Article:
Dutta, A., Peng, G.C. and Choudhary, A. (2013) Risks in enterprise cloud computing: the perspective of IT experts. Journal of Computer Information Systems, 53 (4). pp. 39-48.

Dutta, A., Peng, G.C. and Choudhary, A. (2013). "Risks in enterprise cloud computing: the perspective of IT experts". *Journal of Computer Information Systems*, 53 (4), pp. 39-48

Risks in Enterprise Cloud Computing: the Perspective of IT Experts

Arnab Dutta
Information School, University of Sheffield,
Regent Court, 211 Portobello Street, Sheffield, S1 4DP, United Kingdom

Guo Chao Alex Peng*
Information School, University of Sheffield,
Regent Court, 211 Portobello Street, Sheffield, S1 4DP, United Kingdom
Telephone: 0044 114 2222658. Email: g.c.peng@shef.ac.uk
* Corresponding author

Alok Choudhary
Management School, University of Sheffield,
IWP Building, Mushroom Lane, Sheffield, S10 2TN, United Kingdom

ABSTRACT
Cloud computing has become an increasingly prevalent topic in recent years. However, migrating hitherto internal IT data and applications to the cloud is associated with a wide range of risks and challenges. The study reported in this paper aims to explore potential risks that organisations may encounter during cloud computing adoption, as well as to assess and prioritise these risks, from the perspective of IT practitioners and consultants. A questionnaire was designed and distributed to a group of 295 highly experienced IT professionals involved in developing and implementing cloud based solutions, of which 39 (13.2%) responses were collected and analysed. The findings identified a set of 39 cloud computing risks, which concentrated around diverse operational, organisational, technical, and legal areas. The most critical top 10 risks perceived by IT experts were found to be caused by current legal and technical complexity and deficiencies associated with cloud computing, as well as by a lack of preparation and planning of user companies.

Keywords
Enterprise cloud computing, risks, risk management, legal, technical, data security

1. INTRODUCTION

In the contemporary digital age, Information Technologies (IT) have become an integral part of the organisational infrastructure of most knowledge-intensive organisations in any sectors (e.g. manufacturing firms, banks, universities, hospitals, and even governments) and countries. Traditionally, IT resources (including data, software, CPUs, memory cards, and servers) are internally hosted and maintained by user organisations. However, accompanied with continuous business and technology evolution, modern organisations are supported by an increasing number of IT applications and an ever sophisticated IT infrastructure. This increasing amount of internal IT facilities and resources has now become very costly and time-consuming for companies to maintain. Consequently, and also owing to the global economic crisis started in 2008, organisations nowadays are often facing the dilemma to remain high usage of advanced IT applications to sustain competitiveness on the one hand, and to substantially reduce their IT operation and maintenance costs on the other hand. With the development of new IT and web technologies, cloud computing emerges in recent years as a solution to this IT dilemma.

Cloud computing is an advanced IT model to host and share both software and hardware resources over the Internet. It allows organisations to use a pool of IT resources and applications as services virtually through the web, without physically holding these computing resources internally [1]. This innovative cloud model also enables the on-demand provision of computing resources on a pay-as-you-go basis. This makes the use of IT resources similar to the consumption of other daily utilities, such as water and gas [1, 2]. The emergence of cloud computing also facilitates the progression of IT standardization and commoditization, which refers to the phenomenon that IT resources (especially infrastructure resources, e.g. servers, storage, and networks) can be used by user companies as standardized commodities without the need for being uniquely designed, installed and maintained [3, 4].

However, and despite these attractive features and benefits, migrating the hitherto internal IT resources and sensitive business data to a third-party cloud vendor is never an easy decision to be made by CEOs, CIOs and IT managers. In fact, the adoption of cloud computing is associated with a wide range of potential risks and challenges, which have not been sufficiently explored and studied by previous researchers. Therefore, the study reported in this paper aimed to contribute to this research gap by exploring a comprehensive list of potential risks associated with cloud computing. A systematic literature review was carried out at the early stage of the research. As a result of this extensive review, the researchers established a theoretical risk ontology that contains 39 potential risks that organisations may encounter during cloud computing adoption and usage. A questionnaire was constructed based on this theoretical risk ontology and it was used to seek IT professionals' perceptions of the established cloud risks. This paper is organized in the following manner. The next section of the paper presents a further introduction and overview of cloud computing. Subsequently, the research methodology, including the theoretical risk ontology and the research questionnaire design, is discussed. Section 4 presents the analysis and results derived from the questionnaire survey and discussed the overall risk findings including top 10 cloud computing risks. Finally, the theoretical and practical implications of the study are discussed, with conclusions drawn.

2. AN OVERVIEW OF CLOUD COMPUTING

From a historical perspective, computer and IT architecture has evolved rapidly and significantly over the last half-century, from the originally centric ones to the increasingly distributed ones. Specifically, terminals and mainframes were used prevalently in the market during the 1970s and 1980s. In that period of time, people used terminals (i.e. equipments that were just little more than keyboards and monitors) to connect to local mainframes (i.e. large computer machines to process and store data) that were shared by many users [5]. Such traditional terminal/mainframe model resulted in a very centralized computing architecture, and was shortly replaced by stand-alone personal computers (PCs) – users no longer need to share a mainframe with other people, in the late 1980s [5]. With the emergence of network and internet technologies in the 1990s, users can connect their PCs with other computers and servers to exchange information and documents as well as to use remote applications (e.g. through the client/server model). In the early 2000s, with the support of new technologies like Web 2.0 and distributed (e.g. grid and cluster) computing, users can get accessed to a set of external and shared computer resources through an electronic grid over an Ethernet or the Internet [5]. It is widely recognised that distributed/grid computing forms the basis of today's cloud architecture [6].

