suitable IT disaster recovery sites. In the

future, the proposed analytic framework can be used for evaluating and selecting a disaster recovery site for data centers by public institutes or private firms.

Keywords: disaster recovery (DR); site selection; business continuity (BC); data center (DC); decision making trial and evaluation laboratory (DEMATEL); analytic network process (ANP)

1. Introduction

During the past two decades, organizations have become increasingly dependent on information technology (IT) to enhance business operations, facilitate management decision-making, and deploy business strategies [1,2]. Therefore, IT system availability has become one of the most critical issues that attracted attention from both IT researchers and practitioners [1]. In particular, some organizations (e.g., financial institutes, healthcare organizations, high volume online retailers, government departments, utility companies, *etc.*) require that an IT system operates continuously; those organizations cannot tolerate any failure [3]. Thus, the increased demand for continuous operations of IT systems has created interest in disaster recovery sites (also called remote backup site) [3–7]. An IT disaster recovery site is a second location at which back-ups are available to the main data center in case of primary site failure [3,8]. IT disaster recovery sites would be able to restore data for the organization to ensure continuous operation, even in the presence of extensive failures that may render an entire site unoperational and for which local replication may be inadequate [9,10].

However, problems arising in disaster recovery site selection are practical, complicated, and usually involve massive subjectivities and uncertainties [11,12]. One reason is that disaster recovery sites are often regarded as a "necessary evil", an overhead cost that most organizations would prefer to keep to the minimum instead of being regarded as a revenue-generating function only. Another reason is that disaster recovery site selection decisions are contingent and resource dependent, which may vary based on the available resources, their effects, and their technology. Therefore, the challenges of evaluation and selection of disaster recovery sites has already become the most important issues for public and private firms.

Due to the dominant role of disaster recovery mechanisms on the continuous operation of data centers, various scholars have recently started to investigate related issues. A few researchers explored criteria on the selection of data centers [9,13,14]. However, based on the authors' very limited knowledge, very few or no research explored IT disaster recovery site selection in detail. In the real world, the criteria for evaluating a data center site or a disaster recovery site are different. One study on the evaluation and selection of disaster recovery sites in particular can help management make better decisions regarding their disaster recovery systems. Although some consulting firms (e.g., Cisco, RATH, BSI) proposed specific criteria for disaster recovery site selection, they fall short of the derivation procedure and the calculation of weights being associated with that criteria.

To fill the research gap, this study aims to define an analytic framework for IT disaster recovery site selections. Key decision factors for both public and private sectors were derived, and we explored the context of disaster recovery site selection and proposed an evaluation model for IT disaster recovery

site(s). Based on knowledge in the related areas of disaster recovery, information technology, decision science, and international standard consultancies, the decision-making framework can be developed.

First off, this study will review literature regarding possible aspects that should be used in evaluating and selecting a disaster recovery site. Possible alternatives (or the disaster recovery sites) will also be proposed according the situation of the target organization being studied. These aspects and criteria will be confirmed by experts through the focus group interviews. Then, a hybrid MCDM model combined with the Decision Making Trial and Evaluation Laboratory (DEMATEL) and the Analytic Network Process (ANP) will be introduced. The DEMATEL will be used to construct the decision-making framework. The ANP will then be introduced for the weights corresponding to each aspect and criterion. The performance scores *versus* each criterion will then be graded by the experts. The weighted performance score *versus* each alternative will be aggregated by the simple weighted method. An empirical study on evaluating and selecting a disaster recovery site for a Taiwanese research institute will be used to demonstrate the feasibility of the proposed framework.

The rest of this paper is organized as follows: a literature review on disaster recovery and site section is presented in Section 2. The research methods of the multi-criteria decision-making framework will be presented in Section 3. The empirical study for evaluating and selecting a disaster recovery site for a leading Taiwanese research institute will be presented in Section 4. Advances in management practices and the comparisons between the empirical study results *versus* past research results will be provided in the Discussion Section. Finally, Section 6 summarizes the results and concludes the paper.

2. Literature Review

In order to review the latest disaster recovery site selection researches and to construct an analytic framework accordingly, related literature was reviewed and summarized below. This literature review focuses on IT disaster recovery and site selections, with a focus on past studies regarding the evaluation criteria for the selection of IT disaster recovery sites.

2.1. Disaster Recovery

A disaster, by definition, is a destructive event that results in victims; further, discrepancies arise between their number and the treatment capacity. An accident is similar to a disaster, but refers to an event without victims [15,16]. The impact of disasters can further be classified into the direct and indirect ones. The direct impact of disasters include human injuries, facilities damages, and equipment losses [17,18]. Indirect impact includes business operation interruptions, property value reductions, stock market fluctuations, and possible social and environmental effects [18]. Disasters may occur as the result of unpredictable conditions or underestimated risks, anything from natural disaster, a technical accident, or a system failure [19]. Usually, controlling and preventing disasters is very difficult. Thus, the ability of an organization to recover from a disaster is very critical.

Disaster recovery is defined as the process of recovering an organization or a project affected by some specific damage(s) to its state before the disaster [19]. Early disaster recovery literature concerns various types and impacts of natural disasters (*i.e.*, Loma Prieta Earthquake in 1989, Great Midwest Floods in 1993, Northridge Earthquake in 1994, Red River Flood in 1997, *etc.*) and their different influences on individuals, households, communities, and organizations from environmental and social

viewpoints [20–26]. Over the past two decades, an increasing number of publications and empirical studies have started to focus on the organizational capabilities to respond and recover after disasters [27,28]. Apparently, the emphasis has been changed from the influences of natural disasters on human injuries directly to the potentially catastrophic impact on the business [19,29]. In particular, researchers have started to emphasize the assessment of information infrastructures for disaster recovery after the 11 September 2001 terroristic attacks [30,31]. During the past decade, as information infrastructure availability has become the critical issue for both IT researchers and practitioners, the importance of IT disaster recovery can hardly be overestimated [1].

2.2. Disaster Recovery and the Modern Business Perspective

Traditionally, the disaster recovery was recognized as a set of procedures to recover and protect IT infrastructure when computer(s) shut down accidentally. According to Jon William Toigo, the author of Disaster Recovery Planning, 15 or 20 years ago a disaster recovery plan might consist of powering down a mainframe and other computers, disassembling components, and drying circuit boards in the parking lot with a hair dryer [32]. Thus, the disaster recovery problem was often regarded as the problem belonging to the IT organizations. This recognition assumes that the disaster recovery problem can simply be resolved by constructing good backup system(s) for computers or computer networks. However, this assumption is not realistic as IT systems are gaining greater prominence in the overall structure of most corporations. Except for the traditional IT context, the disaster recover problems are now related to business operations. The seriousness of this problem is supported by a research from Faulkner Information Services, which found that 50% of companies that lose their data due to disasters go out of business within 24 months [33]. Further, the number of organizations that rely on computerized systems to perform daily operations and assist in the decision making process has grown at a rapid pace recently and still continues to grow [34]. Therefore, the disaster recovery problem should be reviewed further from the modern business perspective.

Disasters are significant outages with a greater critical impact to the modern business [10]. Nowadays, there are many more threats except for the natural hazards. Snedaker [35] summarized novel disasters to include human-caused hazards, accidents and technological hazards, electronic data threats, *etc.* Disasters may strike at any moment in any location [36]. Therefore, disaster recovery is becoming increasingly complicated.

As observed by Torabi and Mansouri [37], businesses are increasingly subject to disruptions; it is almost impossible to predict their nature, time and extent. So, the concept of organizational resilience is attracting growing attention among academicians and practitioners [37]. The organizational resilience enquires organizations to develop effective plans for both short-term resuming (*i.e.*, business continuity plans) and long-term restoration *(i.e.*, disaster recovery plans) of their disrupted operations following disruptive events [38]. However, lack of proactive business continuity and disaster recovery planning may lead to loss of reputation and market share, customer service and business process failure, regulatory liability and increased resuming and restoring times [37,39–41].

Most companies' IT systems are too complex to be recovered by using the traditional approach [32,42]. Being prepared for disruptive events requires proactive planning of internal and external resources of the organization so that it can cope with disasters effectively and efficiently [37]. Disaster recovery in

the modern age is a detailed, step-by-step course of actions for quickly recovering after a natural or manmade disaster; the details may vary depending on the business needs, and can be developed in-house or purchased as a service [42]. In general, the disaster recovery has been re-focused on a broader scope, from the traditional IT recovery and protection to the modern organizational processes which affect business operations. Organizations need a proactive approach equipped with a decision support framework to protect themselves against the outcomes of disruptive events [37].

2.3. IT Disaster Recovery

Data centers (DC) have become critical infrastructures for most modern organizations in information society, as eCommerce, cloud-based storage, and a variety of more generic online services are introduced and adopted. Such a trend has become especially significant in the era of cloud-based computation. However, the DCs can easily be affected by a small isolated disaster. Therefore, more and more researchers advocate for IT disaster recovery, the process by which computer systems and the associated infrastructure(s) can be recovered after a service disruption [4].

An IT disaster recovery site is a backup data center that aims to replicate data to a remote location and synchronize those data with the primary site in case of primary site failure [3,43]. IT disaster recovery sites would be able to restore data and keep an organization's IT system operating during or after a disaster [3,9,10]. Since such IT disaster recovery problems happen frequently in the real world, a majority of previous studies were based on empirical studies by consultants or IT companies. Most real world organizations established disaster recovery sites based on the international standards proposed in the International Standard Organization (ISO), International Electro-technical Commission (IEC), International Telecommunication Union (ITU) and national regulations.

The majority of research on IT disaster recovery focused on process or storage technology [8,44], but very few focused on IT disaster recovery site selection, which usually involves multi-disciplinary knowledge such as massive IT, business process, and decision subjectivities [11,12]. For instance, Sembiring and Siregar [3] described risk factors related to information technology, IT organization, and business process, which influence disaster recovery site evaluations and selections from the enterprise architecture perspective. The work by Sembiring and Siregar aims to decide the appropriate disaster recovery DC standard levels (called 1–4 tier) instead of site selection [3].

2.4. Site Selection

Site selection problems have been studied widely and can be found everywhere in the real-world governmental, industrial, or firm level management decision problems. For example, Garcia [45] studied the agricultural warehouse site selection failure, in which an agricultural warehouse localization error could drive business to bankruptcy [45]. Rikalovic [46] discovered that new industrial park site selections are very critical to the successes of the industrial innovation systems [46]. Pereira (2014) found that the power station and the carbon dioxide site selection problems are the most important when it comes to national economy and security [47].

Various groups have worked on site selection problems, and opinions differ as to "where is a suitable site" and "how to select a site". Some scholars advocated that selection of a suitable site requires considerations of various aspects and criteria, especially the facility location. For example, Wang *et al.* [48]

summarized environment and economic factors, including price and distance and constructed a hierarchical decision-making framework for solving the solid waste landfill site-selection problem. Covas *et al.* [14] argued that considerations for evaluating a new data center location site from an energy efficiency perspective, mainly because data centers need a large amount of power for computing equipment and their infrastructure. Other researchers put more emphasis on the site selection procedure and treat site selection as the first step of a comprehensive decision making process [46,49]. A number of studies are based on different decision making methods for evaluating ideal locations. These methods include expanding the classification or scoring methods [50], the Analytic Hierarchy Process (AHP) [51] and the Linear programming (LP) approach [52].

2.5. International Standards of Disaster Recovery

According to Herbane *et al.* [39], many organizations adopted/installed business continuation management due to avoid turning away customers, configuration resilience, or obligation [39]. For these reasons, obligation is the most significant factor influencing the disaster recovery site selection. Some organizations (such as utilities, telecommunications, public sector, financial institutions, health care, *etc.*) have disaster recovery sites or, broadly speaking, a BCM due to legal responsibility; such disaster recovery sites need to be certified by international standards or national regulations [53]. Such international standards being related to IT disaster recovery include ISO, IEC and IUT, as summarized in Table 1. Some standards serve as a high-level framework or guideline of business continuation and information security management, such as ISO 22301: 2012, ISO/IEC 27002: 2013, *etc.* Others focus on Disaster Management, Disaster response policy, and more detailed technology, such as ISO 27031, and ISO 24762.

Table 1. International standards for disaster recovery sites.

Standards	Plan			Tool Kits		
	Business Continuation Management	**Information Security Management**	**Disaster Management**	**Control Policy**	**Control Procedures**	**Recovery Technology and Facility**
ISO 22301: 2012	V			V		
ISO 22313: 2012	V			V	V	
ISO/IEC 27001: 2013		V		V	V	
ISO/IEC 27002: 2013		V		V	V	V
ISO/IEC 27031: 2011	V	V	V	V		
ISO/IEC 24762: 2008	V	V	V		V	V
ITU-T L.92 (10/2012)	V		V		V	V
ITU-T L.1300 (11/2011)	V		V			V

In some counties, disaster recovery sites are regulated by national government. Such governments defined the disaster recovery site selection guidelines (refer to Table 2). For example, according to the 2003 Information Security Management Act (FISMA) in U.S., critical information assets need to be protected with remote backup and information security plans [54]. The U.S. National Institute of Standards and Technology (NIST) enacted regulations of the SP 800-34 in 2006, which requires high and medium level public sectors to implement the Business Impact Analysis (BIA) process and set up

disaster recovery sites. The main emphasis on disaster recovery site selection is to assure backup data confidentiality, procedure integrity and availability [55].

