CONF-IRM 2017 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-1-2017

Regulatory Environment of Cloud Computing in New Zealand

Lech J. Janczewski
The University of Auckland, lech@auckland.ac.nz

Morris Ruoyu Miao
The University of Auckland, morris.miao@outlook.com

Recommended Citation
Janczewski, Lech J. and Miao, Morris Ruoyu, "Regulatory Environment of Cloud Computing in New Zealand" (2017). *CONF-IRM 2017 Proceedings*. 27.
http://aisel.aisnet.org/confirm2017/27

REGULATORY ENVIRONMENT OF CLOUD COMPUTING IN NEW ZEALAND

Lech Janczewski
University of Auckland
lech@auckland.ac.nz

Morris Ruoyu Miao
University of Auckland
morris.miao@outlook.com

Abstract

Cloud computing has changed the world dramatically. The objective of this research is to evaluate the technological changes introduced by cloud computing, followed by a review of the regulatory environment of cloud computing from the point of view of protecting all parties involved in using it. The regulatory environment means, for the purposes of this thesis, the existing New Zealand laws and standards, along with some laws and standards from other countries that are effective with respect to New Zealand organisations. A conceptual model is developed, validated, and refined via findings from the collected data, and changes to the current regulatory environment suggested by New Zealand security experts in the industry are presented and discussed.

Keywords

Cloud computing; security and privacy; risks and issues; IT implementation; regulatory environment

1. Introduction

Technologies can change completely every few years, and what we do not know can hurt us badly [47]. Literature reviews have shown an increasing interest in cybercrime, which is predicted to double within the next two years. In New Zealand, of the 11% of survey participants who suffered cybercrime [47], the results showed that it is highly likely that a number of them may have lacked full awareness of the nature and severity of the crime. Companies may not realise the true economic impact of a cyber-attack until long after an incident has occurred.

Cloud computing, a technology that enables the delivery of computing as a service rather than as a product, now significantly influences our daily lives. Relationships in the cloud are complex when compared with the use of traditional information system (IS) technology. Through the use of the Internet, this borderless technology gives every single international citizen easy access to services. However, it also creates a hazard when people are trying to establish their rights.

Unfortunately, not all laws are equal [61]. Ahmad [1] confirmed that cloud users are not currently enjoying equitable legal rights in the cloud environment. The absence of legal protection can trap cloud users badly. In the meanwhile, conflicting laws constrain the use of cloud technology. Users need something to protect them in a more comprehensive way.

The main aim of this research was to evaluate the technological changes introduced by cloud computing, followed by a review of the regulatory environment for cloud computing from the point of view of protection of all parties involved in using it. The term “regulatory environment” refers to existing New Zealand laws and standards. Suggested changes to the regulatory environment must be verified by security professionals. As a result, this research study may provide an insight into how cutting-edge technology such as cloud computing impacts New Zealand organisations. The risks and issues cloud computing introduces will be examined, followed by a comprehensive review of the regulatory environment of cloud computing from the point of view of protection of all parties involved. Suggestions will be made with respect to changing the current regulatory environment to make New Zealand a better breeding ground for cyber technologies.

The structure of this paper is as follows. Section 2 briefly describe the research background derived from literature review, with an analysis framework for this research. Discussion of the research methodology including how the data was collected in presented in section 3. In section 4 a proposed model of the cloud computing regulatory environment of New Zealand is formulated and discussed. Section 5 contains results of data analysis, review the proposed model, and discusses the improved final model. Section 6 summarizes the results and discuss the findings of this research, and finally, section 7 concludes this research and suggests possible future research areas related to this topic.

2. Research background

While the history of cloud computing can be traced back to the 1960s, it has only been widely implemented in production environments since 2006. Within a five-year timeframe, the statistics reported in the 2011 results [6] indicate a very rapid uptake of the technology. With millions of successful deployments, cloud computing has been proven to help organisations reduce operating costs while increasing efficiency in many ways. The Cloud Power Report [6] also indicated that the primary reason for organisations implementing cloud computing was IT efficiency, followed by operational cost savings, the ability to grow and shrink IT capacity on demand, the ability to rapidly launch new products and services, hardware cost savings, absence of upfront investment, software cost savings, increased collaboration, pricing flexibility, hardware utilisation, and convenience for development teams. Furthermore, respondents believed that the major benefits from the implementation of cloud computing over the next five years would be less time spent updating IT infrastructure, followed by the ability to offer more of a service to the business via a more strategic IT environment [6].

A recent KPMG report [23] also found that organisations started changing their views about the benefits of cloud computing from purely cost reduction to realising they could achieve intangible long-term transformational benefits by implementing cloud computing, such as more efficient processes and more flexible operating models. With a significant uptick in cloud usage, more and more organisations began to develop an understanding of their overall lack of knowledge and security concerns, while only seeing security as a crucial challenge when using cloud technologies [39].

Another KPMG report on 539 global business executives published the next year [22] included workforce mobility as one of the most significant benefits that cloud computing brings to the CSU. It supports a wide range of values for organisations, such as increased employee productivity, higher employee satisfaction, improved field service operations, gaining a competitive advantage, increased sales and revenue, improved maintainability of existing competitive advantages, and decreased IT costs. Cloud computing enables mobility, and mobility improves the productivity of users, as well as connecting users more closely to their customers.

The KPMG survey report [22] also showed that 18% of participants started seeing regulation and legislation as a challenge in 2013 while using cloud services. Ohri [39] suggested that this figure has only just started increasing and as organisations get into more complex situations, legislation and regulation-related compliance issues will rise over the next few years.

While CSUs in New Zealand began considering the “what and how” instead of “when and why” during the cloud implementation process, CSPs supported and voluntarily joined a code of practice [34]. The code of practice has been developed for the purpose of addressing concerns about the integrity of cloud computing, and providing consistent standards for CSPs in New Zealand. All of these efforts stem from feedback from CSUs, aiming to provide better confidence in their CSPs when choosing to implement cloud computing in New Zealand [39].

The New Zealand Privacy Commissioner [38] conducted a survey of a broad range of 50 public and private sector organisations to ascertain their experience with overseas-based ICT infrastructure, namely cloud computing. The survey result supported the viewpoint that New Zealanders' information progressively goes outside of New Zealand to overseas infrastructure for a variety of reasons. These off-shore CSPs are most commonly based in the United States, Australia, or Asia. A majority of the survey respondents stated that they did not check how the CSP used or managed their information. A few of the respondents reported that they had no idea how long the information would be retained in their CSP's infrastructure, and another few thought that the CSP kept the information indefinitely [38].