Cloud computing can be defined as an IT service model, which delivers a set of convenient, on-demand, and configurable computing services and resources [2], to clients

"over a network in a self-service fashion, independent of device and location [and with minimal internal IT effort and…] service provider interaction" [7]. These cloud applications and services can be accessed by not only PCs but also mobile devices, such as smartphones and tablets. Since the emergence of the concept, a wide range of cloud computing services have been developed by IT providers. These cloud services can be divided into three main categories/models [1]:

- *Software as a Service (SaaS).* In the SaaS model, software applications (e.g. organisational email systems, office applications, sales/accounting systems, and even Enterprise Resource Planning or ERP systems) are run on a vendor-managed and controlled infrastructure, and are made available to clients through web browsers.
- *Platform as a Service (PaaS).* In the PaaS model, computing platforms are provided as a service to deploy and run user applications. It offers a programmable environment and middleware to support IT application development and deployment in user companies.
- *Infrastructure as a Service (IaaS).* In the IaaS model, hardware and IT infrastructure resources (e.g. CPUs, hard discs, databases, and servers) are provided as a service to companies through the virtualised cloud environment.

Nowadays organizations are increasingly looking for adopting the various cloud services for supply-chain integration and access to real-time data. Cloud computing also promises to deliver high-quality and advanced IT services to organisations with substantially reduced costs [7], such as reduced hardware investments, less maintenance fees, and lower electricity consumption associated with IT usage. As a result of these features and potential benefits, cloud computing has been widely perceived as one of the most important development in the IT industry in the late 2000s. In particular, from 2008 to 2010 Gartner (a well-known global IT consulting firm) had constantly rated cloud computing as one of the top 10 strategic technologies, which has the potential to change traditional IT usage in organisations and even transform the global IT industry [8]. Furthermore, it was expected in a recent report (entitled "Sizing the Cloud") published by Forrester Research that, the global market size of cloud computing will grow rapidly from US$40.7 billion in the early 2010s to US$241 billion in 2020.

However, and despite these very attractive facts, a wide range of risks can actually occur when adopting cloud computing. A risk can be defined as "the occurrence of an event that has consequences for, or impacts on a particular project" [9]. This definition implies a fundamental characteristic of a risk, namely uncertainty. Specifically, there is a probability that the risk event may occur and can result in an impact on the business processes that may imply substantial losses. Bearing these principles in mind, for the purpose of this study the researchers defined a cloud computing risk as:

> "the occurrence of an event, which is associated with the adoption and use of cloud computing, and can have undesirable consequences or impacts on user companies"

For instance, the inherent features of cloud computing determine that IT operation within a third-party cloud provider will be by no means transparent to user companies, who also have limited control on the subscribed cloud services [10]. Such lack of transparency and control may raise potential risk events related to the security and privacy of business and customer data stored in the cloud [1]. Moreover, user companies need to make a range of internal changes (e.g. designing new business processes, refining IT roles, and downsizing IT department) to prepare themselves to the new cloud environment [11]. This however may

potentially lead to job dissatisfaction of in-house IT and business staff. Furthermore, once companies make the very essential effort to migrate their data and IT applications to the cloud, it will be difficult and very costly for them to move back to the original in-house IT environment if anything goes wrong (e.g. in the case of cloud vendor bankruptcy) [12]. Consequently, fully exploring and understanding these cloud risks and challenges will be fundamental for organisations to decide strategically whether or not cloud computing is the right tool for them, as well as to better prepare them to deal with the potential cloud problems and thus avoid severe technical failure and business disasters. Nevertheless, as a fairly new concept emerged in the late 2000s, there is currently a significant scarcity of studies on cloud computing in general and on cloud computing risks in particular. Moreover, an extensive review of the literature indicated that, existing studies [e.g. 13, 14, 15, 16] on cloud computing risks and challenges focused mainly on security and privacy aspects, but failed to explore a more holistic picture that covers other socio-technical, legal, and business-related risks that are also important in the complicated cloud environment. Therefore, the research reported in this paper is a timely study to address this research gap.

3. RESEARCH METHODOLOGY

3.1. The theoretical risk ontology

In order to establish an explicit IT lens to frame the study and generate data collection tools, a desktop study, based on the process of a critical literature review, was carried out by the researchers. As discussed above, an initial literature review of the study identified that current research on cloud computing risks has been very limited and focuses only on security and privacy aspects. Faced with this scarcity of studies on the topic, a more extensive literature review was conducted at this stage. This critical review followed the systematic approach proposed by Peng and Nunes [17, 18].

Specifically, apart from reviewing studies that directly address cloud computing risks, this systematic review also covers general computing, IT and information systems (IS) journal papers, conference proceedings, books, industrial white papers, and technical reports. The purpose here was "to identify broadly any possible factors and issues that might lead to potential" cloud computing failure [17]. This endeavour resulted in the identification of a large amount of valuable literature, which addressed various IT, cloud computing, legal, and business issues. Subsequently, these retrieved articles and materials were "systematically and critically analysed, compared and synthesised, and then used as raw materials to construct arguments and standpoints for risk identification" [17]. Consequently, through this extensive and critical literature review, the researchers established and proposed a set of 39 potential cloud computing risks. A risk ontology is then developed to organise and present these identified cloud risks. As shown in Figure 1, the established cloud risks were organised into 4 main categories and 12 sub-categories in the risk ontology. The 4 main risk categories include:

- *Organisational risks (OGR).* Cloud adoption can lead to significant impacts on diverse organisational aspects, such as IT governance, compliance to industrial regulations, in-house IT experts, and IT planning. Risks related to these organisational and managerial aspects are categorised as organisational risks.