Table 2. National regulations for disaster recovery sites.

Nations	National Regulations	Organization	Information Security Management	IT Disaster Recovery Plan	DC Management	Telecommunications
US	NIST Special Publication 800-34(SP 800-34)—Contingency Planning Guide for Federal Information Systems	National Institute of Standards and Technology, NIST	V	V		
	Telecommunications Infrastructure Standard for Data Centers:TIA-942	American National Standards Institute, ANSI	V	V	V	V
Japan	Data Center Facility Standard	Japan Data Center Council, JDCC		V	V	
Korea	TTAS.KO-10.0259 on Guidelines for Disaster Management of Information Systems	Telecommunication and Technology Association, TTA	V	V		
Taiwan	Information Security Management Directions for the Executive Yuan and its Subordinate Agencies	Executive Yuan	V	V		
	CNS27001: Information technology—Security techniques—Information security management systems -Requirements	Bureau of Standards Metrology and Inspection, MOEA	V	V		
	The norms of Information and Communication Security Management in Educational Systems	Ministry of Education	V	V		
Saudi Arabia	Guidelines on disaster recovery Planning for ICT Industry	Communications and Information Technology Commission, CITC		V		V

In contrast to the well-regulated public sector organizations, a majority of private firms did not define BC management or disaster recovery plans [4]. However, as a result of the 11 September terrorist attacks, the U.S. Department of Homeland Security is developing a "Voluntary Private Sector Preparedness Accreditation & Certification Program" [4]. This voluntary program proposes a guideline for certifications for businesses, not-for-profit corporations, hospitals, stadiums, universities and other

entities. This program promotes private sector entities to seriously consider certification of their disaster recovery systems.

The above mentioned site selection studies demonstrated that no specific approach for site selections were available. Most scholars agree that the site selection decision making frameworks vary for different problems and no one site selection plan was proposed to deal with unpredicted phenomena [56,57]. To date, no systematic studies have been carried out concerning disaster recovery site selection for data centers.

Based on the very limited knowledge of previous studies, there is a significant research gap between the availability of research work *versus* the actual needs for the analytic frameworks for IT disaster recovery site selections. Therefore, this paper attempts to investigate disaster recovery site selection criteria, propose an analytic framework, and verify the analytic framework by an empirical study case. Disaster recovery site selection problems include a complex array of evaluation aspects and criteria. Such aspects and criteria always include economic, technical, and environmental and risk management issues, which may result in conflicting objectives [46]. This study aims to render a new study by proposing a hybrid MCDM framework, combining aspects from international standards and regulations and summarize the technical and business management related aspects and criteria. The analytic framework can serve as the basis for evaluating and selecting disaster recovery sites for BC by IT managers and researchers. This study is among the very few studies in this field combine international standards, regulations and enterprise architecture.

Furthermore, as disaster recovery related standards and regulations have been developed in the developed countries, such as US, UK and Japan, it is difficult for small and medium enterprises in developing countries to adopt such standards and regulations. The practical cases of this study are from Taiwan and attempt to provide guidelines for disaster recovery sites in developing countries.

3. Analytical Framework and Methods

In this Section, an MCDM framework for a disaster recovery site selection will be developed. Decision criteria will first be summarized based on literature review results. The literature has been collected based on academia journal papers, international standards, national regulations and others as needed to develop a nation's disaster recovery principle. Possible criteria for evaluating a disaster recovery site are summarized based on the literature review results. Then, the focus-group method is introduced to confirm the criteria being derived. The initial weight *versus* each criterion will be calculated by the ANP. Based on the criteria and weights being derived, a decision making framework for a disaster recovery site selection can be established. In summary, this decision making framework consists of three major phases: (1) deriving determinants using the focus group method; (2) constructing a network relation map among determinants by using the DEMATEL; (3) calculating the weight *versus* every determinant by using the ANP based on the NRM being constructed in the phase (2). The flowchart is shown in the following Figure 1. Meanwhile, details of the methods will be introduced in the following subsections and in the Appendices A and B.

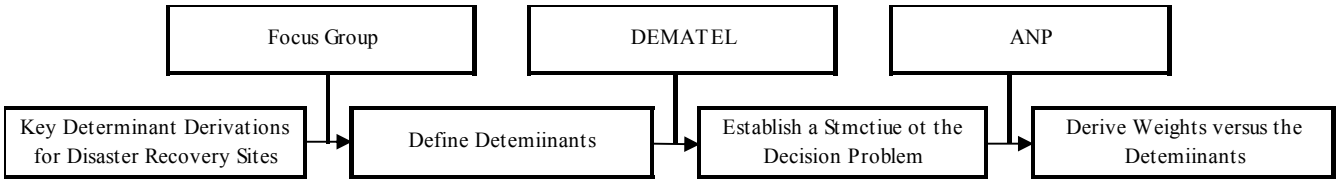

Figure 1. The flowchart of decision making framework.

3.1. Focus Group Method

The focus group method is believed to have originated in the USA and is most usually attributed to the sociologist Robert Merton [58]. The term "focus group" is generally assumed to have derived from the focused interview developed by Merton and his colleagues at Columbia University during the 1940s, when investigating audience reactions to radio programs [59]. During the past few decades, the focus group method has emerged from a number of different disciplinary locations including anthropology, sociology, psychology, education, and advertising, all of which provide different theoretical perspectives on focus group research today [58]. The focus-group is a powerful qualitative research tool which has widely been applied in various academic fields during the past decades.

Using a focus-group method in research is to acquire as much information as possible from a group of experts on a given topic. Such method can be accomplished by prompting the group with pre-specified topics, allowing the discussion to evolve around these open-ended questions, and facilitating interaction among the participants. The focus group process allows participants to interject their own observations and knowledge while also feeding off of the ideas of other participants The focus group further allows a researcher to extract expertise and insights from the participants [60,61].

In the focus group meetings, the participants received feedback about the first round panel results; the meeting was chaired by a consultant pediatrician who had not been previously involved as a participant in the design of the study. The chair person was asked to facilitate discussions and to allow all participants to speak. All participants were encouraged to contribute to the discussion, which was recorded with the consent of the participants.

Focus groups have been used frequently in IT-related studies to address emerging technology-driven phenomena [62]. In this research, the focus group method was chosen because the IT disaster recovery site selection problem is an emerging phenomena in which the available data is very limited and unexplored. Focus groups allow us to derive experts' experiences and perspectives, while also exploring their beliefs and attitudes.

3.2. DEMATEL Method

The DEMATEL method, an MCDM approach originated from the Geneva Research Centre of the Battelle Memorial Institute [63], has typically served to address the question of "whether solving a problem can help solve another one?" The DEMATEL method can convert complex systems into a clear causal structure which simplifies the interrelationships among consideration factors; as a consequence it assists in locating the core issues and quantifies their causality and influence strength [64,65]. In recent years, the DEMATEL method has been popularly applied in diverse fields including decision-making [66,67], technology innovation [68,69], knowledge management [70], operations

research [71], marketing and consumer behavior [72], and competence and performance evaluation [73], *etc.* As the experts of disaster recovery site selection are understandably limited and our research goal is to identify the causation and influence strengths of the consideration factors, we employed the quantitative DEMATEL method in this research. The detailed procedure of the DEMATEL method will be introduced in Appendix A.

3.3. The ANP Method

The ANP method, developed by Saaty [74], provides a general framework to deal with decisions without making assumptions about the independence of higher-level elements from lower level elements and about the independence of the elements within a level as in a hierarchy [75]. ANP is a flexible MCDM approach that can be used to imitate human thinking process resolving complex decision-making problems with some impact factors through analyzing, estimation and synthesizing processes, and so on. The relative importance of the factors can be confirmed through pair-wise comparing each element in the corresponding level and calibrating them on the numerical scale and sequences about the relative importance of the decision-making factors can be determined by synthesizing the judgment of domain experts. ANP method has been widely applied to site selection decision making, such as: shopping center selection [76], landfill site selection [77] and so on. Compared with traditional MCDM methods, e.g., AHP (Analytic Hierarchy Process)—which usually assume the independence between criteria, ANP is a more effective tool for dealing with dependence in feedback in the real world [74,78]. ANP structures a decision problem into a hierarchy as a network. The detailed procedure of the ANP method will be introduced in Appendix B.

4. Using the Hybrid MCDM Method in Evaluation and Selection of a Disaster Recovery Site for the Computing Facilities of a Taiwanese Research Institute

Taiwan is ranked as the world's 12th economy out of 142 listed in global competitiveness rankings [79]. Reflecting on the fact that Taiwanese companies have been active in the information and communication technology sphere for many years, Taiwanese ICT firms now possess first-class hardware design and software development capabilities, flexible production management capabilities, strong global logistics capabilities, and many years of experience in collaborating with leading international brands [80]. Taiwan has made significant progress in research and development of data centers. Therefore, the disaster recovery site is the challenge being faced by both public and private sectors. Based on the experiences from other large landscape countries like Japan and the U.S., the Taiwanese disaster recovery system can be viewed as a different strategy—more flexible disaster recovery guidelines for different sectors. The disaster recovery plan in Taiwan is focused on IT solutions, such as Internet Virtual Private Network, disk, and backup type and so on. This section reviews an empirical study based on the selection of a disaster recovery site for the computing facilities of a Taiwanese research institute.

When considering geographic location, Taiwan is an island facing frequent risks from natural disasters [81]. In 2005, the World Bank report titled "Natural Disaster Hot Spots—A Global Risk Analysis" indicated that Taiwan might be the most vulnerable area to natural hazards on Earth; 73% of the land and population are exposed to three or more hazards. The five major natural hazards

confronting Taiwan include typhoons, earthquakes, landslides, floods, and debris flow [82]. Such natural hazards have caused significant economic losses. According to the statistics being provided by Hale and Moberg [20], typhoons have resulted in annual economic losses of about $667 million USD in average [20], with an average of 3.6 typhoons per year. In addition to natural disasters, Taiwan is also one of the most targeted economies for malware [83]. Combined, these natural and human made disasters stimulated governmental actions in designing an emergency management mechanism and disaster recovery systems and technologies to reduce the negative impacts of such disasters.

In order to construct disaster recovery sites for the Taiwanese data centers, this study aims to define a decision-making framework based on MCDM methods. All the possible criteria for evaluating DR sites will be derived based on experts' opinions. The experts were selected from the participators of the Taiwanese task force for defining "The Guidelines on Disaster Recovery Mechanism of IT Data Center". The task force was initiated by the National Information and Communication Security Taskforce (NICST) of the Executive Yuan, Taiwan. This project is the first official one for defining the reference guidelines for evaluating the disaster recovery mechanisms in public or private sectors. The experts being selected include the 5 IT managers who are responsible for disaster recovery decisions of the Taiwanese Critical Information Infrastructure (CII), 4 IT consultants who are responsible for the international standard definitions of business continues management, 2 IT researchers who work in data centers, and 1 government officers who were responsible for information security policy. All the experts are with more than 5 years of work experiences in the related fields of business continues management and disaster recovery plan definition.

After confirming the qualification of experts, the direct relation/influence matrices will be derived. The possible aspects and criteria for evaluating disaster recovery sites will first be derived based on comprehensive literature review results. Government and industry standards and existing enterprise IT architectures were considered. Then, experts were invited to provide their opinions. Details regarding every aspect and criteria were derived based on the experts' opinions. The decision will be structured based on the aspects and criteria being derived by using the DEMATEL method. Finally, the key determinants for DR sites will be derived using the ANP method. These detailed procedures will be demonstrated in the following sub-sections.

4.1. Aspects and Criteria Derivations by Using the Focus Group Method

At first, the focus-group method being introduced in Section 3.1 was introduced to derive the opinions of 12 Taiwanese experts. The focus group meeting was chaired by a consultant pediatrician who had not been previously involved as a participant in the design of the study. The chair person was asked to facilitate discussions and to allow all participants to speak. All participants were encouraged to contribute to the discussion, which was recorded with the consent of the participants. Based on the results being concluded by the experts in the two iterations of focus groups, five aspects and twenty-two possible criteria for evaluating and selecting a disaster recovery site were derived and demonstrated in the following Table 3.

Table 3. Candidate aspects and criteria for evaluating disaster recovery sites.

Aspects	Criteria	Descriptions
Location and Infrastructure (A)	Natural Disaster (a_1) [35]	An appropriate disaster recovery site should minimize influences by natural disasters. As summarized by Snedaker [35], the natural hazards can be classified into cold weather or warm weather related hazards and geological hazards.
	Manmade Disaster (a_2) [35]	Appropriate geographic location prevents the human-caused hazards. According summarized by Snedaker [35]), the manmade disasters include terrorism, bomb, explosion, fire, cyber-attack, civil disorder, protests, product tampering, radioactive contamination, embezzlement, kidnapping, extortion, and subsidence.
	Distance From Primary Site (a_3) [84]	The distance between the primary and backup recovery sites depends on the risk assessment; the recovery site must be far enough away so that the same catastrophe does not strike both sites [84].
	Transportation (a_4) [85]	The transport network including roads, airports, port, and railways provides essential access to available resources needed for a country's rapid and successful recovery [85,86]. The transport system is critical during a natural disaster due to its pivotal role in resourcing recovery. The high cost of resource transportation and lack of transport alternatives were major barriers to post-disaster reconstruction.
	Electricity and Cooling (a_5) [84,87]	The disaster recovery site should have stable power and a cooling system to prevent power outages and system shut down. The major consideration from the aspect of electricity include: monitor the line and filter out spikes, provision of additional power in case of a brownout or partial outage, provision of sufficient temporary power in case of a total outage, and ensure the transition from normal power supply to emergency power supply without loss of service to critical devices [84]. Meanwhile, as the amount of heat that newer equipment discharges per square foot of space, cooling equipment are becoming daily important [87].
	Detection and Monitoring (a_6) [88]	The management of a computer security system involves intrusion detection and monitoring of the entire enterprise's computers [88]. The disaster recovery site's building should have fast detection, monitoring alarm and operate equipment and design.
IT System Availability (B)	Backup Strategies (b_1) [84]	Proper backups of critical data can survive the organization from a disaster. Effective backups that completely protect critical data require thorough planning. According to Wallace [84], the backup strategies include full system backup, incremental backup, and differential backup.
	Backup Servers (b_2) [89]	Back up in virtual servers, physical servers, and cloud servers. Any backup solution must maintain the transactional integrity of the data so that, when the data is restored, it is left in a transactionally consistent state [89].