PricewaterhouseCoopers New Zealand [46] [47] has carried out a series of New Zealand-specific Global Economic Crime Surveys every three to four years since 2007. The 2011 version was titled "Fraud, fraudsters, and cybercrime", and from that year on, they started looking at what economic crimes organisations had experienced in New Zealand, especially in terms of cybercrime. The result showed a significant increase of interest in this area relative to the previous economic crime surveys, increasing from a "very low and statistically insignificant" level to be the third highest-ranked economic crime in New Zealand. It was also realised that cybercrime can be a real global threat that can originate from anywhere in the world; unlike many other conventional crimes that could be restricted by jurisdictional boundaries. Another risk was found to be that rapid changes in technology, in terms of the implementation of cloud computing, are making cybercrime difficult for organisations in New Zealand to keep up with in terms of prevention plans, legislation and corporate policies, which need to be continually assessed and monitored to ensure they are being kept on track. The overall result showed cybercrime as the third most frequently-reported type of reported economic crime for the year, constituting 24% of total reported frauds, following Asset Misappropriation and Accounting Fraud. This is more than enough to bring cloud computing security and privacy issues associated with cybercrime into the limelight [46].

The subsequent PricewaterhouseCoopers Global Economic Crime Survey in 2014 again put cybercrime under the spotlight. The results confirmed the significant and continuing impact of cybercrime on business, with 25% of the respondents globally saying they had been victims of cybercrime during the previous 12 months. Interestingly, New Zealand respondents showed a significantly different result of 11%, which was less than half the level of the global results, and also less than half the 2011 New Zealand results. Among the 11% who suffered cybercrime in New Zealand, the results indicated that it is highly likely that a number of respondents who had been victims of a cyber-attack may not have been fully aware of the crime; often companies do not realise the true economic impact of a cyber-attack until long after an incident has occurred. There is a popular statement" "What we do not know can hurt us badly" [47]. Pleasingly, the results also show that New Zealand business leaders are beginning to take the threat of cybercrime seriously; the respondents realised cybercrime is a global issue that does not have a border, and they expect cybercrime to double to 22% over the next two years, with the increasing implementation of cloud computing in New Zealand organisations, and amongst New Zealanders in general.

Despite the increasing risk of being a victim of cybercrime, organisations and individuals are still adopting the cloud. Users are no longer required to have in-depth knowledge of how the technology works and how it is deployed. A price list and a copy of a well-written user manual is enough to get going; they can use services in the form of pay-per-use with a small initial investment and expand the business and their IT infrastructure easily as the service demand rises.

Analysis of the publications in the domain of cloud computing allows to identify the following groups of problems:

2.1 Cloud Computing Risks and Issues Model

Four main set of issues were identified and models has been formulated:

2.1.1 Legislation and Jurisdiction

Conflicting laws exist in different countries with respect to equivalent situations [17]. For example, if a person in Australia uploads data to a cloud computer service that is offered by a United States CSP; which set of laws applies to issues associated with that storage? Ahmad [1] indicated four major categories relating to jurisdictional litigations: misrepresentation, illegality, enforceability of the contract, and information disclosure. In this research, there are six issues connected with multi-jurisdictions.

2.1.2 Standards and Policies

Unlike jurisdiction, the second group deals with issues of standards and policies within a country, a region, or a politico-economic union.

2.1.3 Cloud Service Management

Cloud computing is a form of supplier relationship that is sourced from multiple suppliers [28]. Unlike the jurisdiction issues or laws within a specific country, this third group focuses on cloud service management. This includes the contracts between a CSP and CSU, a CSP and its employees, a CSP and its vendor or a third party CSP, and with the public domain. A good or bad (or, a fair or unfair) contract directly impacts the benefits and satisfaction received during the service by each of the parties. In cloud computing, these contracts are generally referred to as Service Level Agreements (SLAs).

2.1.4 Cloud Technological Requirements

Technologies can change completely within two years, which is far too fast to be caught up with by most legislation systems. Furthermore, cloud computing has yet to establish an exact position in the laws of many countries [17]. Some regulations governing the cloud are impractical and unclear, because they are still derived from previous generations of technologies [24]. In this research, six issues are related to technologies.

2.1.5 Review of the New Zealand Regulatory Environment for Cloud Computing

NZ regulatory environment related to cloud computing includes a number or organisations, laws and regulations:

- Government
  - Government, Parliament
- Government Agencies and Departments
  - Security Intelligence Service, Government Communications Security Bureau, Department of Prime Minister and Cabinet, National Cyber Policy Office, Ministry of Justice, Ministry of Business, Innovation and Employment
- Legislation
  - Privacy Act 1993, Crimes Amendment Act 2003, Government Communications Security Bureau Act 2003, Telecommunications (Interception Capability and Security) Act 2013
- International Standards
  - ISO 7498-2: 1989
  - ISO/IEC 17788: 2014, 17789: 2014, 17826: 2012, 27001: 2013, 27002: 201, 27017 (In-Press), 27018: 2014, 27036: 2014, 29100: 2011
- Other Standards and Policies

- CSA Cloud Controls Matrix v3.0.1
- New Zealand: Health Information Privacy Code 1994, Cloud Computing Code of Practice 2013, Information Security Manual 2014

Based on the literature review presented in this chapter, the research gap has been identified and the research objective of this study is defined as:

Exploring the issues introduced by new technologies and the relationship of these technologies to the regulatory environment in New Zealand

To appropriately achieve this research objective, the following research questions will be addressed:

RQ1: What security and privacy risks and issues are likely to confront New Zealand organisations in the use of cloud computing?

RQ2: What is the regulatory environment with respect to cloud computing in New Zealand?

RQ3: What improvements could be made to the regulatory environment to improve the New Zealand cloud computing environment?

3. Model Development

Review of the research allows us to build a preliminary model of the regulatory environment for cloud computing.

The three mediating factors from Biljon's Diagrammatic Representation of Mobile Phone Technology Adoption Model [5] are consistent with the findings from the literature review: twenty-eight issues were categorised into four groups: legislation and jurisdiction, standards and policies, cloud service management, and cloud technological requirements. In conjunction with Jouini's three factors, the four groups can be consolidated with the three mediating factors and optimised into three dimensions:

- Cloud-related legislation, standards, policies, and regulatory jurisdiction;
- Cloud service management; and
- Cloud technological requirements.

In short, these three factors could be labelled: Environment, People, and Technology. These three dimensions are the key areas to consider when implementing a new technology such as cloud computing in New Zealand organisations. Based on the three dimensions, labels have been produced from the twenty-eight issues, which will be used in further investigations.