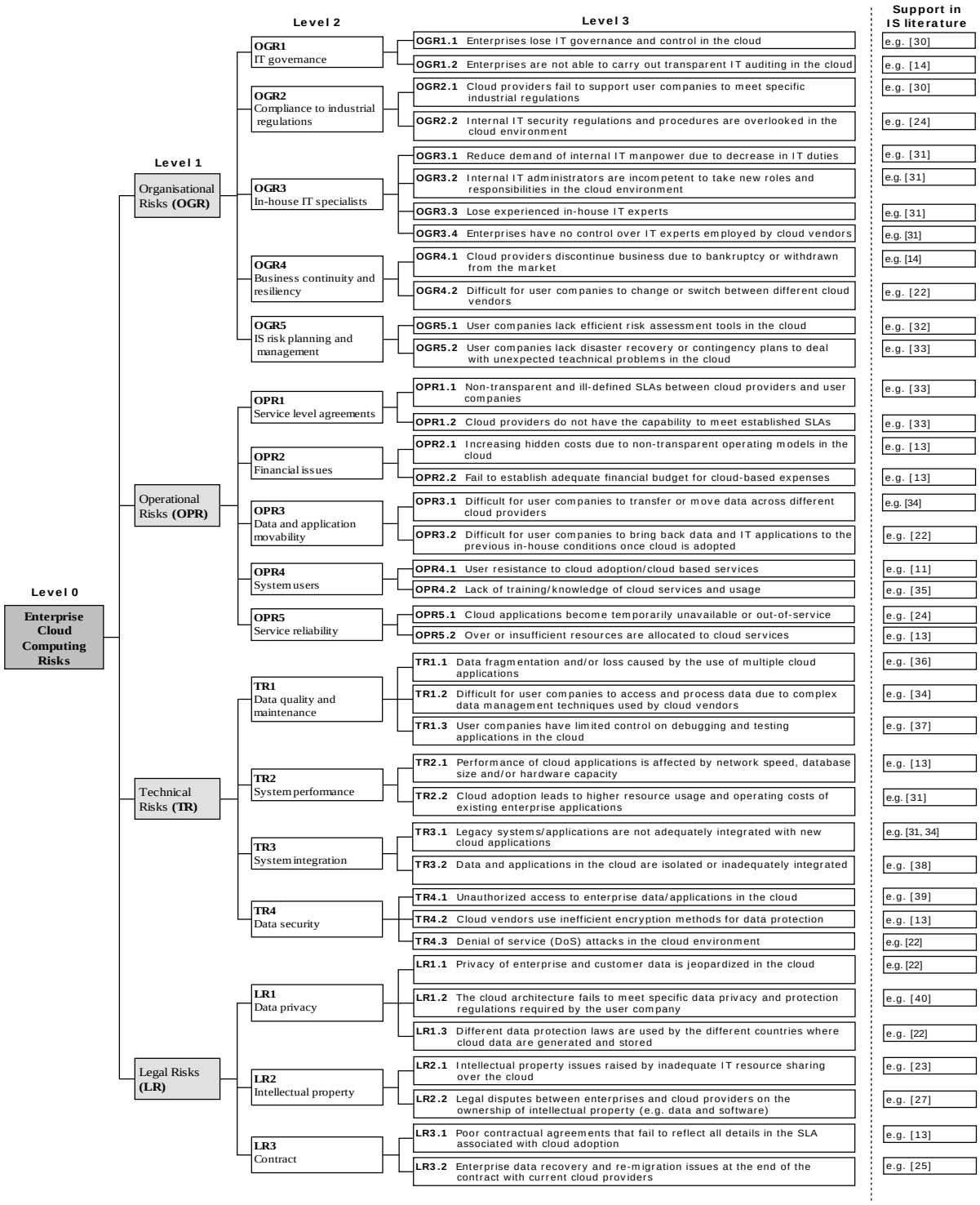

Figure 1. The ontology of cloud computing risks

- *Operational risks (OPR).* The adoption of cloud computing significantly changes the hitherto internal IT and business operations in user companies. Risks affecting daily business and IT operations are thus categorised as operational risks.
- *Technical risks (TR).* The complicated cloud infrastructure and inherent IT deficiencies existed in the company can raise a set of technical risks during cloud computing adoption.

- *Legal risks (LR).* The nature and inherent features of cloud computing can lead to a range of legal risks related to data privacy, intellectual property, and contracts.

In order to examine and explore the suitability of this theoretical risk ontology in current cloud computing practices, a deductive research design based on a cross-sectional questionnaire survey was selected and used as the suitable data collection tool of this study, as further discussed below.

3.2. *The questionnaire design*

The questionnaire began by asking general questions related to respondents' background and previous experience of IT, cloud computing, and risk assessment. Subsequently, the main part of the questionnaire was designed by using the cloud risk ontology as the theoretical basis. In detail, the researchers attempted to identify which of the 39 established events would be perceived by IT experts as risks for cloud adoption, as well as to seek IT professionals' perception on the importance of each identified risk according to its probability of occurrence, level of impact, and frequency of occurrence. In order to achieve these objectives, each predefined risk event was examined in the questionnaire through the following four questions:

1) Whether this event can be perceived as a risk to cloud adoption (1 = yes, 2= no);
2) What is the perceived probability of occurrence of this risk event (measured on a 3-point Likert scale, ranging from high [>60%], to medium [40%~60%], and to low [<40%]);
3) What perceived level of impact this risk could result in (measured on a 3-point Likert scale, ranging from high [i.e. 3 = critical business losses and damage] to low [i.e. 1 = not very critical and may be negligible]);
4) What is the perceived frequency of occurrence of this risk event (measured on a 5-point Likert scale, ranging from very often [i.e. 5 = occur very frequently and repetitively in the cloud service lifetime], to very rarely [i.e. 1 = do not really occur or just occur once in the entire cloud service lifetime]).

Moreover, it was expected that stakeholders, who are interested in cloud computing and have the necessary cloud knowledge to answer the questionnaire, should have good computer literate skills. These potential respondents of the questionnaire thus may prefer filling in the questionnaire electronically, rather than in the traditional paper-based format. Therefore, this questionnaire was developed and conducted electronically.