Table 3. *Cont.*

Aspects	Criteria	Descriptions
IT System Availability (B)	Backup System Architecture(b_3) [90]	According to Brooks *et al.* from IBM [90], backup system architecture and planning plays a critical role in the recovery phase as systems are rebuilt, applications are restored, data is recovered, and systems are put back online into production. Data recovery operations must work synergistically with overall disaster recovery operations. At the completion of the recovery phase, systems will be functioning to the extent determined in the plan. Beyond the critical recovery phases, less critical recovery operations may ensue.
	Telecommunication Infrastructure (b_4) [84]	The infrastructure of telecommunications, which includes internet bandwidth, fiber backbone route, and transaction time/latency. Key concerns include natural and man-made hazards, telephone equipment room (temperature, humidity, *etc.*), internal and external cabling, and route separation.
	Carrier and Support (b_5) [91]	Telephone companies and long distance carriers offer a wide range of virtual network services; loss of virtual network services, like traditional long distance service, can severely impair a company's ability to conduct business [91]. All carriers being present in the vicinity and their support and service models in place. e.g., different source of carriers to avoid unexpected interruption by one carrier.
Disaster Recovery Objectives (C)	Recovery Point Objective (c_1) [92]	Recovery Point Objective describes the acceptable amount of data loss measured in time; the Recovery Point Objective is the point in time to which data must be recovered as defined by the organization [92].
	Recovery Time Objective (c_2) [92]	The Recover Time Objective is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity
	Testing and Exercises (c_3) [92]	The purpose of testing is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Testing may include: crisis command team call-out testing, technical swing test from primary to secondary work locations, technical swing test from secondary to primary work locations, application test, and the business process test. Three types of exercise can be employed when testing the business continuity plan: simple, medium and complex exercises.
Disaster Readiness exercises (D)	Education and Training (d_1) [93]	Regular training and education programs for disaster recoveries, which include operations, technology, information security, and DRP processes. According to Smith (2012), training, education, and outreach initiatives; and the funding needed to implement them—can play an important but often overlooked role in recovery [93].
	Disaster Recovery Work Area (d_2) [87]	Establish an area where critical IT workers can work during and after the recovery operation [87]. The physical precinct in a disaster recovery center, including operation area, equipment handling, and testing area.

Table 3. *Cont.*

Aspects	Criteria	Descriptions
Disaster Readiness Exercises (D)	Emergency Operations Center (d_3) [84]	An Emergency Operations Center is a physical place where all the communications of the recovery effort are focused. The Emergency Operations Center is essential when addressing serious or wide-scale disasters. It allows a company's management to reestablish organizational leadership, allocate resources, and focus on emergency containment and recovery.
Operation Management (E)	Project Management (e_1) [35]	The project management plan of a disaster recovery site, such as the plan–do–check–act continuous quality improvement model. Elements of project success include: executive support, user involvement, experienced project manager, clearly defined project objectives, clearly defined project requirements, clearly defined scope, shorter schedule, multiple milestones, and clearly defined project management process [35].
	Information Security Management Procedure (e_2) [35]	A disaster recovery site should be certified by information Security standards and renewed regularly, such as ISMS, BS 7799, *etc.* As summarized by Snedaker [35], the information security management should be based on an analysis of the most recent, more developed information security statutes, and responsibility for compliance increasingly rests with the BoD or CEO. The development and maintenance of a process-oriented written information security program (WISP) is critical to the ability of a company to meet its legal obligations as it relates to the management of information security. The legal standard dictates minimum requirements your WISP must address, limited to: (1) specific security measures; (2) specific requirements for third-party service provider arrangements; and (3) specific requirements regarding the education of the WISP.
	Disaster Recovery Procedure (e_3) [94]	Disaster management is the discipline of dealing with and avoiding risks; the availability of a good disaster recovery procedure and emergency response plan in place [94] is essential for successful; disaster recovery. A disaster recovery site should have well-documented process of disaster recovery plan to recover and protect a business IT infrastructure in the event of a disaster.
	Top Manager's Supporting (e_4) [35]	Top manager's supports and commitment for DRP operations, including allocating time and resources required in the disaster recovery. Executive support for any IT project is typically the number one success factor [35].
	Resources (e_5) [85]	In disaster recovery projects, the operational environment is uncertain, complex, and dynamic. The "business as usual" way of managing resources may not be fully applicable. Evidence shows that post-disaster recovery projects are more likely to suffer resource shortages and supply disruption. These resourcing problems contribute to final recovery project failures.

4.2. Decision Structuring by Using the DEMATEL

Because the relationships between the twenty-two possible determinants summarized by the focus group methods in Section 4.1 seem to be too complicated to be analyzed, the DEMATEL method being introduced in Section 3.2 is introduced to derive the causal relationships between the criteria. Twelve Taiwanese IT experts have actively participated in disaster recovery site evaluations and selections of public or private organizations.

Based on the experts' opinions, the direct relation/influence matrices for the influence relationships between the five aspects (refer Table 3) and the influence relations between the criteria belonging to each aspect were derived. After that, the direct relation/influence matrices were normalized based on Equation (A1) in the Appendix A. Then, the normalized direct relation/influence matrices are derived by based on Equations (A2) and (A3). Finally, the total relation matrices were derived based on Equation (A4). The detailed calculation procedures are demonstrated in Appendix C. The causal diagram consisting of the influence relationships between the aspects and those influence relationships between each criterion belonging to each aspect are demonstrated in Figure 2.

Because of the complexity of the relationships, the threshold value is defined as 68% (1 sigma). Figure 2 demonstrates the causal diagram mapping in terms of $r_i + c_i$ (x-axis) and $r_i - c_i$ (y-axis). The prominence and relation data set of the five aspects and the 22 detail-level criteria, respectively. The direction of the arrows show the direction of influences. In the central influence diagram in Figure 2 demonstrates the influence relations between aspects, "Business continuity (C)" with the highest $r_i + c_i$ value plays the central role, indicating this aspect's high degree of influence in the overall relationships. At the same time, the $r_i - c_i$ value represents the causal relationship between aspects. "Business continuity (C)" also has the lowest $r_i - c_i$ value and receives the strongest influence from the others, and thus is the effect. On the other end, "location and infrastructure (A)" has the highest $r_i - c_i$ value and dispatches strong influence on the others, and thus is the cause.

4.3. Weights of the Decision Framework

Based on the influence networks being derived in Section 4.2, the ANP was introduced to derive weights *versus* each criteria based on opinions being provided by the 12 experts. First, the pairwise comparison results were derived. Then, the limited super matrices were calculated by using the Super Decisions [95]. The detailed ANP derivation processes for the weights are demonstrated in the Appendix B. The results are demonstrated in Table 4. Weights corresponding to each aspect and criteria can thus be derived based on the weighted super matrices. The detailed calculation procedures are demonstrated in Appendix D.

From the weights associated with the aspects (Table 4), the top three important aspects can be ranked as (1) IT System Availability (0.293); (2) Location and Infrastructure (0.235) and (3) Disaster Recovery Objectives (0.222). The least important aspects can also be ranked as (1) Disaster Readiness Exercises (0.117) and (2) Operation Management (0.133).

As for the most important criteria, the top ranking criteria include (1) Backup Strategies (0.092); (2) Recovery Time Objective (0.085); (3) Electricity and Cooling (0.077); (4) Recovery Point Objective (0.073); and (5) Backup System Architecture (0.072).

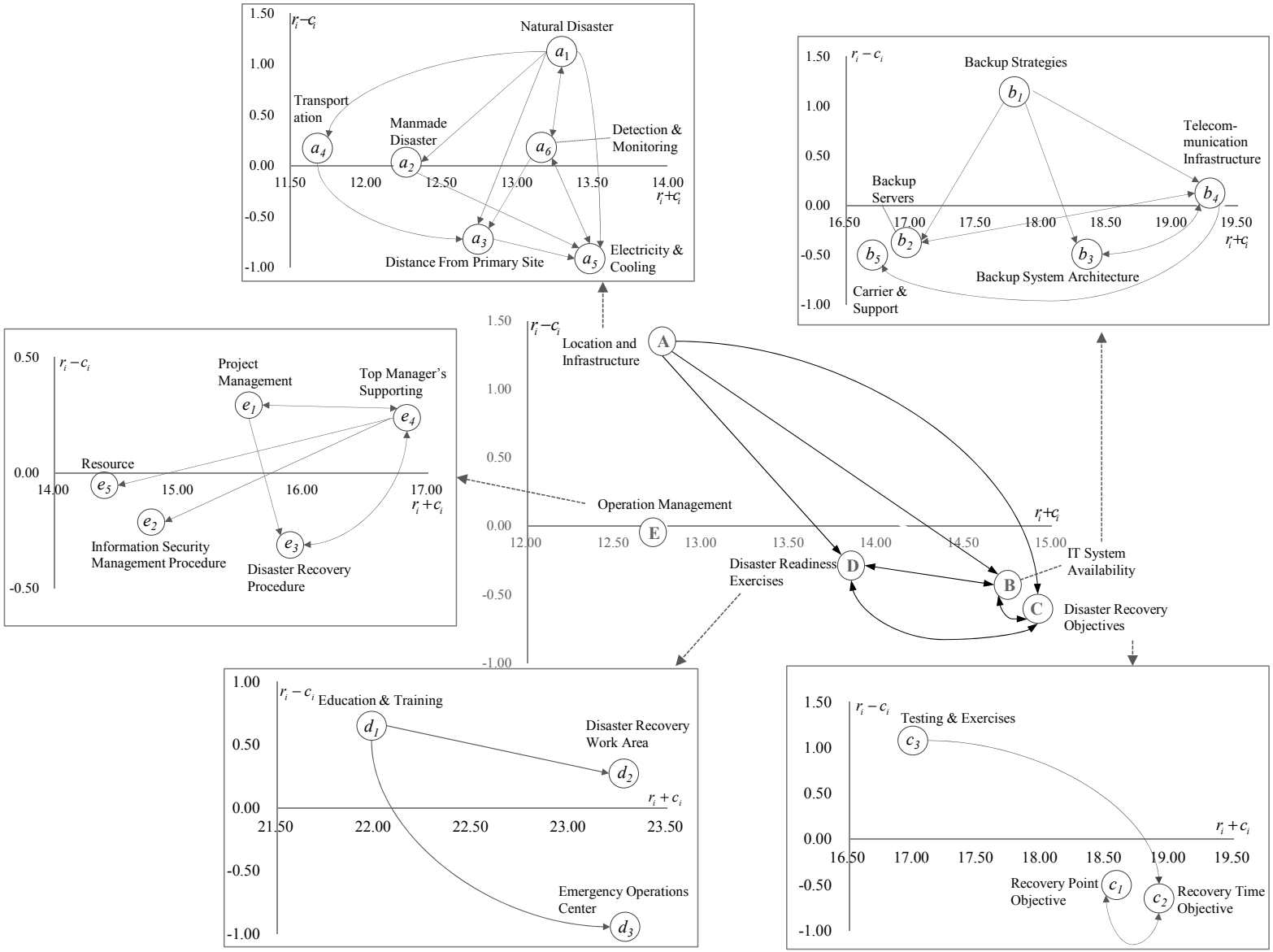

Figure 2. The causal diagram of total relationship. Note: The threshold is set on the 68% of the total relations.

Table 4. Weights *versus* the aspects and criteria.