3.1 The Security Privacy Risk and Issue Model

The labelling of cloud computing security privacy risks and issues derived from the literature review in section 2, a more understandable three-entity model has been developed for security privacy risks and issues.

Environment-related Issues (SPRI-ENV). Environmental issues are caused by non-human agents, including natural disaster threats such as earthquakes, flood, fire, lightning, storm, tsunami, tornado, or animal-caused damages.

- Conflicts in Jurisdiction

- Misuse of Authority
- Inefficient Judicial Cooperation
- Complicated Adaption to Globalisation
- Limited Offshore Service Usage
- Ambiguous Definition in Regulations
- Outdated Policies and Strategies
- Lack of Enforcement Technique
- Lack of Service Continuity Protection

People-related Issues (SPRI-PPL). The human-related issues include threats caused by human actions such as insiders or hackers who cause damage or risk to information systems.

- Lopsided Contractual Balance
- Ambiguous Data Residual Policy
- Lack of SLA Alteration Notification
- Lack of Risk Prediction from User Side
- ICT Supply Chain Visibility
- Disaster Recovery Plan Notification
- Diverse Understanding of Contract
- Ambiguous ICT Supply Chain Responsibility
- Diverse Understanding of Terms
- Ambiguous Definitions in Contract

Technology-related Issues (SPRI-TEC). Technological issues are caused by physical and chemical processes acting on materials: physical processes include the use of physical means to gain entry into access-controlled areas or any illegal physical access and ownership of information, whereas the chemical components consist of hardware and software technologies as well as indirect system support equipment like power supplies [20].

- Lack of Activity Detection
- Unforeseeable Data Location
- Lack of Evidence Preservation
- Lack of Data Flow Monitoring
- Inappropriate Multi-tenancy Management
- Inappropriate API Usages

3.2 The New Zealand Cloud Regulatory Environment Model

According to the literature review in section 2, the current New Zealand regulatory environment is categorised into five groups (Group 1 to Group 5). In this research study, we will only focus on Group 3: Legislation, Group 4: International Standards, and Group 5: Other Standards and Policies. This is due to the irrelevance and lack of usefulness of Group 1: Government and Group 2: Government Agencies with respect to this research. Thus, the three groups has been remodelled as shown below.

- Legislation
  - Privacy Act
  - Crimes Amendment Act
  - GCSB Act
  - Telecommunication Act
- International Standards
  - ISO/IEC
- Other Standards and Policies
  - CSA CCM
  - NZ HIPC
  - NZ Cloud Code
  - NZISM

3.3 Model Evaluation

The model shows the influence of security and privacy issues on the acceptance of new technology. However, this influence can be mitigated by a sound regulatory environment.

The initial conceptual model was theoretically verified by a matrix of evaluations between cloud computing issues and New Zealand cloud computing legal statutes and standards as listed in the literature review. Fourteen effective New Zealand regulations were sampled against twenty-eight issues from three groups through the Initial Conceptual Model of Cloud Computing Influence. The result shows how much cloud computing security and privacy issues would be covered by the current regulatory environment, as illustrated in Table 4.3.

Issue Type	Issue Count	Statutes Count	Matching Cells	Cells Matched	Coverage %
SPRI-ENV	9 (12)	14	126	56	44.44
SPRI-PPL	10		140	60	42.86
SPRI-TEC	6		84	31	36.90
SPRI	25		350	147	42.00

Table 4.3. Cloud Regulatory Environment Issues Matrix

Theoretically, the study has supposed that the regulations mitigate each type of issue and lead to a higher acceptance level at the end. The results from the matching matrix suggest that the selected statutes have covered around two-fifth of the issues over the three groups. However, this will be further discussed and verified in the next chapter, with data collected from interviews with information security experts in New Zealand organisations.

3.4 Deriving of Propositions

The model shows the influence of security and privacy issues on the acceptance of new technology. However, this influence can be mitigated by a sound regulatory environment.

To solve the research questions, a list of propositions were derived, based on the research models.

RQ1: What security and privacy risks and issues are likely to confront New Zealand organisations when they use cloud computing? (P1-P3)

RQ2: What is the regulatory environment for cloud computing in New Zealand? (P4)

RQ3: What improvements could be made to the regulatory environment to make the New Zealand cloud computing environment better?

The propositions will be discussed, verified, and further elaborated in the empirical section to check whether the literature concurred with the experiences of interview participants from New Zealand organisations.

P1: The environment-related issues introduced by the use of cloud computing have possible impacts on New Zealand organisations.

P2: The person-related issues introduced by the use of cloud computing have possible impacts on New Zealand organisations.

P3: The technology-related issues introduced by the use of cloud computing have a possible impact on New Zealand organisations.

P4: The current New Zealand regulatory environment has a possible impact on risks and issues introduced by the use of cloud computing in New Zealand organisations.

4. Research Methodology

4.1 Using Documents

Myers [62] defined a document as anything that can be stored in a digital file on a computer. As the primary data source for the initial model of this research, a broad range of documents was included and used for building up this model. "Documents" in the context of the current research means administrative papers produced by governmental and privacy agencies, and includes New Zealand legislations, international standards that are effective with respect to New Zealand organisations, and other standards and policies.

4.2 Interview

To acquire primary data, this research study used semi-structured qualitative interviews, with open-ended questions. This approach involved the use of some pre-formulated questions, with some unlisted questions potentially arising during the conversation; this enabled a greater chance of gathering rich data from participants in various roles and situations [9] [62]. With this structure, each interview was expected to require no more than one hour; this provided more flexibility and ease of analysis and comparison. All participants in this study were experts in the field, but from different backgrounds. This study was conducted either face-to-face at the University of Auckland's facilities, at the participants' facilities, or via online video-conferencing, depending on the preference and location of the participants. After the interview, the recording was transcribed as a summary and used in the research.

The interviews were audio-recorded for review and data analysis purposes. Data was de-identified so the participants could not be identified as the source of information. The participants have the option to request a copy of any publications resulting from this research. Participants were chosen from a range of major organisations in New Zealand, and interviewed in a number of individual semi-structured interviews. More information about the participants is provided in section 5.

Finally, recommendations for this research were sought from the participants.

5. Data Analysis and Findings

Background information of the seven chosen experts is presented in Table 5.1 below. The majority of participants were from the 31-40 age range, two of them were in the 41-50 age range, and one was in the 51-60 age range. The job title categories were distributed relatively equally, indicating that the participants were from a wide range in their organisational structures; the participants were also from a range of backgrounds across their industries, with most of them from IT Services, followed by Computer Software, Banking, and Civil Engineering. Almost half of the participants were from organisations with 1 to 1,000 employees, with a similar proportion from organisations employing 1,001 to 10,000 staffs. There was also one participant from an organisation with over 10,000 employees. Regarding their organisation's role in the cloud, two of the participants were from cloud service providers, another two were from cloud service users, and three were from cloud service partners.