3.3. Target respondents

As discussed above, cloud computing as a relatively new concept may not currently be fully understood by user companies. Therefore, it was considered that business managers and users may not have sufficient insights on the cloud computing risks explored in this study. In contrast, IT consultants and experts working in the frontier areas of the IT industry were expected to hold more in-depth knowledge on cloud computing issues. Consequently, these considerations led the researchers to select IT professionals and consultants as the prospective respondents of the questionnaire. Moreover, Linkedin as a social networking site has been increasingly used by professionals to establish and maintain personal and specialist networks. This networking site was thus used as a very valuable resource to identify and select potential IT specialists to get involved in the survey.

In details, a thorough search in Linkedin identified that there were more than 1600 cloud-related professional groups that involved hundreds of thousands of members on the site. It

was however found that the same member would often register in at least 3 to 4 groups. Moreover, some smaller groups were actually subgroups of a larger professional group. In other words, there were a lot of duplications among these 1600 groups. There was therefore no need to study all of them. After a further investigation on the search results shown in Linkedin, the researchers specifically selected to target on the following two cloud professional groups that seemed to cover the majority of the current members in this online cloud community:

- The professional group called 'Cloud Computing', created in Feb 2008, with 127,988 members;
- The professional group called 'Cloud Computing, SaaS & Virtulization', created in Dec 2007, with 100,576 members.

More importantly, it was identified that the registered members in these two professional groups vary significantly in terms of IT qualifications and skills, years of IT industrial experience, stages of IT careers, and participation in forums and group discussions. In order to choose the most suitable IT professionals from these groups to be involved in the survey, a set of selection criteria were established and used. In particular, the prospective respondents should:

- Have at least 3 years of professional IT experience (the more IT experience that the member has, the richer insights that he/she may offer to the study);
- Have experience and/or knowledge of cloud computing (having a good knowledge, and even practical experience, of cloud computing is fundamental for stakeholders to provide meaningful answers to the survey);
- Have experience in IT risk assessment and management (previous knowledge and experience in IT risk management can allow potential respondents providing more valuable responses to the questionnaire);
- Show potential willingness to participate in the survey (stakeholders that have a strong willingness and interest to participate in the survey can lead to higher response rate of the study. It was expected that members who were more active in online discussion in these groups might have a stronger willingness to take part in this survey).

Subsequently, the researchers randomly selected and investigated the profiles of members in these two professional groups, as well as observed and analysed online discussions made by them, in order to identify suitable members that satisfied the above selection criteria. Consequently, a sample of 295 highly-qualified IT professionals was selected to participate in this questionnaire survey. An invitation email, which contained 1) a covering letter to explain the purpose of the study, and 2) the URL to the online questionnaire, was sent to these 295 IT professionals. Three weeks after the original email, a reminder was sent out. With these efforts, a total of 39 valid and usable responses were received, representing a response rate of 13.2%. A full demographic profile of the respondents together with the survey findings are presented in the next section.

4. DATA ANALYSIS AND FINDINGS

4.1. Demographic profile of respondents

As mentioned above, demographic information about the respondents' background and experience in IT, cloud computing and risk assessment was explored at the beginning of the

questionnaire. In general, the majority (31 = 80%) of the respondents are located in Western countries, and the remaining 20% are from India. All respondents have international IT working experience (e.g. in the Europe, USA and Asia), and 85% (i.e. 33) of them had previously worked with clients in diverse manufacturing industries and service sectors. In addition, Figure 2 provides an overview of IT and cloud computing experience of these survey respondents.

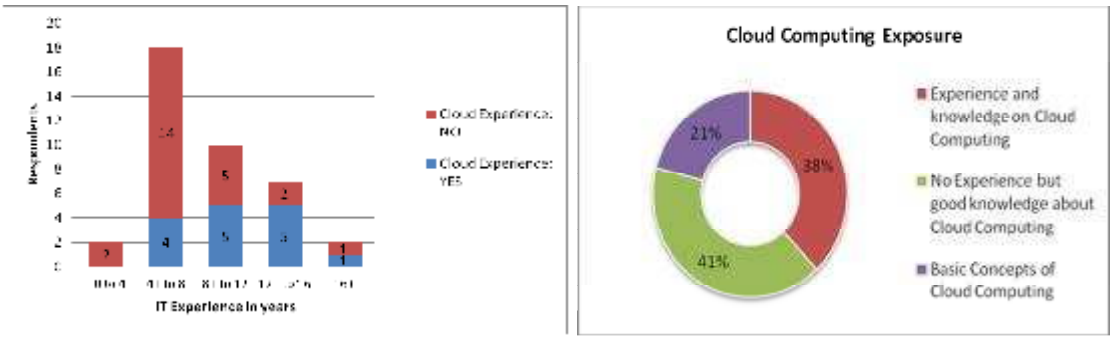

Figure 2. IT and cloud computing experience of respondents

In the bar chart shown in the left side of the figure, it is clearly indicated that the vast majority (37 = 95%) of the respondents have more than 4 years of IT industrial experience. A significant percentage (38.5%) of them also have practical experience in cloud computing. Moreover, the pie chart shown in the right side of the figure indicates that respondents, who do not currently have practical cloud experience, still have good knowledge about cloud computing (41%) or at least understand the basic concepts of this advanced IT model (21%). Apart from general IT and cloud knowledge, Figure 3 below shows that 72% of the respondents also have previous experience in IS risk assessment, and 46% of them even have experience in managing IT projects that involved risk assessment and management practices. Overall, this demographic information proves that respondents of the survey have the necessary IT knowledge and experience to give valuable insights to the cloud risks studied.