Aspect	Weight	Criteria	Local Weight	Global Weight	Rank
Location and Infrastructure (A)	0.235 (2)	Natural Disaster (a_1)	0.169	0.040	11
		Manmade Disaster (a_2)	0.083	0.020	20
		Distance From Primary Site (a_3)	0.118	0.028	16
		Transportation (a_4)	0.094	0.022	18
		Electricity and Cooling (a_5)	0.327	0.077	3
		Detection and Monitoring (a_6)	0.209	0.049	9
IT System Availability (B)	0.293 (1)	Backup Strategies (b_1)	0.313	0.092	1
		Backup Servers (b_2)	0.106	0.031	15
		Backup System Architecture(b_3)	0.246	0.072	5
		Telecommunication Infrastructure (b_4)	0.226	0.066	6
		Carrier And Support (b_5)	0.109	0.032	13
Disaster Recovery Objectives (C)	0.222 (3)	Recovery Point Objective (c_1)	0.329	0.073	4
		Recovery Time Objective (c_2)	0.384	0.085	2
		Testing And Exercises (c_3)	0.287	0.064	7
Disaster Readiness Exercises (D)	0.117 (5)	Education And Training (d_1)	0.231	0.027	17
		Disaster Recovery Work Area (d_2)	0.268	0.031	14
		Emergency Operations Center (d_3)	0.502	0.059	8
Operation Management (E)	0.133 (4)	Project Management (e_1)	0.133	0.018	21
		Information Security Management Procedure (e_2)	0.101	0.013	22
		Disaster Recovery Procedure (e_3)	0.152	0.020	19
		Top Manager's Supporting (e_4)	0.352	0.047	10
		Resources (e_5)	0.263	0.035	12

5. Discussion

In order to resolve the complex IT disaster recovery site selection problem, this study has established the IT disaster recovery site selection analytic framework by considering aspects such as the disaster recovery site location, IT infrastructure, disaster recovery objectives, *etc.* The critical criteria have been derived accordingly. An empirical study based on the real case of a Taiwanese government's evaluation and selection of the disaster recovery site have demonstrated the feasibility of the proposed analytic framework. In Section 4, the key determinants for IT disaster recovery site selections have been derived by using the proposed hybrid MCDM framework. In this section, the analytic results will be discussed from both aspects of managerial implications in IT disaster recovery site selections, as well as the managerial implications from sustainable IT operations.

5.1. Managerial Implications from the Evaluation and Selection of IT Disaster Recovery Sites

Based on the analytic results being demonstrated in Table 4, we found that "IT System Availability (B)" is the most critical aspect in disaster recovery site selection. The aspect, IT System Availability, is tied closely with overall business continuity management procedures. Business continuity management can be separated into two distinct parts: (1) IT system design and implementation from the IT

department and (2) business analysis from IT users' departments (e.g., R&D, manufacturing, *etc.*). The IT system design and implementation phase identifies the most cost-effective disaster recovery solutions that meet the business's most critical recovery point objective (c_1) and recovery time objective (c_2) requirements, which are the major job responsibilities of an IT department. Therefore, the mechanisms being used by disaster recovery vary, depending on the kind of IT department. Apparently, IT System Availability is the first and the most critical aspect of any successful disaster recovery process for IT managers. Therefore, the analytic result is consistent with the actual situation.

Therefore, in comparison with the IT System Availability (B), the "Location and Infrastructure (A)" is only ranked the second important aspect for an IT disaster recovery site selection problem. Common sense says that the major concerns of a site selection will be the physical location risk assessment. However, "Location and Infrastructure (A)" was ranked as the second important aspect from the viewpoint of the Taiwanese experts. For small economies like Taiwan, the area is very limited. The distance from the northernmost part to the southernmost point is only about 400 kilometers. The easiest solution is to position a disaster recovery site in a neighboring country with compatible laws and regulations. However, in the case of public sector data, the above solution is not feasible. Furthermore, from the aspect of costs, construction and maintenance of a foreign site are much more expensive than those of a primary building. Therefore, for a small economy, the "IT System Availability" aspect is much more important and reality than the geographic location.

"Disaster Recovery Objectives (C)" is the third most critical aspect in evaluating disaster recovery sites. This result is consistent with the argument by Reich & Benbasat [96] that the establishment of strong alignments between information technology (IT) and organizational objectives has consistently been reported as one of the key concerns of information systems managers. The objective of disaster recovery site selection is not for risk avoidance only; instead, the objective(s) should be aligned with business continuity strategies, such as recovery point, recovery time, *etc.* As the concept of business continuity has emerged in industries as a systematic process to counter the effects of crises and interruptions, such value preservation is central to the business strategy and business continuity relationships [39]. Thus, business continuity is one of the key concerns of information system design [96].

Furthermore, according to the analytic results being derived by DEMATEL (Figure 2), the "Disaster Recovery Objectives (C)" is the main effect aspect to receive influences from the other aspects. Especially, the "Disaster Recovery Objectives (C)" depends highly on "Location and Infrastructure (A)", "IT System Availability (B)" and "Disaster Readiness Exercises (D)". People's common sense is that once the Disaster Recovery Objectives for an IT application have been defined, business continuity managers can decide which disaster recovery technologies are most suitable for such applications. For example, if the recovery time objective for a given IT application is one hour, redundant data backup on external hard drives will be the best alternative. If the recovery time objective is five days, then the tapes, compact disks, or offsite disk storage may be more cost-effective alternatives. Our research results are different. There are two possible explanations for the analytic results. At first, an organization will define disaster recovery objectives after the evaluation of physical risks from location and IT system based on the business continuity management processes has been regulated by international standards, like BS 25999 [97]. Thus, location and IT system will influence the Disaster Recovery Objectives. Second, the characteristics of an economy contribute to the analytic results. Disaster recovery site investment is undoubtedly one of the most difficult tasks where IT

managers cannot evaluate the cost performance. Due to limitations of performance uncertainty, most IT managers prefer to define disaster recovery objectives under constraints, such as physical location and IT System Availability to control the cost rather than performance.

In the following subsections, the managerial implications for the criteria belonging to each aspect will be discussed further.

5.1.1. Criteria in the IT System Availability Aspect

Based on the analytic results being demonstrated in Table 4, the Backup Strategies (b_1) is the most important criteria for a disaster recovery site selection. The major concern here is the data change or new data acquisition frequencies. Data systems that acquire new files regularly (e.g., clinical chemistry or chromatography data systems) or where data are extensively manipulated require higher data backup frequencies than those systems with fewer changes. Various alternatives are available in developing backup strategies. The full backup refers to the regular backup, which is a complete tape copy of the whole system, applications, and user files. Incremental backups refers to a regular, but partial, copy of the system, applications, and user files to standard media; the incremental backups are identified by the backup profile. The differential backup means a regular, but partial, copy of the files that have been changed since the last full backup. The various backup strategies influence both the system architecture and the internet bandwidth, which account for a majority of the cost structure of an IT system in a data center. Thus, IT managers prioritize the Backup Strategies as the most important concern.

These backup strategies are usually defined based on customers' applications and the goals, which include the backup operation time, cost, *etc.* IT systems being defined based on different backup strategies operate differently. Various backup strategies include the full backup, the incremental backup, as well as the differential backup, a mixture of the former two, are the most popular ones [84]. For the full backup strategy, all the files should be synchronized to the backup server; thus, more storage space and time are required. For the incremental backup strategy, the files being added or modified should be recorded into a temp file so as to accelerate the backup speed. Such incremental backup strategy can achieve better space performance [98]. The backup strategies can be extremely time consuming and are dependent on tape speed, network availability, tape numbers being involved, *etc.* [99]. Some scholars further focus on a mixture of different backup strategies and minimizing the overall cost of the backups [100].

For a disaster recovery site, recovery operations require restorations from the backup image(s) for the full backup scenario or from multiple backup images and tapes for the incremental backup strategy or the mixture strategies. Thus, the availability of the network becomes a major concern risk. The finding is also consistent with the research results being derived by using the DEMATEL (refer Figure 2). Telecommunication Infrastructure (b_4) plays a central role in Infrastructure Availability (B) aspect. The aspect further influences the Backup Strategies (b_1) significantly. Thus, evaluations of the Backup Strategies and the cost for network services play dominant roles for DR site selections.

The Backup System Architecture (b_3) is another issue to be considered. The major concern here is the allowance for backup time. For critical data, the intervals between data backups and the type of data backups being performed will be higher than the low-priority systems, where the data backup frequency can be lower. Possible options include system restoration within a working day (with little

impact on the system performance) or the need for restoration at the earliest possibility. The recovery time will affect both the frequency and nature of the backup as well as the recovery schemes and the linkage with database transaction logging. These issues need to be considered when designing the backup and recovery process [101].

Various approaches for system backup architecture are available: (1) hot or online backup, which takes place while the system is still operating and (2) cold or off-line backup which occurs when the system has been stopped and users have been logged out of the system. The cold backup is generally regarded as the safest backup strategy; the hot backup requires the system to be buffered while the backup occurs and the system must be updated after the backup is complete. The above options depend on system usage, data value and cost. For instance, if the data and system needs to operate during a disaster, then a hot backup of the system would be required. Alternatively, if the system was only required to be available 95% of the time, then a cold or off-line backup approach could be devised [101]. Thus, Backup Strategies (b_1) and Backup system architecture (b_3) are the major concerned criteria in the IT System Availability aspect. These two factors are also the most important ones which influence the cost-performance of an overall IT disaster recovery solution. According to the results being derived by the DEMATEL (Figure 2), the Backup Strategies (b_1) is the root cause and dispatches strong influence on Backup System Architecture (b_3) and the Telecommunication Infrastructure (b_4). Our research results provide strong evidence about the influence relationship.

5.1.2. Criteria in Location and Infrastructure Aspect

The analytic result also demonstrates that electricity and cooling (a_5) and detection and monitoring (a_6) are the most important criteria in location and infrastructure aspect of a disaster recovery site evaluation problem (Table 4). Rising power density and unpredictable disasters are the two major criteria for evaluating and selecting an IT disaster recovery site. For example, the blade servers have tremendously increased power densities and dramatically changed the power and cooling dynamics of the surrounding environments of a data center. Thus, electricity and cooling become the major source of risks and maintenance costs of data centers.

Besides, disaster recovery sites being located far away from the primary computing facilities further highlight the need for automated monitoring; it is impractical and unreliable to have people physically present to check conditions such as temperature and humidity of electricity and cooling facilities . The fully automatic remote disaster recovery site requires reliable detection and monitoring systems in place to know what is going on. This paper addresses the importance of electricity and cooling (a_5) and detection and monitoring (a_6) issues for disaster recovery site selections. The analytic results being derived by DEMATEL (Figure 2) also confirm the inter-relationships between electricity and cooling (a_5) and detection and monitoring (a_6).

Additionally, there is another point worth attention. The key issue of disaster recovery site selection is to find the ideal distance from the primary site. For instance, in 2002 and 2003, U.S. federal regulators had planned to require financial institutions to move their disaster recovery sites 200 or 300 miles away from primary sites. The Chinese government requires critical business to have disaster recovery site 1000 kilometers from primary sites. In previous studies, Pirkul [102] presents that location of emergency service facilities it is desirable to have primary and backup service facilities

within a certain distance from every district [102]; Miyagawa [103] derived the joint distribution of the distance to the first and the second nearest facilities. However, in our research, there being no significant support showing that distance from primary site and disaster recovery site is a key issue. This criterion ranks 16th.

For the U.S. or China, the distance of a few hundred miles is never a problem; however, in small economies like Taiwan with the geographical size of only 400 kilometers, the hundred miles distance from the primary site is quite infeasible. The alternative solution is to position a disaster recovery site in a neighboring country. However, in many cases, such as health care data or public sector data, they could never put those systems and data in another country due to laws and regulations. The international standards, e.g., ISO 22301, BS 25999-2, or any one of the NIST SP 800 or ISO 27000 series standards also have similar regulations. Such standards regulated that a disaster recovery site must be located within a "safe distance" rather than a far away one.

Improving computer or storage system ability to recover from disasters and meet user defined disaster recovery objectives, organizations prefer to use more flexible IT system availability than physical location selection [5,104]. For example, other studies discussed how cloud computing platforms are well suited for offering disaster recovery as a service due to their pay-as-you-go pricing model that can lower costs and their use of automated virtual platforms that can minimize the recovery time after a failure [105]. Thus, this study demonstrated that the IT System Availability (such as hot site backup) is preferred to geographic location by small economies.

5.1.3. Criteria Belonging to the Disaster Recovery Objectives Aspect

The analytic results demonstrate that the recovery point objective (c_1) and the recovery time objective (c_2) are the most important criteria in the Disaster Recovery Objectives aspect (Table 4). The recovery point objective specifies how much data loss can be tolerated during some specific time period (*i.e.*, minutes, hours, or days) [97]. The recovery time objective is defined as the maximum tolerable shutdown time an IT-based business process can tolerate before the organization starts to suffer from unacceptable consequences.

The recovery point objective and recovery point objective are determined by the business impact analysis (BIA), which differentiates critical (urgent) and non-critical (non-urgent) organizational functions/activities. A function may also be considered critical if such function is regulated by law. Thus, for firms or organizations belonging to some specific industries or sectors, such as telecommunications, banking, healthcare industries and public sectors, the business continuation should be assured and the recovery point objective (c_1) and the recovery time objective (c_2) should be close to zero, according to the government regulations. Those two criteria are also the major reasons why the disaster recovery sites are essential for such industries and sectors.

In general, the recovery time and the recovery point are the most critical key performance indicators (KPI) for business continuity, and thus, sustainable operations. The work by Ning and Luo (2008) is a typical example. Their work mapped the business criticality to disaster recovery readiness by assessing both the recovery point objective (c_1) and the recovery time objective (c_2) to guarantee business continuity under the maximum tolerable period of disruption [106]. The research findings of this work are consistent with the research results by Ning and Luo [106].