Attributes	Groups	Number of Participants
Age Distribution	31-40	4
	41-50	2
	51-60	1
Job Title Category	IT Security Consultant	2
	IT Security Manager	2
	C-Level Executive (Technology)	3
Industry of Organisations	IT Services	3
	Computer Software	2
	Banking	1
	Civil Engineering	1
Number of Employees	1-1000	3
	1001-10000	3
	10000+	1
Role in the Cloud	Cloud Service Provider	2
	Cloud Service User	2
	Cloud Service Partner	3

Table 5.1. Demographic Profile of the Interview Participants

The interview data was analysed in accordance with the seven entities, that is, three from the Risk and Issue Model and four from the Regulatory Model, which was derived from the literature review and subsequent interview analysis. A summary table is shown in table 5.3. The table provides findings based on the seven entities, namely Environment-related Issues, People-related Issues, Technology-related Issues, International Standards, New Zealand Standards and Policies, New Zealand Legislation, and Foreign Legislation and Standards.

Domains	**Entities**	**Count**
Risks and Issues	Environment-related Issues	18
	People-related Issues	24
	Technology-related Issues	7
Regulatory Environment	International Standards	19
	New Zealand Standards and Policies	11
	New Zealand Legislation	10
	Foreign Legislation and Standards	9

Table 5.3. Summary of Findings

6. Discussion

6.1 The Risks and Issues of Using Cloud Computing in New Zealand

Under the category of ***environment-related issues***, security experts were particularly concerned about the limitation of offshore service usage, followed by outdated policies and strategies, and complicated adaptions for going offshore. Under the category of people-related issues, the diverse understandings of contracts and terms were of most concern, followed by the lack of SLA alteration notification and lopsided contractual balance. Experts also suggested attention needed to be paid to risk and issue management techniques, the shadow-IT phenomenon, and users' awareness problems. Finally, in the technology-related category, the major issues were network speed and latency, followed by inappropriate multi-tenancy management and API usage, authentication, access control, and encryption. Experts noted that cloud services rely on reliable connections with good speed. This view was not found in the literature review. Experts also commented that New Zealand currently has only a limited number of optical cables connecting to the rest of the world and that another optical cable would be helpful for New Zealand.

6.2 The Risks and Issues of Using Cloud Computing in New Zealand

Based on the data analysis and findings, a model of the New Zealand regulatory environment with four entities was used in this section to discuss the research findings obtained from the experts' experience and knowledge.

One proposition was developed to help answer the outlined research question. In general, the findings from the data analysis showed that security experts from New Zealand organisations engage with the cloud with the regulatory environment in mind. The statements of interview participants were mostly consistent with the literature, and the comments also indicated the existence of an additional category. The findings supported the proposition that the current New Zealand regulatory environment has a possible impact on risks and issues introduced by the use of cloud computing in New Zealand organisations. More details are shown in the section below.

International Standards. The findings from the data analysis showed that international standards are widely accepted in the industry. The ISO/IEC 27000 family has been fully accepted and was used by all of the security experts; a few of them also suggested it should be used as a starting point for an organisation to build up its security policy. Interestingly, the research study also showed that the interviewed experts were not particularly interested in any other ISO standards. The second most significant international standard for the interviewees was the PCI DSS, a standard used only by the credit card industry; this may because the financial industry is so big that no one can really ignore them while designing a cloud service. The CSA, STAR and CCM have also been recognised as very helpful. The special format of CCM means the experts and their organisations simply need to go through a list to get a good understanding of where their security level lies. Some other international standards such as the OWASP, COBIT, and SOC, are also being considered in some specific industries.

New Zealand Standards and Policies. For those working in a New Zealand organisation, New Zealand standards and policies are the most-considered areas when talking about the regulatory environment. The findings showed six main regulations of interest, with the top two being the NZISM and the New Zealand Cloud Code. The NZISM has existed for some years and is widely accepted, not only by the public sector but also by many organisations from the private sector. As a mandatory regulation for government agencies, the private sector recognises it as a good set of controls to follow, with significant benefits. The New Zealand Cloud Code has received both positive and negative comments. The good side is that this code of practice provides another "good set of rules" for cloud service providers to follow which will make them more "trustworthy" for cloud service users; however the negative side is that many experts do not see the code as practicable for global providers because of its local orientation. Some experts also worried that the Cloud Code may be used for "cloud wash." Some other regulations such as the DIA 104 Question Framework, NZ HIPC, RSP, and BS11 were also mentioned by the experts with the emerging nature of the technology, experts thought that New Zealand still has a long way to go. Person 5 suggested that the government should create a mechanism to allow certification of certain group of cloud services, but not every single cloud service, which he thought "would be too many", for the majority of services that all agencies are likely wanting to use. In that way he suggested that it would be "much more efficient and accurate than every agency doing a certification every time they're wanting to use a service."

New Zealand Legislation. All New Zealand organisations are subject to New Zealand legislation by default. The interviews showed that most of the experts were aware of New Zealand legislation. Some of them have come from a political background with a strong understanding of legislation, while others had a good legal team helping them to cope with the legislation.

The New Zealand Privacy Act 1993 was the legislation most mentioned by the experts, in terms of both providing and using cloud services in New Zealand, followed by the Public Records Act, the Tax Act, and the Customs and Excise Act. A common point of these three Acts, as stated by the experts, was that they all limit the storage of specific types of data offshore, or in the cloud. The main point of such limitation is to protect the information owners' rights or to protect certain sensitive information. The experts appeared to be quite happy about the current New Zealand legislation system as it can be flexible, with exemptions offered in some special cases, and changes in technology will sometimes result in amendments to the Act when necessary. The experts hoped that this situation would continue and improve.

Foreign Legislation and Standards. The main difference between foreign legislation and international standards is that the former are local regulations that do not have any legal effect and may not be usable in New Zealand; the latter are internationally recognised. The interviewed experts suggested adding foreign legislation and standards to this research study, because the cloud is a borderless space and foreign legislation and standards must therefore be considered. Not surprisingly, the United States and the European Union, as the two major world economies, receive the most attention in terms of their legislation and standards. However, this area is still a case-by-case situation, and organisations often have to choose an appropriate jurisdiction to follow based on their target market, to help them work better with the local government and local culture and allow them to remain in contact with customers or providers without too much risk.