Figure 3. IT risk management experience of respondents

4.2. Overall risk findings

The questionnaire findings show that all of the 39 events contained in the risk ontology were perceived by the majority (86%) of the respondents as risk events to cloud computing adoption. Nonetheless, these risks were perceived to have different levels of importance. In particular, the questionnaire asked respondents to indicate and assess the importance of each risk item from three dimensions, namely probability of occurrence, level of impact, and frequency of occurrence. The need for all this information lies in the fact that from a risk management perspective, a risk event that has a high probability of occurrence may not have a high impact, and vice versa. As a typical example, system crash is a risk event that often

has high impact but low probability of occurrence. Moreover, while probability refers to 'how likely' a risk event may occur, frequency refers to 'how often' this event may happen. Therefore, when evaluating the importance of a risk event, it is necessary and vital to take into account all these three risk aspects [19]. Consequently, and in order to facilitate risk assessment, the following formula was developed:

$$\textit{Risk score of each cloud computing risk} = \Sigma\ [W\ *(\textit{Probability} + \textit{Impact} + \textit{Frequency})]$$

This formula was initially established and proposed by Peng and Nunes [19] and then further improved by Pan et al [20], which aimed to identified and assessed ERP post-implementation risks. Because the structure of this formula is consistent with and clearly reflects the questionnaire design of this research, it is adopted as a suitable method to assess cloud computing risks in this study. Based on this formula, the calculation of the risk score for each identified risk event should go through the following 3 steps:

Step 1 *(Probability + Impact + Frequency)*: sum up the values given by each respondent for the three independent dimensions of a risk event, namely probability of occurrence (i.e. high = "2", medium = "1", low = "0.5"), level of impact (i.e. high = "2", medium = "1", low = "0.5"), and frequency of occurrence (i.e. 5 values from very often to very rarely = "2", "1.5", "1", "0.75" and "0.5").

Step 2 *W*(Probability + Impact + Frequency)*: 'W' refers to whether or not the respondent perceived this risk event as a cloud computing risk, with '1' stands for 'yes' and '0' means 'no'. In case that the respondent did not perceive the given risk event as a cloud computing risk, the formula will turn the value generated from Step 1 into 0.

Step 1 and 2 thus generate the individual score that each respondent gave for a specific risk event.

Step 3 Σ *[W*(Probability + Impact + Frequency)]*: sum up the individual score that each of the 39 respondents of the survey gave for a particular risk event, and thus generate the total risk score that this risk event received.

By using this formula, the researchers calculated the risk scores for all of the 39 cloud computing risks identified, and then prioritised these risks based on their risk scores. The top 10 cloud risks ranked by their risk scores are shown in Table 1 below. These top 10 risks were identified as the most critical to current cloud computing practice, and are thus selected to be discussed extensively in the next section.

Table 1. Top 10 cloud computing risks

Rank	Risk ID	Top 10 critical Risk Events for Enterprise Cloud Computing	Risk Score (n=39)
1	LR1.1	Privacy of enterprise or customer data is jeopardised in the cloud	153.50
2	LR1.3	Inconsistent data protection laws adopted by different countries where cloud data are generated and stored	151.75
3	OGR4.2	Difficult for user companies to change cloud vendors even in the case of service dissatisfaction (also known as vendor lock-in)	148.50
4	OGR5.2	User companies lack disaster recovery and contingency plans to deal with unexpected technical issues in cloud environment	147.75
5	LR3.2	Enterprise data re-migration difficulties at the end of the cloud contract	140.25
6	OPR4.2	Inadequate user training/knowledge on cloud services and usage	139.75
7	OPR5.1	Cloud applications become temporarily unavailable or out-of-service	137.25
8	OPR2.1	Increasing hidden costs due to non-transparent operating models in the cloud	136.00
9	TR4.3	Denial-of-Service (DoS) attacks in the cloud environment	135.50
10	TR4.1	Unauthorised access to enterprise data/applications in the cloud	135.00

4.3. Top 10 cloud computing risks

This section further discusses and interprets the questionnaire findings associated with the top 10 cloud computing risks identified. Moreover, possible causes and consequences of these risks are also discussed, with support of evidence drawn from the critical literature review.

Inconsistent laws adopted by different countries and *Privacy of enterprise or customer data is jeopardized*

As presented in Table 1, the top 2 critical cloud risks identified by IT professionals were 'inconsistent data protection laws adopted by different countries' and 'privacy of enterprise or customer data is jeopardized'. As discussed before, the virtualisation feature of cloud computing enables cloud providers to separate enterprise data from internal hardware used by companies. Business and customer data of local companies may often be kept and stored by cloud providers in a different country [21, 22], where resources (e.g. labour and electricity) are cheaper, and thus allowing cloud vendors to maximise their profit levels. However, this common cloud practice may imply the risk that different and inconsistent data protection laws may be applied, in the country that the cloud data were originally generated, and in the country where these sensitive data are stored. The vast majority (81%) of the respondents perceived that the probability of occurrence of this risk event is high to medium. Moreover, the occurrence of this risk event can often lead to potential data privacy concerns. For instance, European customers adopting cloud services provided in the US are often concerned about the U.S Patriot Act, which empowers the US government to access any data without obtaining consent of the data owner [22]. Therefore, 89% of the respondents also considered that this risk event has a high to medium impact on successful cloud adoption.

A further review of the literature identified that apart from inconsistent data protection laws of different countries, inefficient monitoring processes of cloud providers and loose privacy control in the complex cloud environment are also common reasons leading to potential data privacy risks [23]. A significant number (46%) of the survey respondents thus confirmed that there is a high probability and frequency for data privacy to be jeopardised in the cloud. Since these cloud data are concerned with information of not just the user company but very often also their customers, the occurrence of data privacy risk can lead to

very significant impacts, e.g. financial losses and reputational and customer loyalty damages [21], as also confirmed by the majority (86%) of the respondents.