5.1.4. Criteria in Disaster Readiness Exercise Aspect

In this research, the "Emergency Operation Center (d_3)", the "Disaster Recovery Work Area (d_2)", and "Education and Training (d_1)" rank as the 8th, 14th, and 17th, respectively, among all the criteria being summarized in Table 4. These criteria are related to the emergency response of the organization. Due to the very limited land area of Taiwan (35,980 km^2) and the exposition of the majority (70%) of Taiwanese lands and populations to three or more natural hazards, the best ways for organizations to recover from a disaster may be emphasizing more on responding from an emergency instead of preventing the possible disasters. Such emergency response activities are carried out in "Emergency Operation Center (d_3)" belonging to the disaster recovery sites. Therefore, according to Figure 2, the "Education and Training (d_1)" and "Disaster Recovery Work Area (d_2)" criteria influences the operations of an emergency operation center (d_3).

5.2. Managerial Implications from Sustainable IT Operations

The IT disaster recovery site evaluation and selection problems have some intrinsic features that are tightly linked to a number of organizational concerns, including IT technology, risk management, and site selection. Most of the concerns are linked with customer's needs as well as laws or regulations being defined by the third parties or governments. Therefore, the IT disaster recovery site selection decision making problems include a wide range of criteria because the failure of IT disaster recovery may lead to either business losses or over investments for disaster recovery.

According to weights being demonstrated in Table 4, the "Location and Infrastructure (A)" and "Disaster Recovery Objectives (C)" are critical aspects which are as important as the "IT System Availability (B)" in a disaster recovery site selection problem for IT professionals. Such empirical findings provide several important managerial implications from the aspect of IT sustainable operations. Following, the managerial implications for both the changing roles of IT management from the aspect of sustainable operations as well as the disaster recovery objectives will be discussed.

5.2.1. The Changing Roles of IT Management for the Aspect of Sustainable Operations

The "Location and Infrastructure (A)" aspect often includes environment-related risks and disasters as well as the strategies to prevent such risks or disasters. Related issues can be the IT professionals' responsibility. However, the aspect "Disaster Recovery Objectives (C)" is required by business continuity operations, which links to users' needs. This is a critical issue from the viewpoint of organization behavior because IT professionals who respond to IT disaster recovery site selection decision seem to have emphasized both of them.

Albeit very complicated, organizations often assign such roles of decision making to the IT professionals. Such assignments indicate that the IT professionals belonging to the data centers should not only take care of the IT-related issues such as system downtime, but also negotiate the disaster recovery goals, including the recovery point objective (c_1) and the recovery time objective (c_2), with customers. Sometimes, IT professionals are even required to be in charge of the business continuity process so as to assure organizational operations can meet the disaster recovery goal.

Traditional IT professionals are responsible for IT-related issues; customer needs are usually ignored by the IT professionals. Our findings are different. In modern organizations, all the IT technical and logistical activities are carried out by IT professionals, who are responsible for ensuring the availability and functionality of information systems.

However, as IT disaster recovery issues are becoming more important for most of modern organizations, the IT teams are not responsible for the availability and functionality of information systems as usual. Modern IT teams have fiduciary responsibilities for the availability of mission-critical strategies [97]. Therefore, IT professionals would place disaster recovery objectives as higher priority missions than functional operations. Therefore, our results are consistent with the argument by Herbane *et al.* [39]. The roles of IT managers have been changing from emphasis on purely functional operations to strategic roles [39].

5.2.2. Recovery Point Objective *versus* Recovery Time Objective

Further, proactive risk management also requires deeper understanding of the key criteria for IT disaster recovery site selections. The "Disaster Recovery Objectives (C)" is the central role and has the highest degree of influence in the total influence relations being demonstrated in Figure 2. According to the "Disaster Recovery Objectives (C)" aspect, protecting data and maintaining uptime are almost equally important. However, prioritizing the recovery point objective (c_1) and the recovery time objective (c_2) is very critical for IT professionals in the real world because the architecture and cost for the recovery time oriented or the recovery point oriented disaster recovery sites are different.

If an organization is recovery time oriented, the disaster recovery site should be application centric. The multiple system approach, e.g., clustering, should be adopted. Such an approach can monitor the system availability and can switch users immediately to a fully redundant hot-standby system whenever the primary system is unavailable [17].

However, if an organization is more recovery point oriented, the disaster recovery site should be data-centric. Feasible solutions include Redundant Array of Independent Disks (RAIDs), disk mirroring, journaling, and/or data vaulting [17]. Therefore, based on the above arguments, the cost for a recovery time oriented disaster recovery site are higher than that of a recovery point oriented one.

While prioritizing the recovery point oriented or recovery time oriented approaches in a disaster recovery site problem, our research findings provide another viewpoint. Based on the empirical study results, the recovery time objective (c_2) is more important than the recovery point objective (c_1). Albeit there can be data losses within a very short recover time objective, the computer system should be recovered at the earliest possibility. So, the nature of the disaster recovery site problem dominates the results.

For some situations, organizations focus primarily on recovery time objectives. The telecommunication services (e.g., 3G/4G mobile telecommunications) are very typical examples which maintaining uptime may be more important than protecting data. Such service providers do not need to keep data for analysis and follow-ups. Instead, the most important concern for such firms is to maintain the ability to respond immediately to the current telecommunication service requirements.

Due to government regulations, some public sector organizations are also recovery time oriented. The critical information infrastructure (CII) such as the high speed railway system, the highway toll

collection system, *etc.* are typical examples. Such systems usually adopt active-active configurations, synchronous replications, and network transactions, which can fulfill the zero recovery time and zero recovery point goals concurrently. For such cases, the recovery time objective should be prioritized over the recovery point objective. That is also the major reason why such organizations implement disaster recovery sites. Another possible reason for the implementation of disaster recovery sites may be attributed to the protections of the data integrity. Finally, the most important reason may due to IT managers' requirements to get back online at the earliest possibility, preferably without any noticeable interruption.

According to the analytic research results being derived by the DEMATEL (Figure 2), the recovery point objective is influenced by the recovery time objective. The result is consistent with the inclusion of the recovery point objectives by the recovery time objectives in ISO 22301:2012. Therefore, the research findings provide empirical evidences to clarify the influence relationships of the recovery time objective on the recovery point objective.

For most firms or organizations (e.g., most public sector institutes, research institutes, commercial banks, for the data protection purposes, the recovery point objectives are still more important than the recovery time objectives. For example, commercial banks concern more on data protections than maintaining very short uptime. Bank customers may feel inconvenient if their account information is unavailable for a very short system (e.g., ATM or online banks) down time. However, any loss of the deposit or payment records is not allowable.

5.3. Limitations and Future Research Possibilities

In this research, the experts were invited for deriving the aspects and criteria. Albeit some exiting researches have provided valuable insights for disaster recovery site selections, to the best of our knowledge, this research is the first attempt to derive factors for evaluating the disaster recovery site(s) via an MCDM based systematic approach, which consider the influence relationships between criteria. Since the disaster recovery site problem is highly knowledge-intensive, only the experts who are responsible for disaster recovery site evaluations and planning can provide valuable insights. However, the total number of available Taiwanese experts is less than 30. The statistical analysis based approaches including the exploratory and confirmatory factor analysis, which require more than 30 experts to fulfill the minimum sample number requirements, are not suitable. Therefore, the expert system based approach is more feasible and reasonable for this specific problem.

From this aspect, the future disaster recovery researches may include studies of larger economies by using the exploratory or confirmatory factor analyses based on theoretic models, e.g., the resource based theory, the resource dependence theory, *etc.* The results being derived based on experts' opinions by MCDM methods and the results being derived based on the statistical analyses (e.g., the covariance based structure equation model or the partial least squares structure equation model) can further be compared and studied. Further, other possible studies include the applications of the analytic framework in other economies or industries. Meanwhile, much more research is still required for differentiating the research point *versus* research time oriented disaster recovery needs.

6. Concluding Remarks

IT system availability and continuous operations have become increasingly important for most modern organizations. Therefore, the IT disaster recovery site evaluation and selection problems are very critical for such organizations. However, very few scholars tried to resolve the IT disaster recovery site selection problems. This paper attempts to derive the decision criteria. Like the main data center, choosing a disaster recovery site has a lot of criteria for making the best decision for a company and IT. However, a disaster recovery site is more focused on business continuity purposes and to be part of a company's strategy for providing uninterrupted services to its customers and end users.

The main contribution of this study is the definition of a disaster recovery site selection framework from both aspects of international standards and regulations as well as the enterprise IT infrastructure. This framework provides the guidelines for evaluating and selecting of IT disaster recovery site for disaster recovery service providers, organization IT managers and information/data owners, no matter from business or governmental organizations.

A major finding of this research is that the key aspect for disaster recovery site selection is business continuity as well as the location and the infrastructure aspect. The disaster recovery site selection is aligned with business continuity. Therefore, such disaster recovery site selections have played strategic roles, rather than purely IT functional decision. Such decisions cannot be from the IT or the facility viewpoint alone.

Furthermore, this empirical result shows that the recovery time is the most important business continuity management criteria for an organization's evaluation and selection of a disaster recovery site. This finding implies that the "recovery time" is the most important determinant, other than cost or quality. In practice, the priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes. The recovery time for an IT resource should match the recovery time requirements for the business function or processes, which depend on the IT resources. Our findings are not in contradiction with those of empirical studies discussed the disaster recovery was cost-prohibitive. The result of this study may be of interest to organizations attempting to define disaster recovery site strategies and to researchers interested in disaster recovery aspects of IT facilities and technology.

Acknowledgments

We thank to National Center for High-performance Computing' staff for inspiring conversations, suggestions, and feedback in preparing this article.

Author Contributions

Chia-Lee Yang and Professor Benjamin J. C. Yuan designed and proposed the concept of this research. Chia-Lee Yang and Professor Chi-Yo Huang performed research, analyzed the data and wrote the paper.

Appendix A. DEMATEL

The following are explanations of the DEMATEL calculation steps.

Step 1: Build an initial direct-relation matrix

Experts are asked to indicate the direct influence degree between factor *i* and factor *j*, as indicated by a_{ij} , using a pair-wise comparison scale designated with five levels. The initial direct-relation matrix $\boldsymbol{A}$ is obtained by deriving the influence relationships between criteria through Equation (A1).

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \tag{A1}$$

a_{ij} is denoted as the degree to which the ith objective affects the j th objective

Step 2: Normalize the direct-relation matrix

The normalized direct-relation matrix $\boldsymbol{N}$ is obtained through Equations (A2) and (A3).

$$\boldsymbol{N}=y\boldsymbol{A} \tag{A2}$$

$$y=\min\left\{1/\max_{i}\sum_{j=1}^{n}a_{ij},1/\max_{j}\sum_{i=1}^{n}a_{ij}\right\},i,j\in\{1,2,...,n\}. \tag{A3}$$

Step 3: Build the total relation matrix $\boldsymbol{T}$

The total-relation matrix $\boldsymbol{T}$ is acquired by Equation (A4):

$$\boldsymbol{T}=N+N^2+...+N^{\varepsilon}=\boldsymbol{N}\left(\boldsymbol{I}-\boldsymbol{N}\right)^{-1} \tag{A4}$$

where ε →∞, $\boldsymbol{I}$ is the identity matrix and $N=\left[x_{ij}\right]_{nxn}$.

Step 4: Compute the influence strength of the factors

Aggregate the values of the rows and columns in matrix $\boldsymbol{T}$ to obtain a value r_i and c_i through the Equations (A5) and (A6) respectively. The r_i represents the level of direct or indirect impacts on other factor, and c_i represents the level to which it is affected by other factor:

$$r_i=\left[\sum_{j=1}^{n}t_{ij}\right]_{nx1}=\left[t_i\right]_{nx1} \tag{A5}$$

$$c_i=\left[\sum_{j=1}^{n}t_{ij}\right]_{1xn}=\left[t_i\right]_{nx1} \tag{A6}$$

Step 5: Produce a causal diagram

A causal diagram can be acquired by mapping a data set (r_i+c_i, r_i-c_i). The value of r_i+c_i indicates the strength of influence. The higher the value of r_i+c_i a factor has, the more related it is to the other factors. Similarly, the value of r_i-c_i indicates the causal relationship between factors. If

$r_i - c_i$ is positive, then the factor is a "cause factor", dispatching influence to the others. If $r_i - c_i$ is negative, the factor is an "effect factor", receiving influence from others. The higher the value of $r_i - c_i$ a factor has, the more influence it has on the other factors, and hence this factor is presumed to have a higher priority than the others. In other words, the lower the value of $r_i - c_i$ a factor has, the greater its received influence from the other factors, and consequently, the lower the priority it is assumed to have.

Appendix B. ANP

The ANP is a coupling of two parts. The first consists of a control hierarchy or network of criteria and subcriteria that control the interactions. The second is a network of influences among the elements and clusters. The network varies from criterion to criterion and a different supermatrix of limiting influence is computed for each control criterion. Finally, each of these supermatrices is weighted by the priority of its control criterion and the results are synthesized through addition for all the control criteria [78].

Analysis of priorities in a system can be thought of in terms of a control hierarchy with dependence among its bottom-level alternatives arranged as a network as shown in Figure B1. Dependence can occur within the components and between them. A control hierarchy at the top may be replaced by a control network with dependence among its components, which are collections of elements whose functions derive from the synergy of their interaction and hence has a higher-order function not found in any single element. The criteria in the control hierarchy that are used for comparing the components are usually the major parent criteria whose subcriteria are used to compare the elements need to be more general than those of the elements because of the greater complexity of the components.