6.3 The Refined Model

Based on the discussions, the initial conceptual model has been improved, and the refined model is shown in Figure 6.1. The changes are explained below.

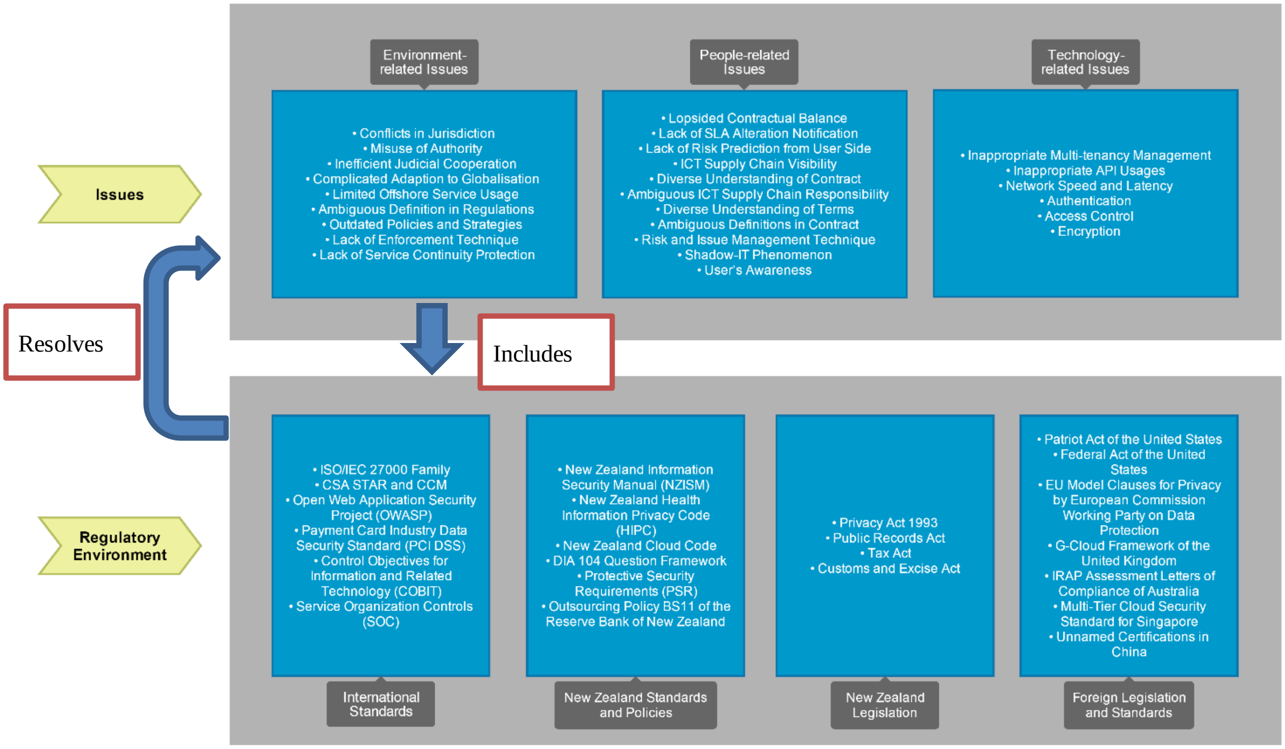
Environment-related Issues
People-related Issues
Technology-related Issues
Issues
• Conflicts in Jurisdiction
• Misuse of Authority
• Inefficient Judicial Cooperation
• Complicated Adaption to Globalisation
• Limited Offshore Service Usage
• Ambiguous Definition in Regulations
• Outdated Policies and Strategies
• Lack of Enforcement Technique
• Lack of Service Continuity Protection
• Lopsided Contractual Balance
• Lack of SLA Alteration Notification
• Lack of Risk Prediction from User Side
• ICT Supply Chain Visibility
• Diverse Understanding of Contract
• Ambiguous ICT Supply Chain Responsibility
• Diverse Understanding of Terms
• Ambiguous Definitions in Contract
• Risk and Issue Management Technique
• Shadow-IT Phenomenon
• User's Awareness
• Inappropriate Multi-tenancy Management
• Inappropriate API Usages
• Network Speed and Latency
• Authentication
• Access Control
• Encryption
Resolves
Includes
Regulatory Environment
• ISO/IEC 27000 Family
• CSA STAR and CCM
• Open Web Application Security Project (OWASP)
• Payment Card Industry Data Security Standard (PCI DSS)
• Control Objectives for Information and Related Technology (COBIT)
• Service Organization Controls (SOC)
• New Zealand Information Security Manual (NZISM)
• New Zealand Health Information Privacy Code (HIPC)
• New Zealand Cloud Code
• DIA 104 Question Framework
• Protective Security Requirements (PSR)
• Outsourcing Policy BS11 of the Reserve Bank of New Zealand
• Privacy Act 1993
• Public Records Act
• Tax Act
• Customs and Excise Act
• Patriot Act of the United States
• Federal Act of the United States
• EU Model Clauses for Privacy by European Commission Working Party on Data Protection
• G-Cloud Framework of the United Kingdom
• IRAP Assessment Letters of Compliance of Australia
• Multi-Tier Cloud Security Standard for Singapore
• Unnamed Certifications in China
International Standards
New Zealand Standards and Policies
New Zealand Legislation
Foreign Legislation and Standards

Figure 6.1. The Refined Model

Firstly, in the risks and issues section, nothing was changed under the entity environment-related issues; however, in the people-related issues section, ambiguous data residual policy and disaster recovery plan notification were removed. Additions were: risk and issue management technique; the shadow-IT phenomenon; and user’s awareness. Under the technology-related issues, four points were removed: lack of activity detection; unforeseeable data location; lack of evidence preservation; and lack of data flow monitoring. Additions were: network speed and latency; authentication; access control; and encryption. Secondly, in the regulatory environment section under international standards, all of the ISO standards were removed apart from the ISO/IEC 27000 family. In the New Zealand standards and policies section, nothing was changed. Under the New Zealand legislation heading, the Crimes Amendment Act 2011, Government Communications Security Bureau Act 2013, and Telecommunications (Interception Capability and Security) Act 2013 were removed and the Tax Act, Public Records Act, and Customs and Excise Act were added. Finally, under the newly added foreign legislation and standards section, seven entries were added: the Patriot Act of the United States; the Federal Act of the United States, EU Model

Clauses for Privacy by the European Commission Working Party on Data Protection; the G-Cloud Framework of the United Kingdom; IRAP Assessment Letters of Compliance of Australia; the Multi-Tier Cloud Security Standard of Singapore; and Unnamed Certifications in China.