Cloud services become temporarily unavailable and *Increasing hidden costs in the cloud*

For marketing purposes, cloud vendors always promise to make their services reliable and available to user companies. However, owing to a wide range of potential reasons (e.g. unexpected internet disruptions and inadequate system maintenance of cloud vendors), cloud applications may sometimes become temporarily out-of-service. This event was found in previous reports [24] to occur on a regular basis, even with leading cloud vendors (e.g. Google and Microsoft) in the industry. A significant number of the respondents confirmed that this risk event can have a relatively high probability and frequency of occurrence (Figure 6). On the other hand, in the complicated cloud environment, IT services provided by cloud vendors may often be associated with a lot of hidden costs, e.g. disaster recovery costs, application configuration fees, and data loss insurance [13]. These hidden costs may not always be made clear to user companies when they subscribe to the service. Moreover, in order to achieve higher profit levels, cloud vendors may gradually increase their service fees. Consequently, user companies may find that the actual costs of their subscribed cloud services are much higher than their original expectations. A significant number (over 56%) of the respondents perceived that this critical risk event has a high to medium probability and frequency of occurrence in current cloud practices.

The occurrence of these two critical cloud risks can directly reduce user satisfaction [1], and thus may trigger the intention of companies to change their current cloud providers. However, changing cloud vendors, either during or at the end of the service contract, is associated with a lot of difficulties, as further discussed below.

Difficult to change cloud vendors and *Data re-migration difficulties at the end of the cloud contract*

It is apparent that the quality of IT services provided by different vendors in the market can vary significantly. This may be particularly true for cloud computing, since the cloud market is still relatively new and immature. As a result, user companies may sometimes feel unsatisfied about the services provided by their cloud vendors, and thus may want to change to a different service provider. However, changing cloud vendors will not normally be possible during the term of service contracts. Moreover, the potential costs, time and resources required for moving software applications and data across different cloud servers often prevent user companies from changing their cloud vendors [22]. Therefore, user companies were expected to face the risk of not being able to switch their cloud vendors even in the case of service dissatisfaction. This risk event is also known as the vendor lock-in scenario in the cloud environment [22]. A significant number (73%) of the respondents perceived that this critical risk event has a high to medium probability of occurrence

Moreover, the complicated cloud infrastructure, as well as possible legal restrictions made by current cloud providers [25], may also make it difficult for user companies to retrieve and relocate their data to a different cloud server at the end of the existing service contract. 83% of the respondents perceived that there is a high to medium probability for this critical cloud risk to occur.

Overall, these findings clearly suggest that user companies must be very careful when making decisions towards the selection of cloud vendors. Considering potential difficulties

for changing vendors either during or at the end of the cloud contact, companies can suffer very substantial financial loss if they did not make a strategically correct vendor selection decision at the very beginning.

Denial-of-Service (DoS) attacks and *Unauthorised access to enterprise data in the cloud environment*

'Denial-of-Service attacks' and 'unauthorised access to enterprise data' were identified in this study as the two main data security risks in the cloud. A Denial-of-Service (DoS) attack is an attempt by attackers/hackers to prevent legitimate users of an internet service (ranging from normal email to cloud services), from effectively using the service or related network resources [26]. It is one type of most common security risks occurred during the use of internet services, and can take many different forms, such as: 'flood' a network and thus reduce the network bandwidth of a legitimate user; prevent legitimate users from accessing to a service; or disrupt service to a specific user [26]. Nevertheless, although a DoS attack can cost user companies a great amount of time and money to get back to the normal operation, it does not usually lead to data leakage or loss.

In fact, data leakage and loss are more likely to be caused by unauthorised data access, which is another type of critical security risk that may occur in the cloud environment. Unauthorised data access can be the result of either technical deficiencies (e.g. inefficient system security that enables unauthorised people to hack in and steal data in the cloud), or human reasons (e.g. internal staff disclose sensitive data to business competitors) [17]. The majority (69%) of the survey respondents confirmed that, there is a high to medium possibility for these two security risks to occur during cloud usage. The occurrence of these risk events can lead to substantial financial losses, reputation damage, and even business crisis [17]. Therefore, the vast majority (over 86%) of the respondents considered that these critical cloud risks can cause very significant and negative impacts.

User companies lack disaster recovery & contingency plans and *Inadequate user training on cloud usage*

In response to the above unexpected security attacks and any natural system crash in the cloud, it is crucial for user companies to establish efficient internal disaster recovery or contingency plans to prevent data loss and ensure business continuity [27]. However, due to a lack of awareness, training and knowledge, 73% of the respondents stated that there is a high to medium probability for user companies to fail to establish efficient disaster recovery or contingency plans.

On the other hand, system users of client companies need to be properly trained in order for them to use the new cloud services and applications effectively. Substantial training should also be provided to in-house IT experts, who can therefore have the necessary technical knowledge and skills to configure and manage the new cloud database and applications [28]. Otherwise, IT services and applications provided by cloud vendors may not be properly used and maintained by user companies. However, close to 90% of the respondents perceived that there is a relatively high likelihood for companies to fail to provide sufficient cloud training to system users and internal IT staff.

Overall, these findings seem to suggest that companies may not currently have sufficient understanding on possible technical disasters and user issues that can occur in the cloud environment. They may also rely too much on cloud providers, and thus fail to fully prepare themselves to deal with unexpected and undesirable technical and data issues in the cloud.

This lack of planning and preparation may lead to very negative impacts and consequences (such as severe technical and business failures in cloud adoption).

5. FURTHER DISCUSSION AND IMPLICATIONS

As discussed above, when sensitive business and customer data is processed by third-party service providers outside the organisation, business managers of user companies are less immediately aware of the occurrence of any risks in the cloud, and also have no direct ability to control and manage these risks [29]. These inherent features and inevitable issues in the cloud raise immediate concerns and risks related to data privacy and security, which have been the main focus of the majority of current academic studies [e.g. 13, 14, 15, 21] and industrial reports [e.g. 27, 29] on cloud computing. The findings of this study confirmed that data privacy and security risks represent some of the significant challenges in the cloud. However, the findings also identified that the most critical cloud computing risks do not just cluster around privacy and security aspects. That is, critical risks in the cloud as discussed above were also found across diverse legal, operational and business areas. Therefore, it seems that potential failure of cloud computing adoption cannot just be simply attributed to privacy and security risks, but will also be triggered by various operational, organisational, and managerial problems related to both cloud vendors and user companies.