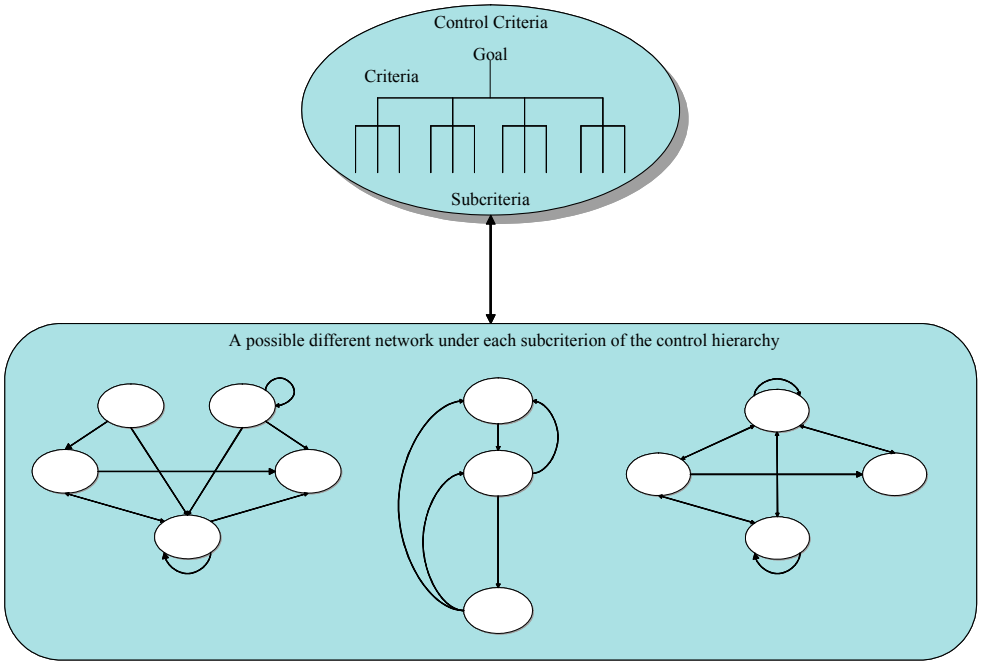

Figure B1. The control hierarchy. Source: [74].

A network connects the components of a decision system. The system is made up of subsystems, with each subsystem made up of components, and each component made up of elements. Figure B2 demonstrates a typical network. Those components which no arrow enters are known as source

components such as C_1 and C_2. Those from which no arrow leaves are known as sink component such as C_5. Those components which arrows both enter and exit leave are known as transient components such as C_3 and C_4. In addition, C_3 and C_4 form a cycle of two components because they feed back and forth into each other. C_2 and C_4 have loops that connect them to themselves and are inner dependent. All other connections represent dependence between components which are thus known to be outer dependent.

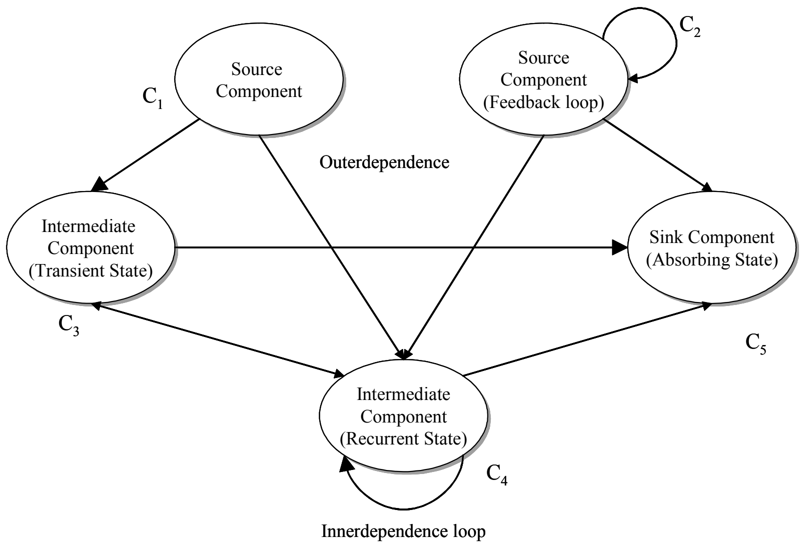

Figure B2. Connections in a network. Source: [74].

A component of a decision network which was derived by the DEMATEL method in Appendix A will be denoted by $C_h, h=1,\cdots,m,$ and assume that it has n_h elements, which we denote by $e_{h1}, e_{h2},\cdots, e_{hm}$. The influences of a given set of elements in a component on any element in the decision system are represented by a ratio scale priority vector derived from paired comparisons of the comparative importance of one criterion and another criterion with respect to the interests or preferences of the decision makers. This relative importance value can be determined using a scale of 1–9 to represent equal importance to extreme importance. The influence of elements in the network on other elements in that network can be represented in the following supermatrix:

$$
\boldsymbol{W} = \begin{array}{cc} & \begin{array}{ccccccccccc} & \boldsymbol{C}_1 & & & \boldsymbol{C}_2 & & \cdots & & \boldsymbol{C}_m & \\ e_{11} & \cdots & e_{1n_1} & e_{21} & \cdots & e_{2n_2} & \cdots & e_{m1} & \cdots & e_{mn_m} \end{array} \\ \begin{array}{cc} & e_{11} \\ & e_{12} \\ \boldsymbol{C}_1 & \vdots \\ & e_{1n_1} \\ & e_{21} \\ & e_{22} \\ \boldsymbol{C}_2 & \vdots \\ & e_{2n_2} \\ \vdots & \vdots \\ & e_{m1} \\ & e_{m2} \\ \boldsymbol{C}_2 & \vdots \\ & e_{mn_m} \end{array} & \begin{bmatrix} \boldsymbol{W}_{11} & \boldsymbol{W}_{12} & \cdots & \boldsymbol{W}_{1m} \\ \boldsymbol{W}_{21} & \boldsymbol{W}_{22} & \cdots & \boldsymbol{W}_{2m} \\ & & \ddots & \\ \vdots & \vdots & & \vdots \\ \boldsymbol{W}_{m1} & \boldsymbol{W}_{m2} & \cdots & \boldsymbol{W}_{mm} \end{bmatrix} \end{array}
$$

A typical entry $\boldsymbol{W}_{ij}$ in the supermatrix is a principal eigenvector of the influence of the elements in the *i*th component of the network on an element in the *j*th component. Some of its entries may be zero corresponding to those elements that have no influence.

$$\boldsymbol{W}_{ij} = \begin{bmatrix} w_{i_1 j_1} & w_{i_1 j_2} & \cdots & w_{i_1 j_{n_j}} \\ w_{i_2 j_2} & w_{i_2 j_2} & \cdots & w_{i_2 j_{n_j}} \\ \vdots & \vdots & \ddots & \vdots \\ w_{i_{n_i} j_1} & w_{i_{n_i} j_2} & \cdots & w_{i_{n_i} j_{n_j}} \end{bmatrix}$$

After forming the supermatrix, the weighted supermatrix is derived by transforming all columns sum to unity exactly. The weighted supermatrix is raised to limiting powers, such as Equation (B1) to get the global priority vector or called weights.

$$\lim_{\theta \to \infty} \boldsymbol{W}^{\theta} \tag{B1}$$

In addition, if the supermatrix has the effect of cyclicity, the limiting supermatrix is not the only one. There are two or more limiting supermatrices in this situation, and the Cesaro sum would need to be calculated to get the priority. The Cesaro sum is formulated as follows.

$$\lim_{\psi \to \infty} (\frac{1}{\nu}) \sum_{j=1}^{\nu} \boldsymbol{W}_j^{\psi} \tag{B2}$$

to calculate the average effect of the limiting supermatrix (*i.e.*, the average priority weights) where $\boldsymbol{W}_j$ denotes the *j*th limiting supermatrix. Otherwise, the supermatrix would be raised to large powers to get the priority weights [107].

Appendix C. The detailed calculation procedures of the DEMATEL

Table C1. The direct relation/influence matrix $\boldsymbol{A}_{\text{dim}ensions}$ of dimensions.

$\boldsymbol{A}_{\text{dim}ensions}$ =	0.000	2.667	2.250	2.417	1.750
	1.917	0.000	3.000	2.333	2.000
	1.833	3.000	0.000	2.167	2.250
	1.917	2.333	2.417	0.000	2.000
	1.333	1.917	2.500	2.250	0.000

Table C2. The direct relation/influence matrix $\boldsymbol{A}_a$ of factors in A dimensions.

$\boldsymbol{A}_a$ =	0.000	1.500	2.417	2.083	2.333	2.083
	0.667	0.000	2.000	1.583	2.417	2.083
	2.000	1.417	0.000	2.250	1.417	1.333
	1.667	1.583	2.667	0.000	1.250	1.167
	1.917	2.083	1.083	1.250	0.000	2.417
	2.167	1.917	1.583	0.833	2.917	0.000

Table C3. The direct relation/influence matrix A_b A of factors in B dimensions.

A_b =	0.000	2.333	2.500	2.583	2.167
	2.083	0.000	2.333	2.000	1.750
	2.083	2.333	0.000	2.500	2.000
	2.417	2.167	2.750	0.000	2.583
	1.583	1.750	1.917	2.667	0.000

Table C4. The direct relation/influence matrix A_c of factors in C dimensions.

A_c =	0.000	2.917	2.083
	3.000	0.000	2.083
	2.333	2.667	0.000

Table C5. The direct relation/influence matrix A_d of factors in D dimensions.

A_d =	0.000	2.000	2.083
	1.917	0.000	2.417
	1.833	2.167	0.000

Table C6. The direct relation/influence matrix A_e of factors in E dimensions.

A_e =	0.000	2.273	2.545	2.636	2.091
	2.091	0.000	2.455	2.364	1.727
	2.364	2.455	0.000	2.455	2.091
	2.727	2.455	2.727	0.000	2.636
	1.909	1.727	2.091	2.727	0.000

Table C7. The normalized direct relation/influence matrix $N_{diemensions}$ of dimensions.

$N_{diemensions}$ =	0.000	0.262	0.221	0.238	0.172
	0.189	0.000	0.295	0.230	0.197
	0.180	0.295	0.000	0.213	0.221
	0.189	0.230	0.238	0.000	0.197
	0.131	0.189	0.246	0.221	0.000

Table C8. The normalized direct relation/influence matrix N_a of factors in A dimensions.

N_a =	0.000	0.144	0.232	0.200	0.224	0.200
	0.064	0.000	0.192	0.152	0.232	0.200
	0.192	0.136	0.000	0.216	0.136	0.128
	0.160	0.152	0.256	0.000	0.120	0.112
	0.184	0.200	0.104	0.120	0.000	0.232
	0.208	0.184	0.152	0.080	0.280	0.000

Table C9. The normalized direct relation/influence matrix N_b of factors in B dimensions.

N_b =	0.000	0.235	0.252	0.261	0.218
	0.210	0.000	0.235	0.202	0.176
	0.210	0.235	0.000	0.252	0.202
	0.244	0.218	0.277	0.000	0.261
	0.160	0.176	0.193	0.269	0.000

Table C10. The normalized direct relation/influence matrix N_c of factors in C dimensions.

N_c =	0.000	0.522	0.373
	0.537	0.000	0.373
	0.418	0.478	0.000

Table C11. The normalized direct relation/influence matrix N_d of factors in D dimensions.

N_d =	0.000	0.444	0.463
	0.426	0.000	0.537
	0.407	0.481	0.000

Table C12. The normalized direct relation/influence matrix N_e of factors in E dimensions.

N_e =	0.000	0.216	0.241	0.250	0.198
	0.198	0.000	0.233	0.224	0.164
	0.224	0.233	0.000	0.233	0.198
	0.259	0.233	0.259	0.000	0.250
	0.181	0.164	0.198	0.259	0.000

Table C13. Total relation matrix $T_{\dim ensions}$ of dimensions.

$T_{\dim ensions}$ =	1.036	1.589	1.592	1.477	1.306
	1.208	1.401	1.659	1.488	1.340
	1.201	1.626	1.429	1.476	1.355
	1.152	1.512	1.546	1.233	1.277
	1.045	1.395	1.461	1.331	1.040

Table C14. Total relation matrix T_a of factors in dimension A.

T_a =	1.018	1.145	1.309	1.126	1.380	1.246
	0.934	0.872	1.109	0.944	1.213	1.090
	1.008	0.968	0.941	0.983	1.116	1.013
	0.972	0.966	1.134	0.795	1.088	0.986
	1.038	1.058	1.070	0.937	1.054	1.138
	1.113	1.103	1.162	0.963	1.342	1.011

Table C15. Total relation matrix T_b of factors in dimension B.

T_b =	1.626	1.879	2.039	2.076	1.857
	1.599	1.481	1.801	1.807	1.621
	1.706	1.782	1.732	1.963	1.749
	1.861	1.910	2.100	1.918	1.927
	1.531	1.596	1.736	1.814	1.439

Table C16. Total relation matrix T_c of factors in dimension C.

T_c =	2.952	3.369	2.732
	3.334	3.059	2.759
	3.244	3.347	2.459

Table C17. Total relation matrix T_d of factors in dimensions D.

T_d =	3.328	3.895	4.095
	3.763	3.736	4.285
	3.575	3.867	3.732

Table C18. Total relation matrix T_e of factors in dimensions E.

T_e =	1.411	1.565	1.694	1.737	1.504
	1.466	1.278	1.570	1.598	1.375
	1.569	1.551	1.472	1.698	1.480
	1.729	1.686	1.824	1.660	1.646
	1.435	1.400	1.526	1.601	1.217

Table C19. $r_i + c_i$ and $r_i - c_i$ values calculated from the direct/indirect matrix ***T***.