The two refined models were joined together according to the relationship that was further defined through the findings of this research, as discussed earlier in this section.

7. Conclusion

The objective of the research was to explore the technological changes introduced by cloud computing, especially the issues raised by such changes, along with presenting a comprehensive review of the current regulatory environment of New Zealand for the technology field. The study spanned one and a half years. The expansion of this research study was heavily connected with the diverse and evolving nature of cloud computing, and the entrenched and rigid nature of regulatory environments. The issues, requirements and objectives of the research study were addressed by building an initial conceptual framework for the security risks and issues involved in cloud computing as well as the current regulatory environment of New Zealand. The models were then interconnected and validated by security experts from New Zealand organisations via seven semi-structured open-ended interviews.

The research study covered the objectives with the aim of helping cloud practitioners to protect themselves, especially in terms of regulatory matters, and of improving the regulatory environment for cloud computing in New Zealand:

Exploring the issues introduced by new technologies and relations to the regulatory environment of New Zealand

In order to develop a thorough analysis in this research study, the entire process was split into two stages: in the first stage, the relevant literature was reviewed, covering a range of documents types dealing with the cloud regulatory environment in New Zealand and internationally. The results of the literature review were then used to develop an initial conceptual model that was used in the second stage. In the second stage, the model was used to develop a set of open-ended interview questions for use in interviews with security experts from New Zealand organisations who had experience working with cloud computing and the regulatory environment. The interviews were to allow these experts to share their stories and to validate the initial conceptual model. Finally, the findings from the literature review and the analysed interviews were summarised and used to develop a theoretical model to fulfil the research objective and address the research questions.

RQ1: What security and privacy risks and issues are likely to confront New Zealand organisations in the use of cloud computing?

This research question is answered by the findings from both the literature review and the analysis of the interviews. The literature review identified three categories of risks and issues that are introduced by the use of cloud computing. The interview analysis agreed with the categorisation, and suggested some additions to and removals from the proposed risks and issues, based on the interview participants' actual working experience in New Zealand.

Both the literature review and the data analysis showed that the three major categories of issues introduced by the use of cloud computing – environment-related, people-related, and technology-related, – all have a possible impact on New Zealand organisations. People-related issues presented the most concerns and were mentioned twenty-four person-times, followed by environment-related issues (eighteen person-times), and technology-related issues (seven person-times). Each person-time here means one relevant concern raised by an interview participant during the interview. The findings also suggest that the top three concerns within the environment-related issue group were limited offshore service usage, complicated adaption to globalisation, and outdated policies and strategies, with five, three, and three persons out of seven mentioning them respectively. The top three issues within the people-related group were the diverse understanding of contract and terms, lopsided contractual balances, and the lack of SLA alteration notification, with five, three, and three persons out of seven mentioning these respectively. Lastly, the top three issues within the technology-related group were network speed and latency, inappropriate multi-tenancy management, and inappropriate API usages, with two, one, and one persons out of seven mentioning these respectively.

The findings suggested that the cyberspace in New Zealand is still so young that we have not yet suffered any major incidents. Of those that have occurred in the past, people have been the primary cause and technology-related matters have not been a major issue. As the interview participants pointed out, to mitigate such issues, especially the people-related ones, the best practice will be to manage the risks and issues rather than trying to completely avoid them.

RQ2: What is the regulatory environment for cloud computing in New Zealand?

This research question is again answered by the findings from both the literature review and the interview data analysis. The literature review identified three collections of regulations within the regulatory environment of New Zealand that are related to the use of cloud computing. In agreement with the literature review, the interviews conducted with New Zealand security experts suggested that in addition to the three previously identified issues (international standards, New Zealand standards and policies, and New Zealand legislation), foreign legislation and standards are also of concern and should be included in this research study, because cyberspace is borderless.

Within the collection of international standards, the findings suggested that the most well-known and well-used regulations are the ISO/IEC 27000 family, which is seen not only as a good set of rules for organisations engaging with the cloud, but also as a starting point for any organisation that is beginning to develop its enterprise information security policy. In addition, the Payment Card Industry Data Security Standard (PCI DSS), the Cloud Security Alliance STAR and CCM programme (CSA STAR and CCM), the Open Web Application Security Project (OWASP), the Control Objectives for Information and Related Technology (COBIT), and the Service Organisation Controls orders (SOC orders) are also considered by organisations while using cloud computing in New Zealand.

The findings also suggested that in the New Zealand standards and policies collection, the New Zealand Information Security Manual (NZISM, now a part of PSR) and the New Zealand Cloud Computing Code of Practice (NZ Cloud Code) were both winners. The NZISM was designed as a mandatory set of controls for the New Zealand public sector to follow; however, it is also frequently referred to by the private sector as a best practice guide. The NZ Cloud Code was designed as guidance to ensure cloud service providers have the capability to provide good-quality products for users; however, it is sometimes called into question as a potential tool for “cloud-wash.” In addition, the DIA 104 Question Framework, the New Zealand Health Information Privacy Code (HIPC), the Protective Security Requirements (PSR), and the Outsourcing Policy BS11 of the Reserve Bank of New Zealand (RBNZ BS11) were all mentioned by the security experts based on the industries relevant to their organisations.

In terms of New Zealand legislation, the mostly frequently mentioned set of laws in New Zealand was the Privacy Act 1993, with five out of the seven interview participants aware of it; followed by the Public Records Act, the Tax Act, and the Customs and Excise Act. The findings suggested that security experts in New Zealand organisations are aware of the legal aspects, with the belief that compliance with the relevant laws will protect both them and their users or providers.

The findings of this research study also suggested the inclusion of an extra section: foreign legislation and standards. In the rapidly evolving virtual world, cyberspace changes continually and without the limitations imposed by national borders. Therefore, a list of non-New Zealand laws and standards were also considered by New Zealand organisations and recommended to the researcher. However, because such jurisdiction-specific legislation and standards are dependent on the location of an organisation's operation, the names of specific regulations are not listed here.

RQ3: What improvements could be made to the regulatory environment to improve the New Zealand cloud computing environment?

This research question was answered by the findings from the interviews with New Zealand information security experts. The findings suggested that cloud computing and the regulatory environment surrounding it in New Zealand is on the right track, exhibiting flexibility and tolerance; exemptions are available upon request if necessary to cope with the fast-changing environment. The experts suggested that New Zealand should continue on this path to further improve the regulatory environment for cloud computing and other new technologies. The interviewees indicated a good approach to security management was to be "thinking of security as a service, rather than a big lock, saying no, and stopping people from being an idiot." The experts also suggested that "in many cases solutions are offshore, go to providers with greater security for that information than New Zealand onshore systems." This is because firstly, "New Zealand doesn't have the scale to be able to invest that way"; secondly, as mentioned in RQ1, New Zealand still has too little experience with major incidents to have generated a high enough level of enforcement for security and privacy violations involving new technologies.