The results of this study have important practical and research implications. In practical terms, the 39 cloud risks in general and the top 10 critical risks in particular, can be used by business managers and IT experts, as a checklist for risk exploration, management and prevention in cloud adoption. The findings of this study also provide useful and valuable insights to support CEOs and in-house IT managers in the process of strategic planning and decision making towards successful cloud computing adoption and usage. In addition, the top 10 critical risks also represent some of the most important areas that current cloud providers should strive to improve, if they want to make their services become more widely used in the industry and consequently facilitate the IT transformation initiated by innovative cloud technologies.

In research terms, this study reinforced the results of previous studies on data privacy and security issues in the cloud, but also complemented these earlier findings by suggesting and confirming the importance of a wide range of cloud-related risks. The extensive risk ontology established in this study can serve as a starting point and theoretical foundation for IT researchers to carry out further investigation in this increasingly important research area. Furthermore, it should be pointed out that some of the top 10 risks discussed are particularly relevant to the cloud environment (e.g. inconsistent laws adopted by different countries). However, giving the shared features of certain IT issues, and also due to the fact that many of the 39 risks were originally grounded from general computing, IT and IS studies (as mentioned in section 3.1), some of these top risks (e.g. inadequate user training) will also be relevant in general IT/IS context. In order words, the findings of this study also contribute to existing knowledge about general IT/IS challenges and risks.

6. CONCLUSIONS

The study reported in this paper employed a questionnaire survey to seek IT experts' perception on potential risks related to enterprise cloud computing. Previous cloud computing studies conventionally put a strong emphasis on data privacy and security challenges. The findings of this study suggest that under the very complicated socio-technical environment in the cloud, risks that can lead to potential cloud computing failure are not restricted to security and privacy aspects. In fact, the study confirmed that a much wider range of cloud computing risks can occur in diverse legal, operational, organisational,

and technical areas. More importantly, the most critical top 10 risks were found to be originated by current legal and technical complexity and deficiencies in the cloud environment. Such legitimate deficiencies and technical complexity can raise substantial challenges for enterprise preparation and planning towards cloud service adoption and usage. Overall, it can be concluded that despite the potential IT and business benefits promised by cloud vendors, the adoption of cloud computing is in fact fraught with challenges and difficulties. In order to achieve success in cloud computing adoption and usage, companies must neither hold an over-optimistic view nor rely merely on their service providers. Instead, a clear understanding and awareness on the identified risks, as well as a thorough preparation across all levels of the organisation, are essential to prevent potential cloud computing failure and business disasters.

Finally, it should be noted that this study has certain limitations. The first limitation of the study lies in the relatively small number of questionnaire respondents. It was experienced in this study that highly qualified IT professionals and consultants always have a tight schedule and thus may not often have sufficient time to participate in research studies. However, their perceptions and insights are very valuable to understand current cloud computing challenges and risks. Further studies may reuse the risk ontology developed in this study to explore cloud computing risks in a larger group of stakeholders, which may involve not just IT professionals but also business managers and users. The results derived from such further studies may be used to compare with the findings of this research, and thus providing a more holistic picture on cloud computing risks. Furthermore, it shall be highlighted that IT risks, including those on a cloud, can also depend on the specific conditions of the industry in which the user company operates (e.g. comparing with manufacturing firms, financial companies dealing with confidential client data may often face more severe cloud challenges). When this paper focused on a set of common cloud computing risks that may occur in any sectors, future studies can investigate what additional cloud risks may be triggered by the specific conditions of diverse industries. It will also be interesting to explore and assess the levels of impact of the identified risks within the context of different industries. Overall, further research on this topic is very much needed.

ACKNOWLEDGMENTS

We would like to thank Professor Alex Koohang (i.e. JCIS Editor-in-Cheif) and the anonymous reviewers for their rapid, encouraging and very constructive comments to improve the quality of this paper.

REFERENCE

[1] Voorsluys, W., Brober, J. and Buyya, R. Introduction to cloud computing. In: Buyya, R., Broberg, J. and Goscinski, A. (eds.), *Cloud Computing Principles and Paradigms*. New Jersey: John Wiley & Sons Inc; 2011.

[2] Mell, P. and Grance, T. The NIST definition of cloud computing - recommendations of the National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [2011, accessed Apr 2012].

[3] Muhss, F., Neumann, R. and Schmietendorf, A. The commoditization of IT services with cloud computing. *In proceedings of the International Conference on Semantic Web and Web Services (SWWS'11)*, Las Vegas, USA, July 2011.

[4] Lee, C.A. A perspective on scientific cloud computing. *In proceedings of the 19th ACM International Symposium on High Performance Distributed Computing*, Chicago, Illinois, June 20-25 2010; 451-459.

[5] Voas, J. and Zhang, J. Cloud Computing: New Wine or Just a New Bottle?. *IT Professional*, 2009; 11 (2): 15-17.

[6] Furht, B. Technologies and Systems: Cloud Computing Fundamentals. In: Furht, B. and Escalante, A. (eds.), *Handbook of cloud computing*. New York: Springer; 2010.