Dimensions	**A**	**B**	**C**	**D**	**E**
$r_i + c_i$	12.64	14.62	14.77	13.72	12.59
$r_i - c_i$	1.36	−0.43	−0.60	−0.29	−0.04

Factors	a_1	a_2	a_3	a_4	a_5	a_6	b_1	b_2	b_3	b_4	b_5
$r_i + c_i$	13.31	12.27	12.75	11.69	13.49	13.18	17.80	16.95	18.34	19.29	16.71
$r_i - c_i$	1.14	0.05	−0.70	0.19	−0.90	0.21	1.15	−0.34	−0.48	0.14	−0.48
Factors	c_1	c_2	c_3	d_1	d_2	d_3	e_1	e_2	e_3	e_4	e_5
$r_i + c_i$	18.58	18.93	17.00	21.98	23.28	23.29	15.52	14.77	15.86	16.84	14.40
$r_i - c_i$	−0.48	−0.62	1.10	0.65	0.29	−0.94	0.30	−0.19	−0.32	0.25	−0.04

Appendix D. The Detailed Calculation Procedures of the ANP

Table D1. The weighted supermatrix $W_{Dimensions}$ for deriving weights of dimensions.

Dimensions	A	B	C	D	E	Weight
Location and Infrastructure (A)	0.000	0.000	0.000	0.000	0.000	0.235
IT System Availability (B)	0.503	0.000	0.727	0.632	0.000	0.293
Disaster Recovery Objectives (C)	0.331	0.692	0.000	0.368	0.000	0.222
Disaster Readiness Exercises(D)	0.167	0.308	0.273	0.000	0.000	0.117
Operation Management (E)	0.000	0.000	0.000	0.000	0.000	0.133

Table D2. The weighted supermatrix W_a for deriving weights of factors in dimension A.

Measurement Factors	a_1	a_2	a_3	a_4	a_5	a_6	Weight
Natural Disaster (a_1)	0.000	0.000	0.000	0.000	0.000	0.490	0.169
Manmade Disaster (a_2)	0.106	0.000	0.000	0.000	0.000	0.000	0.083
Distance From Primary Site (a_3)	0.129	0.000	0.000	1.000	0.000	0.510	0.118
Transportation (a_4)	0.110	0.000	0.000	0.000	0.000	0.000	0.094
Electricity and Cooling (a_5)	0.405	1.000	1.000	0.000	0.000	0.000	0.327
Detection and Monitoring (a_6)	0.251	0.000	0.000	0.000	1.000	0.000	0.209

Table D3. The weighted supermatrix W_b for deriving weights of factors in dimension B.

Measurement Factors	b_1	b_2	b_3	b_4	b_5	Weight
Backup Strategies (b_1)	0.000	0.000	0.000	0.313	0.000	0.313
Backup Servers (b_2)	0.181	0.000	0.000	0.106	0.000	0.106
Backup System Architecture(b_3)	0.511	0.000	0.000	0.246	0.000	0.246
Telecommunication Infrastructure (b_4)	0.309	0.000	1.000	0.226	0.000	0.226
Carrier and Support (b_5)	0.000	0.000	0.000	0.109	0.000	0.109

Table D4. The weighted supermatrix W_c for deriving weights of factors in dimension C.

Measurement Factors	c_1	c_2	c_3	Weight
Recovery Point Objective (c_1)	0.000	1.000	0.000	**0.329**
Recovery Time Objective (c_2)	1.000	0.000	1.000	0.384
Testing and Exercises(c_3)	0.000	0.000	0.000	0.287

Table D5. The weighted supermatrix W_d for deriving weights of factors in dimension D.

Measurement Factors	d_1	d_2	d_3	Weight
Education and Training (d_1)	0.000	0.000	0.000	0.231
Disaster Recovery Work Area (d_2)	0.681	0.000	1.000	0.268
Emergency Operations Center (d_3)	0.319	1.000	0.000	0.502

Table D6. The weighted supermatrix W_e for deriving weights of factors in dimension E.

Measurement Factors	e_1	e_2	e_3	e_4	e_5	Weight
Project Management (e_1)	0.000	0.000	0.000	0.133	0.000	0.133
Information Security Management Procedure(e_2)	0.000	0.000	0.000	0.101	0.000	0.101
Disaster Recovery Procedure (e_3)	0.334	0.000	0.000	0.152	0.000	0.152
Top Manager's Supporting (e_4)	0.666	0.000	1.000	0.352	1.000	0.352
Resources (e_5)	0.000	0.000	0.000	0.263	0.000	0.263

Table D7. The limted supermatrix $\lim_{\theta\to\infty} W_a^{\theta}$ of factors in dimension A.

$\lim_{\theta\to\infty} W_a^{\theta} =$	0.158	0.158	0.158	0.158	0.158	0.158
	0.017	0.017	0.017	0.017	0.017	0.017
	0.202	0.202	0.202	0.202	0.202	0.202
	0.017	0.017	0.017	0.017	0.017	0.017
	0.283	0.283	0.283	0.283	0.283	0.283
	0.158	0.158	0.158	0.158	0.158	0.158

Table D8. The limted supermatrix $\lim_{\theta\to\infty} W_b^{\theta}$ of factors in dimension B.

$\lim_{\theta\to\infty} W_b^{\theta} =$	0.167	0.000	0.167	0.167	0.167
	0.092	0.000	0.092	0.092	0.092
	0.231	0.000	0.231	0.231	0.231
	0.452	0.000	0.452	0.452	0.452
	0.058	0.000	0.058	0.058	0.058

Table D9. The limted supermatrix $\lim_{\theta\to\infty} W_c^{\theta}$ of factors in dimension C.

$\lim_{\theta\to\infty} W_c^{\theta} =$	0.000	0.000	0.000
	0.500	0.500	0.500
	0.500	0.500	0.500

Table D10. The limted supermatrix $\lim_{\theta\to\infty} W_d^{\theta}$ of factors in dimension D.

$\lim_{\theta\to\infty} W_d^{\theta} =$	0.000	0.000	0.000
	0.500	0.500	0.500
	0.500	0.500	0.500

Table D11. The limted supermatrix $\lim_{\theta\to\infty} W_e^{\theta}$ of factors in dimension E.

$\lim_{\theta\to\infty} W_e^{\theta} =$	0.081	0.081	0.000	0.081	0.081
	0.062	0.062	0.000	0.062	0.062
	0.122	0.122	0.000	0.122	0.122
	0.574	0.574	0.000	0.574	0.574
	0.161	0.161	0.000	0.161	0.161

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Feng, N.; Li, M. An information systems security risk assessment model under uncertain environment. *Appl. Soft Comput.* **2011**, *11*, 4332–4340.
2. Kankanhalli, A.; Teo, H.H.; Tan, B.C.Y.; Wei, K.-K. An integrative study of information systems security effectiveness. *Int. J. Inf. Manag.* **2003**, *23*, 139–154.
3. Sembiring, J.; Siregar, M.I.H. A Decision Model for IT Risk Management on Disaster Recovery Center in an Enterprise Architecture Model. *Proc. Technol.* **2013**, *11*, 1142–1146.
4. The Australian National Audit Office (ANAO). *Business Continuity Management: Building Resilience in Public Sector Entities*; ANAO: Barton, Australia, 2009.
5. Cegiela, R. Selecting Technology for Disaster Recovery. In Proceedings of the International Conference on Dependability of Computer Systems (DepCos-RELCOMEX 06), Szklarska Poreba, Poland, 25–27 May 2006.
6. Rajagopalan, S.; Cully, B.; O'Connor, R.; Warfield, A. SecondSite: Disaster tolerance as a service. *ACM SIGPLAN Not*. **2012**, *47*, 97–108.
7. Sengupta, S.; Annervaz, K. Multi-site data distribution for disaster recovery—A planning framework. *Future Gener. Comput. Syst.* **2014**, *41*, 53–64.
8. Hawkins, S.M.; Yen, D.C.; Chou, D.C. Disaster recovery planning: A strategy for data security. *Inf. Manag. Comput. Secur.* **2000**, *8*, 222–230.
9. Kant, K. Data center evolution: A tutorial on state of the art, issues, and challenges. *Comput. Netw.* **2009**, *53*, 2939–2965.
10. Lumpp, T.; Schneider, J.; Holtz, J.; Mueller, Z.; Lenz, N.; Biazetti, A.; Petersen, D. From high availability and disaster recovery to business continuity solutions. *IBM Syst. J.* **2008**, *47*, 605–619.
11. Bryson, K.-M.; Millar, H.; Joseph, A.; Mobolurin, A. Using formal MS/OR modeling to support disaster recovery planning. *Eur. J. Oper. Res.* **2002**, *141*, 679–688.
12. Daim, T.U.; Bhatla, A.; Mansour, M. Site selection for a data centre–a multi-criteria decision-making model. *Int. J. Sustain. Eng.* **2013**, *6*, 10–22.
13. Chen, C.-T. A fuzzy approach to select the location of the distribution center. *Fuzzy Sets Syst.* **2001**, *118*, 65–73.
14. Covas, M.T.; Silva, C.A.; Dias, L.C. On locating sustainable Data Centers in Portugal: Problem structuring and GIS-based analysis. *Sustain. Comput.* **2013**, *3*, 27–35.
15. De Boer, J. An introduction to disaster medicine in Europe. *J. Emerg. Med.* **1995**, *13*, 211–216.
16. Rutherford, W.H.; de Boer, J. The definition and classification of disasters. *Injury*. **1983**, *15*, 10–12.
17. Asgary, A.; Anjum, M.I.; Azimi, N. Disaster recovery and business continuity after the 2010 flood in Pakistan: Case of small businesses. *Int. J. Disaster Risk Reduct.* **2012**, *2*, 46–56.
18. Rose, A.Z. A framework for analyzing the total economic impacts of terrorist attacks and natural disasters. *J. Homel. Secur. Emerg. Manag.* **2009**, *6*, 1–26.

19. Anthopoulos, L.G.; Kostavara, E.; Pantouvakis, J.-P. An Effective Disaster Recovery Model for Construction Projects. *Procedia* **2013**, *74*, 21–30.
20. Hale, T.; Moberg, C.R. Improving supply chain disaster preparedness: A decision process for secure site location. *Int. J. Phys. Distrib. Logist. Manag.* **2005**, *35*, 195–207.
21. Lindell, M.K.; Prater, C.S. Assessing community impacts of natural disasters. *Nat. Hazards Rev.* **2003**, *4*, 176–185.
22. Van Aalst, M.K. The impacts of climate change on the risk of natural disasters. *Disasters* **2006**, *30*, 5–18.
23. Alexander, D. Natural disasters: A framework for research and teaching. *Disasters*. **1991**, *15*, 209–226.
24. Alexander, D. The study of natural disasters, 1977–1997: Some reflections on a changing field of knowledge. *Disasters*. **1997**, *21*, 284–304.
25. Fothergill, A.; Maestas, E.G.; Darlington, J.D. Race, ethnicity and disasters in the United States: A review of the literature. *Disasters.* **1999**, *23*, 156–173.
26. Nigg, J.M. *Disaster Recovery as a Social Process*; Disaster Research Center: Newark, NJ, USA, 1995.
27. Fothergill, A.; Peek, L.A. Poverty and disasters in the United States: A review of recent sociological findings. *Nat. Hazards* **2004**, *32*, 89–110.
28. Rose, A. Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environ. Hazards* **2007**, *7*, 383–398.
29. Spillan, J.; Hough, M. Crisis planning in small businesses: Importance, Impetus and Indifference. *Eur. Manag. J.* **2003**, *21*, 398–407.
30. Seifert, J.W. The effects of 11 September 2001, terrorist attacks on public and private information infrastructures: A preliminary assessment of lessons learned. *Gov. Inf. Quart.* **2002**, *19*, 225–242.
31. Zsidisin, G.A.; Melnyk, S.A.; Ragatz, G.L. An institutional theory perspective of business continuity planning for purchasing and supply management. *Int. J. Prod. Res.* **2005**, *43*, 3401–3420.
32. Toigo, J.W. *Disaster Recovery Planning: Strategies for Protecting Critical Information*; Prentice Hall PTR: Upper Saddle River, NJ, USA, 2000.
33. Chisholm, P. Disaster Recovery Planning Is Business-Critical. *CPA J.* **2008**, *78*, 11.
34. Omar, A.; Alijani, D.; Mason, R. Information technology disaster recovery plan: Case study. *Acad. Strateg. Manag. J.* **2011**, *10*, 127–141.
35. Snedaker, S. *Business Continuity and Disaster Recovery: Planning for IT Professionals*; Newnes: New South Wales, Australia, 2013.
36. Iyer, R.K.; Sarkis, J. Disaster recovery planning in an automated manufacturing environment. *IEEE Trans. Eng. Manag.* **1998**, *45*, 163–175.
37. Sahebjamnia, N.; Torabi, S.; Mansouri, S. Integrated business continuity and disaster recovery planning: Towards organizational resilience. *Eur. J. Oper. Res.* **2015**, *242*, 261–273.
38. Riolli, L.; Savicki, V. Information system organizational resilience. *Omega.* **2003**, *31*, 227–233.
39. Herbane, B.; Elliott, D.; Swartz, E.M. Business continuity management: Time for a strategic role? *Long Range Plan.* **2004**, *37*, 435–457.
40. Hiles, A. *The Definitive Handbook Business Continuity Management*; John Wiley & Sons: Hoboken, NJ, USA, 2010.