The findings have also shown that the situation in the private sector is much different to the public sector in the use of cloud computing in the New Zealand regulatory environment. There are also differences between different sizes of organisations.

In the private sector, the easiest way to build up a security policy for an organisation with limited resources is, according to one respondent, "when you are in the environment where you need to be compliant, let's grab 27001 as the framework, and put the other requirements into it, depending on what it is, that's what I usually recommend to the clients. Start with the framework, choose the bit you want, clear up what your other requirements are, and slide them in."

In the public sector, the findings also suggested that New Zealand does not currently have a certification framework for the government's infrastructure around providing risk assurance for cloud services. Australia has the IRAP certification framework, to provide high-quality ICT services to government in support of Australia's security. "And that will be much more efficient and accurate than every agency doing a certification every time they want to use a service, and in that way the taxpayers' money would no longer be wasted or poorly applied in this field."

Furthermore, the findings suggested that the New Zealand government should commit to not "weaponizing" the Internet while making efforts to improve security. The cloud and the Internet make things easy to do, and should be free for everyone to use.

7.1 Research Contribution

This research study contributed to the field by providing a comprehensive analysis and discussion of the issues concerning the use of cloud computing technologies, and the regulatory environment of cloud computing in New Zealand. Suggestions were made by New Zealand security experts from the industry, seven of whom participated in semi-structured interviews designed in four sections, using open-ended questions. The experts provided insights and opinions from their experience in the field, in terms of both using cloud computing and dealing with information security related to the use of the cloud. Their contribution helped this research study to validate the findings of the literature review and to improve the initial conceptual model from a best practice perspective in New Zealand. Seven entities were identified in the final refined model, representing the developed concepts. These were divided into two main areas; issues and risks, and the regulatory environment of cloud computing in New Zealand. The relationships between the two areas were identified and validated in this research study. This model will aid understanding of the cloud computing environment in New Zealand. Finally, the findings from the interviews were summarised to provide concluding comments aimed at enabling regulatory environment decision makers and cloud practitioners to improve the New Zealand cloud computing environment.

7.2 Research Limitation

This study on emerging field of cloud computing and its relationship with the regulatory environment involved a number of limitations. Generally, the selection of interview participants was restricted because the researcher's interest was focused on security experts who were familiar with both the regulatory environment and cloud computing, within New Zealand. Therefore, a very limited number of experts were interviewed. The "C-levels", for example, CIOs, CTOs, and CSOs who are often expert in multiple areas and who would have been ideal participants in this research proved to be very difficult to arrange meetings with. Therefore, this research study was conducted using only seven participants who met the research criteria. A larger interview group could provide much more data.

7.3 Future Research

This research study laid the groundwork for future research in several areas as discussed below. Firstly, as mentioned previously, the results would be more reliable with more data-points available for validation. The findings also suggested that cloud computing is not likely to be subject to one-size-fits-all solutions. Therefore, further studies could validate the conceptual model with additional experts representing specified mixes of industries, specified sizes of organisations, and specified types of businesses. Secondly, this research study illustrated three domains relating to risks and issues and four domains relating to regulations. Each of the proposed domains could be used as a starting point for future research.

References

[1] Ahmad, R. 2013. *A Cloud Governance Framework for Cloud Computing: an information security governance perspective to protect cloud users*. Doctoral thesis, University of Auckland, New Zealand.

[2] Al-Qirim, N. 2007. *The adoption of eCommerce communications and applications technologies in small businesses in New Zealand.* Electronic Commerce Research and Applications, 6(4), 462-473.

[3] Avram, M.G. 2014. *Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective.* Procedia Technology, 12, 529-534.

[4] Bhattacherjee, A. 2012. *Social Science Research: Principles, Methods, and Practices.* Textbooks Collection. Book 3.

[5] Biljon, J., Renaud, K. 2008. *A Qualitative Study of the Applicability of Technology Acceptance Models to Senior Mobile Phone Users. Advances in Conceptual Modeling – Challenges and Opportunities.* ER 2008 Workshops CMLSA, ECDM, FP-UML, M2AS, RIGiM, SeCoGIS, WISM, Barcelona Spain, October 20-23, 2008. Proceedings, Pages 228–237.

[6] Cloud Power. 2011. *Cloud computing survey: The results, Microsoft TechNet.*

[7] Cloud Security Alliance. 2015. *Cloud Controls Matrix (CCM).*

[8] Cloud Security Alliance Australia. 2011. *CSA Standards Development Summary.*

[9] Collis, J., & Hussey, R. 2003. *Business Research: A Practical Guide for Undergraduate and Postgraduate Students, (2nd Ed).* New York, NY: Palgrave Macmillan.

[10] CSOonline.com. 2012. *The security laws, regulations and guidelines directory.*

[11] Ferreira, O., & Moreira, F. 2012. *Cloud Computing Implementation Level in Portuguese Companies*. Procedia Technology, 5, 491-499.

[12] Fu, L. 2009. *Social Engineering-based Attacks: Model and New Zealand Perspective*. Master thesis, University of Auckland, New Zealand.

[13] Gauld, R. 2007. *Public sector information system project failures: Lessons from a New Zealand hospital organization*. Government Information Quarterly, 24(1), 102-114.

[14] Government Communications Security Bureau of New Zealand. 2015. *GCSB – Our Work*.

[15] Government Communications Security Bureau of New Zealand. 2011. *New Zealand Information Security Manual*.

[16] Goyal, T., Singh, A., & Agrawal, A. 2012. *Cloudsim: simulator for cloud computing infrastructure and modeling*. Procedia Engineering, 38, 3566-3572.

[17] Gray, A. 2013. *Conflict of laws and the cloud*. Computer Law and Security Review, 29(1), 58-65.

[18] Hooper, C., Martini, B., & Choo, K.R. 2013. *Cloud computing and its implications for cybercrime investigations in Australia*. Computer Law and Security Review, 29(2), 152-163.

[19] Janczewski, L.J., & Fu, L. 2010. *Social Engineering-based Attacks: Model and New Zealand Perspective*. Proceedings of the International Multiconference on Computer Science and Information Technology pp. 847–853.