[7] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. Cloud computing - the business perspective. *Decision Support Systems*, 2011; 51 (1): 176-189.
[8] Pettey, C. Gartner identifies the top 10 strategic technologies for 2011. http://www.gartner.com/it/page.jsp?id=1454221 [2010, accessed Jan 2011]
[9] Kleim, R. L. and Ludin, I. S. *Reducing project risks*. Hampshire: Gower Publishing Ltd; 2000.
[10] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J. Controlling data in the cloud: outsourcing computation without outsourcing control. *In proceedings of the 2009 ACM workshop on Cloud computing security*, Chicago, Illinois, USA, 2009. 85-90.
[11] Ali, K.H. Cloud migration: a case study of migrating an enterprise IT system to IaaS. *In proceedings of the 3rd IEEE International Conference on Cloud Computing*, Miami, Florida, 2010. 450-457.
[12] Black, E. Let market decide about mainframes. *Financial Times* (London, England), 16-Oct-2009.
[13] Mather, T., Kumaraswamy, S. and Latif, S. *Cloud security and privacy: an enterprise perspective on risks and compliance*. Sebastopol: O'Reilly; 2009.
[14] Onwubiko, C. Security Issues to Cloud Computing. In: Antonopoulos, N. & Gillam, L. (eds.), *Cloud Computing Principles, Systems and Applications*. London: Springer; 2010.
[15] Bisong, A. and Rahman, S.S.M. An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications*, 2011; 3 (1): 30-45.
[16] Sosinsky, B. *Cloud computing bible*. Indiapolis: Wiley Publishing Inc; 2011.
[17] Peng, G.C. and Nunes, J.M.B. Surfacing ERP exploitation risks through a risk ontology. *Industrial Management & Data Systems*, 2009; 109 (7): 926-942.
[18] Peng, G.C. and Nunes, J.M.B. Establishing and verifying a risk ontology for ERP post-implementation. In Ahmad, M., Colomb, R.M. and Abdullah, M.S. (editors), *Ontology-based applications for enterprise systems and knowledge management*. Hershey, USA: IGI Global; 2012.
[19] Peng, G.C. and Nunes, J.M.B. Identification and assessment of risks associated with ERP post-implementation in China. *Journal of Enterprise Information Management*, 2009; 22 (5): 587-614.
[20] Pan, K., Nunes, J.M.B. and Peng, G.C. Risks affecting ERP post-implementation: insights from a large Chinese manufacturing group. *Journal of Manufacturing Technology Management*, 2011; 22 (1): 107-130.
[21] Pearson, S. Taking account of privacy when designing cloud computing services. *In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009; 44-52.
[22] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. A view of cloud computing. *Communications of the ACM*, 2010; 53 (4): 50-58.
[23] Jaeger, P.T., Lin, J. and Grimes, J. M. Cloud computing and information policy: computing in a policy cloud?. *Journal of Information Technology & Politics*, 2008; 5 (3): 269-283.
[24] Williams, M.I. *A quick start guide to cloud computing: moving your business into the cloud*. London: KoganPage; 2010.
[25] Joint, A., Baker, E. and Eccles, E. Hey, you, get off of that cloud?. *Computer Law & Security Review*, 2009; 25 (3): 270-274.
[26] Lau, F., Rubin, S.H., Smith, M.H. and Trajkovic, L. Distributed denial of service attacks. *In proceedings of the 2000 IEEE International Conference on Systems, Man, and Cybernetics*, 2000; 2275 - 2280
[27] Catteddu, D. and Hogben, G. Cloud computing: benefits, risks and recommendations for information security. Technical report. European Network and Information Security Agency (ENISA). www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport [2009, accessed Mar 2012].
[28] Hurwitz, J., Bloor, R., Kaufman, M. and Halper, F. *Cloud computing for dummies*. Indianapolis: WIley Publishing Inc; 2010.
[29] Heiser, J. and Nicolett, M. Assessing the security risks of cloud computing. http://cloud.ctrls.in/files/assessing-the-security-risks.pdf [2008, accessed Mar 2012]
[30] Chaput, S.R. and Ringwood, K. Cloud compliance: a framework for using cloud computing in a regulated world. In: Antonopoulos, N. and Gillam, L. (eds.), *Cloud computing principles, systems and applications*, 241-255. London: Springer-Verlag; 2010.
[31] Bannerman, P.L. Cloud computing adoption risks: state of play. *In proceedings of the 17th Asia Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop*. Sydney, Australia, 30 Nov-03 Dec, 2010.
[32] Fito, J.O. and Guitart, J. *Introducing risk management into cloud computing*. Barcelona: Barcelona Supercomputing Center and Technical University of Catalonia; 2010.

[33] Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I.M., Montero, R., Wolfsthal, Y., Elmroth, E., Ben-Yehuda, J.C.M., Emmerich, W. and Galán, F. The Reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development*, 2009; 53 (4), paper 4.
[34] Goyal, P. Enterprise usability of cloud computing environments: issues and challenges. *In proceedings of the 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, 28-30 June 2010; 54-59.
[35] Hayes, B. Cloud computing. *Communications of the ACM*, 2008; 51 (7): 9-11.
[36] Vouk, M.A. Cloud computing - issues, research and implementations. *In proceedings of the 30th International Conference on Information Technology Interfaces*, 23-26 June 2008; 31-40.
[37] Rimal, B.P., Choi, E. and Lumb, I. A taxonomy, survey, and issues of cloud computing ecosystems. In: Antonopoulos, N. and Gillam, L. (eds.), *Cloud computing principles, systems and applications*. London: Springer; 2010.
[38] Govindarajan, A. and Lakshmanan, G. Overview of cloud standards. In: Antonopoulos, N. and Gillam, L. (eds.), *Cloud computing principles, systems and applications*, London: Springer-Verlag; 2010.
[39] Morrow, S. Data security in the cloud. In: Buyya, R., Broberg, J. and Goscinski, A. (eds.), *Cloud computing principles and paradigms*. New Jersey: John Wiley & Sons Inc; 2011.
[40] Abadi, D.J. Data management in the cloud: limitations and opportunities. *IEEE Data Engineering*, 2009; 32 (1): 3-12.