41. Losada, C.; Scaparra, M.P.; O'Hanley, J.R. Optimizing system resilience: A facility protection model with recovery time. *Eur. J. Oper. Res.* **2012**, *217*, 519–530.
42. TechAdvisory.org. Disaster Recovery: An Increasingly Important Aspect of Your Business. Available online: http://www.techadvisory.org/2010/05/disaster-recovery%E2%80%94an-increasingly-important-aspect-of-your-business/ (accessed on 21 May 2010).
43. King, R.P.; Halim, N.; Garcia-Molina, H.; Polyzois, C. A. Management of a remote backup copy for disaster recovery. *ACM Trans. Database Syst. (TODS)* **1991**, *16*, 338–368.
44. Wold, G.H. Disaster recovery planning process. *Disaster Recovery J.* **2006**, *5*, 1–8.
45. García, J.L.; Alvarado, A.; Blanco, J.; Jiménez, E.; Maldonado, A.A.; Cortés, G. Multi-attribute evaluation and selection of sites for agricultural product warehouses based on an Analytic Hierarchy Process. *Comput. Electron. Agric.* **2014**, *100*, 60–69.
46. Rikalovic, A.; Cosic, I.; Lazarevic, D. GIS Based Multi-criteria Analysis for Industrial Site Selection. *Proc. Eng.* **2014**, *69*, 1054–1063.
47. Pereira, N.; Carneiro, J.F.; Araújob, A.; Bezzeghoudc, M.; Borgesc, J. Seismic and structural geology constraints to the selection of CO_2 storage sites—The case of the onshore Lusitanian basin, Portugal. *J. Appl. Geophys.* **2014**, *102*, 21–38.
48. Wang, G.; Qin, L.; Li, G.; Chen, L. Landfill site selection using spatial information technologies and AHP: A case study in Beijing, China. *J. Environ. Manag.* **2009**, *90*, 2414–2421.
49. Dermol, U.; Kontić, B. Use of strategic environmental assessment in the site selection process for a radioactive waste disposal facility in Slovenia. *J. Environ. Manag.* **2011**, *92*, 43–52.
50. Schniederjans, M.J.; Hoffman, J.J.; Sirmans, G.S. Using goal programming and the analytic hierarchy process in house selection. *J. Real Estate Financ. Econ.* **1995**, *11*, 167–176.
51. Vahidnia, M.H.; Alesheikh, A.A.; Alimohammadi, A. Hospital site selection using fuzzy AHP and its derivatives. *J. Environ. Manag.* **2009**, *90*, 3048–3056.
52. Dissanayake, S.; Önal, H. Amenity driven price effects and conservation reserve site selection: A dynamic linear integer programming approach. *Ecol. Econ.* **2011**, *70*, 2225–2235.
53. Hristidis, V.; Chen, S.-C.; Li, T.; Luis, S.; Deng, Y. Survey of data management and analysis in disaster situations. *J. Syst. Softw.* **2010**, *83*, 1701–1714.
54. NASA. *Cyber Security: The Status of Information Security and the Effects of the Federal Information Security Management Act (FISMA) at NASA*; National Aeronautics and Space Administration (NASA): Washington, DC, USA, 2003.
55. Bowen, P.; Hash, J.; Wilson, M. *Information Security Handbook: A Guide for Managers*; NIST Special Publication 800–100; National Institute of Standards & Technology(NIST): Gaithersburg, MD, USA, 2006.
56. Bertrand, C. Business continuity and mission critical applications. *Netw. Secur.* **2005**, *2005*, 9–11.
57. Thompson, R.G.; Singleton, F.D., Jr.; Thrall, R.M.; Smith, B.A. Comparative site evaluations for locating a high-energy physics lab in Texas. *Interfaces* **1986**, *16*, 35–49.
58. Belk, R.W. *Handbook of Qualitative Research Methods in Marketing*; Edward Elgar Publishing: Cheltenham, UK, 2007.
59. MacGregor, B.; Morrison, D.E. From focus groups to editing groups. A new method of reception analysis. *Med. Cult. Soc.* **1995**, *17*, 141–150.

60. Asbury, J.E. Overview of focus group research. *Qual. Health Res.* **1995**, *5*, 414–420.
61. Stewart, D.W. *Focus Groups: Theory and Practice*; Sage: Thousand Oaks, CA, USA, 2007.
62. Sutton, S.G.; Arnold, V. Focus group methods: Using interactive and nominal groups to explore emerging technology-driven phenomena in accounting and information systems. *Int. J. Account. Inf. Syst.* **2013**, *14*, 81–88.
63. Fontela, E.; Gabus, A. *The DEMATEL Observer*; Dematel, Battelle Geneva Research Center: Geneva, Switzerland, 1976.
64. Lee, S.G.; Chae, S.H.; Cho, K.M. Drivers and inhibitors of SaaS adoption in Korea. *Int. J. Inf. Manag.* **2013**, *33*, 429–440.
65. Zhou, Q.; Huang, W.; Zhang, Y. Identifying critical success factors in emergency management using a fuzzy DEMATEL method. *Saf. Sci.* **2011**, *49*, 243–252.
66. Ginda, G.; Dytczak, M. Identification of building repair policy choice criteria role. *Technol. Econ. Dev. Econ.* **2009**, *2*, 213–228.
67. Wu, H.-H.; Tsai, Y.-N. A DEMATEL method to evaluate the causal relations among the criteria in auto spare parts industry. *Appl. Math. Comput.* **2011**, *218*, 2334–2342.
68. Huang, C.Y.; Shyu, J.Z.; Tzeng, G.H. Reconfiguring the innovation policy portfolios for Taiwan's SIP Mall industry. *Technovation.* **2007**, *27*, 744–765.
69. Lee, Y.C.; Li, M.L.; Yen, T.M.; Huang, T.H. Analysis of adopting an integrated decision making trial and evaluation laboratory on a technology acceptance model. *Expert Syst. Appl.* **2010**, *37*, 1745–1754.
70. Voudouris, C.; Owusu, G.; Dorne, R.; Lesaint, D. *Service Chain Management: Technology Innovation for the Service Business*; Springer-Berlin: Heidelberg, Germany, 2008.
71. Yang, Y.P.O.; Shieh, H.M.; Leu, J.D.; Tzeng, G.H. A novel hybrid MCDM model combined with DEMATEL and ANP with applications. *Int. J. Oper. Res.* **2008**, *5*, 160–168.
72. Hsu, C.Y.; Chen, K.T.; Tzeng, G.H. FMCDM with fuzzy DEMATEL approach for customers' choice behavior model. *Int. J. Fuzzy Syst.* **2007**, *9*, 236–246.
73. Wu, H.H.; Chen, H.K.; Shieh, J.I. Evaluating performance criteria of Employment Service Outreach Program personnel by DEMATEL method. *Expert Syst. Appl.* **2010**, *37*, 5219–5223.
74. Saaty, T.L. *Decision Making with Dependence and Feedback: The Analytic Network Process*; RWS Publication: Pittsburgh, PA, USA, 1996.
75. Saaty, T.L. Decision making—The analytic hierarchy and network processes (AHP/ANP). *J. Syst. Sci. Syst. Eng.* **2004**, *13*, 1–35.
76. Cheng, E.W.; Li, H.; Yu, L. The analytic network process (ANP) approach to location selection: A shopping mall illustration. *Construct. Innov.* **2005**, *5*, 83–97.
77. Banar, M.; Kose, B.M.; Ozkan, A.; Poyraz, A. Choosing a municipal landfill site by analytic network process. *Environ. Geol.* **2007**, *52*, 747–751.
78. Saaty, T.L. Fundamentals of the analytic network process—Dependence and feedback in decision-making with a single network. *J. Syst. Sci. Syst. Eng.* **2004**, *13*, 129–157.
79. World Economic Forum. *The Global Competitiveness Report 2013–2014*; World Economic Forum: Cologny, Switzerland, 2013.
80. Taiwan External Trade Development Council. *Taiwan Ict Industry*; Taiwan External Trade Development Council: Taipei City, Taiwan, 2013.

81. Tso, Y.-E.; McEntire, D.A. Emergency Management in Taiwan: Learning from Past and Current Experiences. Available online: http://training.fema.gov/hiedu/downloads/compemmgmtbookproject/comparative%20em%20book%20-%20em%20in%20taiwan.pdf (accessed on 22 April 2015).
82. Dilley, M. *Natural Disaster Hotspots: A Global Risk Analysis*; World Bank Publications: Washington, DC, USA, 2005; Volume 5.
83. Dai, S.-Y.; Kuo, S.-Y. Mapmon: A host-based malware detection tool. In Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing, 2007, (PRDC 2007), Melbourne, Victoria, Australia, 17–19 December 2007; IEEE: New York, NY, USA.
84. Wallace, M.; Webber, L.; Webber, L. T*he Disaster Recovery Handbook: A Step-by-step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*; AMACOM: Saranac Lake, NY, USA, 2011.
85. Chang, Y.; Wilkinson, S.; Potangaroa, R. Managing resources in disaster recovery projects. *Eng. Constr. Arch. Manag.* **2012**, *19*, 557–580.
86. Hanaoka, S.; Qadir, F.M. Logistics Problems in Recovery Assistance of Indian Ocean Earthquake and Tsunami Disaster. In Proceedings of the Scientific Forum on The Tsunami, Its Impact and Recovery, Bangkok, Thailand, 6–7 June 2005; Asian Institute of Technology: Khlong, Thailand.
87. Gregory, P.H. *IT Disaster Recovery Planning for Dummies*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
88. Whitson, G. Computer security: Theory, process and management. *J. Comput. Sci. Coll.* **2003**, *18*, 57–66.
89. Rozanski, N.; Woods, E. *Software Systems Architecture: Working with Stakeholders Using Viewpoints and Perspectives*; Pearson Education: NY, USA, 2011.
90. Brooks, C.; Bedernjak, M.; Juran, I.; Merryman, J.; Brooks, C. Disaster Recovery Strategies with Tivoli Storage Management. Available online: ftp://skolai.daba.lv/pub/Arhivatori/adsm_clients/SG246844/sg246844_disaster_recovery.pdf (accessed on 22 April 2015).
91. Rothstein, P.J. *Disaster Recovery Testing: Exercising Your Contingency Plan (2007 Edition)*; Rothstein Associates Incorporated: Brookfield, CT, USA, 2007.
92. Roebuck, K. *Business Continuity and Disaster Recovery: High-Impact Technology—What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*; Emereo Publishing: Brrisbane, Australia, 2012.
93. Smith, G. *Planning for Post-Disaster Recovery: A Review of the United States Disaster Assistance Framework*; Island Press: Washington, DC, USA, 2012.
94. Judson, J. *Disaster Recovery Best Practices—Templates, Documents and Examples of Disaster Recovery in the Public Domain PLUS Access to Content. Theartofservice.com for Downloading*; Emereo Publishing: Brrisbane, Australia, 2012.
95. Saaty, T.L.; William, A. *Super Decisions Software*; RWS Publications: Pittsburg, PA, US, 2004.
96. Reich, B.H.; Benbasat, I. Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quart.* **2000**, *24*, 81–113.
97. Tammineedi, R.L. Business continuity management: A standards-based approach. *Inf. Secur. J.* **2010**, *19*, 36–50.

98. Qian, H.; Yafeng, G.; Yong, W.; Baohua, Q. A web site protection oriented remote backup and recovery method. In Proceedings of the 8th International ICST Conference on Communications and Networking in China (CHINACOM), Guilin, China, 14–16 August 2013.
99. Roberts, W.C. Business Continuity Planning for Disasters is Just Good Planning. In Proceedings of the in Military Communications Conference (MILCOM 2006), Washington, DC,USA, 23–25 October 2006.
100. Nakamura, S.; Nakayama, K.; Nakagawa, T. Optimal backup interval of database by incremental backup method. In Proceedings of IEEE International Conference on Industrial Engineering and Engineering Management (IEEM 2009), Hong Kong, China, 8–11 December 2009.
101. McDowall, R. Computer (In) security–2: Computer system backup and recovery. *Qual. Assur. J.* **2001**, *5*, 149–155.
102. Pirkul, H.; Schilling, D. The capacitated maximal covering location problem with backup service. *Ann. Oper. Res.* **1989**, *18*, 141–154.
103. Miyagawa, M. Joint distribution of distances to the first and the second nearest facilities. *J. Geogr. Syst.* **2012**, *14*, 209–222.
104. Hoopes, J. *Chapter 10—Disaster Recovery. Virtualization for Security*; Hoopes, J., Ed.; Syngress: Boston, MA, USA, 2009; pp. 255–270.
105. Wood, T.; Cecchet, E.; Ramakrishnan, K.K.; Shenoy, P.; van der Merwe, J.; Venkataramani, A. Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges. In Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing, Boston, MA, USA, 22–25 June 2010.
106. Ning, W.; Luo, P. Research on the Information Resources Management Center Construction in E-Government. In Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08, Dalian, China, 12–17 October 2008.
107. Huang, J.J.; Tzeng, G.H.; Ong, C.S. Multidimensional data in multidimensional scaling using the analytic network process. *Pattern Recognit. Lett.* **2005**, *26*, 755–767.