[20] Jouini, M., Rabai, L.B.A., & Aissa, A.B. 2014. *Classification of Security Threats in Information Systems*. Procedia Computer Science 32, 489-496.

[21] Jula, A., Sundararajan, E., & Othman, Z. 2013. *Cloud computing service composition: A systematic literature review*. Expert Systems with Applications, 41(8), 3809-3824.

[22] KPMG. 2014. *KPMG 2014 Cloud Survey Report – Elevating Business in the Cloud*.

[23] KPMG New Zealand. 2013. *The cloud takes shape - Global cloud survey: the implementation challenge*.

[24] Kshetri, N. 2012. *Privacy and security issues in cloud computing: The role of institutions and institutional evolution*. Telecommunications Policy, 37(4–5), 372-386.

[25] Lindqvist, U., Jonsson, E. 1997. *How to Systematically Classify Computer Security Intrusions*. Proceedings of the 1997 IEEE Symposium on Security and Privacy, page 154. Washington, DC: IEEE.

[26] Livingston, S. 2015. *The Implications of China's Draft Anti*-Terrorism Law for Global Technology. Privacy Tracker Website.

[27] International Organization for Standardization. 1989. *ISO 7498-2: Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*. Geneva, Switzerland: ISO/IEC.

[28] International Organization for Standardization. 2014. *ISO/IEC 17788: Information technology – Cloud computing – Overview and vocabulary*. Geneva, Switzerland: ISO/IEC.

[29] International Organization for Standardization. 2005. *ISO/IEC 17799: Information Technology - Security Techniques - Code of Practice for Information Security Management*. Geneva, Switzerland: ISO/IEC.

[30] International Organization for Standardization. 2006. *ISO/IEC 27002: Information Technology - Security Techniques - Code of Practice for Information Security Management*. Geneva, Switzerland: ISO/IEC.

[31] International Organization for Standardization. 2013. *ISO/IEC 27002: Information Technology - Security Techniques - Code of Practice for Information Security Controls.* Geneva, Switzerland: ISO/IEC.

[32] Mezgára, I., & Rauschecker, U. 2014. *The challenge of networked enterprises for cloud computing interoperability.* Computers in Industry, 65(4), 657-674.

[33] New Zealand Department of the Prime Minister and Cabinet. 2015. *Security and Intelligence Group - National Cyber Policy Office.*

[34] New Zealand Institute of IT Professionals. 2013. *New Zealand Cloud Computing Code of Practice version 2.0.*

[35] New Zealand Security Intelligence Service. 2015. *NZSIS Website.*

[36] New Zealand Law Commission. 2011. *Review of the Privacy Act 1993.*

[37] New Zealand Ministry of Justice. 2015. *Ministry of Justice - Tāhū o te Ture — Ministry of Justice, New Zealand.*

[38] New Zealand Privacy Commissioner. 2011. *International Disclosures and Overseas Information and Communication Technologies Survey May 2011.*

[39] Ohri, C. 2013. *Cloud adoption challenging businesses.*

[40] Organisation for Economic Co-operation and Development. 1980. *Annex to the Recommendation of the Council of 23 September 1980.* Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980).

[41] Organisation for Economic Co-operation and Development. 2013. *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).*

[42] Parliamentary Counsel Office. 2003. *Crimes Amendment Act 2003.*

[43] Parliamentary Counsel Office. 1993. *Privacy Act 1993.*

[44] Parliament of New Zealand. 2006. *How parliament works – Role of Parliament.*

[45] Paul, P.K., & Ghose, M.K. 2012. *Cloud Computing: Possibilities, Challenges and Opportunities with Special Reference to its Emerging Need in the Academic and Working Area of Information Science.* Procedia Engineering, 38, 2222–2227.

[46] PricewaterhouseCoopers New Zealand. 2011. *The 2011 Global Economic Crime Survey results for New Zealand - Fraud, fraudsters and cybercrime.*

[47] PricewaterhouseCoopers New Zealand. 2014. *Economic crime: What you don't know can hurt you - PwC's 2014 Global Economic Crime Survey Results for New Zealand.*

[48] Prinz. 2015. *Investigating of the Impact of National Culture on IT-Governance: An Explorative Study Contrasting German and Japanese National Culture.* Twenty-first Americas Conference on Information Systems, Puerto Rico.

[49] Quick, D. & Choo, K.R. 2012. *Dropbox analysis: Data remnants on user machines.* Digital Investigation, 10(1), 3-18.

[50] Rabai, L.B.A., Jouini, M., Aissa, A. B., & Milli, A. 2013. *A cybersecurity model in cloud computing environments.* Journal of King Saud University Computer and Information Sciences, 25(1), 63-75.

[51] Riessman, C.K. 2002. *Doing justice: Positioning the interpreter in narrative work*. In W. Patterson (Ed), Strategic Narrative: New Perspectives on the Power of Personal and Cultural Storytelling (pp. 195-216). Lanham, MA: Lexington Books.

[52] Riessman, C.K. 2008. *Narrative methods for the human sciences.* Thousand Oaks, CA: Sage Publications.

[53] Rong, C., Nguyen, S.T., & Jaatun, M.G. 2012. *Beyond lightning: A survey on security challenges in cloud computing.* Computers and Electrical Engineering, 39(1), 47-54.

[54] Rowlingson, R.R. 2006. *Marrying Privacy Law to Information Security.* Computer Fraud and Security. 2006(8), 4–6.

[55] Ruf, L., et al. (n.d.). Threat Modeling in Security Architecture. Information Security Society Switzerland.

[56] Schutt, R. K. 2012. *Qualitative Data Analysis. In R. K. Schutt, (Ed.).* Investigating the Social World: The process and practice of research (pp 320-357) Thousand Oaks, CA: Sage Publications.

[57] Sen, J. 2013. *Security and Privacy Issues in Cloud Computing.* In A. Ruiz-Martinez, F. Pereniquez-Garcia & R. Marin-Lopez (Eds.), Architectures and protocols for secure information technology. Hershey, PA: Information Science Reference, IGI Global.

[58] Shahzad, F. 2014. *State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions.* Procedia Computer Science, 37, 357-362.

[59] Snedaker, S., & Rima, C. 2014. *Business Continuity and Disaster Recovery Planning for IT Professionals.* Waltham, MA: Syngress Elsevier.

[60] Southampton Education School. 2012. *Analysing your Interviews.* University of Southampton.

[61] Sundt, C. 2006. *Information Security and the Law.* Information Security Technical Report, 11(1), 2-9.

[62] Myers, M.D. 2013. *Qualitative Research in Business and Management.* SAGE Publications Ltd; 2nd edition.