Research online Publishing
www.ronpub.com

Open Access

Open Journal of Cloud Computing (OJCC)
Volume 5, Issue 1, 2018
http://www.ronpub.com/ojcc
ISSN 2199-1987

Cyber Supply Chain Risks in Cloud Computing – Bridging the Risk Assessment Gap

Olusola Akinrolabu[A], Steve New[B], Andrew Martin[A]

[A] Department of Computer Science, University of Oxford, Oxford OX1 3QD, UK,
{olusola.akinrolabu, andrew.martin}@cs.ox.ac.uk
[B] Said Business School, University of Oxford, Oxford OX1 1HP, UK, steve.new@sbs.ox.ac.uk

Abstract

Cloud computing represents a significant paradigm shift in the delivery of information technology (IT) services. The rapid growth of the cloud and the increasing security concerns associated with the delivery of cloud services has led many researchers to study cloud risks and risk assessments. Some of these studies highlight the inability of current risk assessments to cope with the dynamic nature of the cloud, a gap we believe is as a result of the lack of consideration for the inherent risk of the supply chain. This paper, therefore, describes the cloud supply chain and investigates the effect of supply chain transparency in conducting a comprehensive risk assessment. We conducted an industry survey to gauge stakeholder awareness of supply chain risks, seeking to find out the risk assessment methods commonly used, factors that hindered a comprehensive evaluation and how the current state-of-the-art can be improved. The analysis of the survey dataset showed the lack of flexibility of the popular qualitative assessment methods in coping with the risks associated with the dynamic supply chain of cloud services, typically made up of an average of eight suppliers. To address these gaps, we propose a Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, a quantitative risk assessment model which is supported by decision support analysis and supply chain mapping in the identification, analysis and evaluation of cloud risks.

Type of Paper and Keywords

Regular research paper: *cloud computing, cloud risks, supply chain, risk assessment, quantitative, transparency, visualisation, visibility*

1 Introduction

Cloud computing is an Information Technology (IT) revolution, whose emergence not only disrupted IT service delivery but also altered infrastructure architecture and application development. Its ability to transform people and processes with every adoption has gradually made it a core component of digital transformation strategies of organisations. Often referred to as a computing resources management model [49], cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, and can be rapidly provisioned and released, with minimal management effort or service provider interaction [56]. While cloud computing technologies can be implemented based on a wide variety of architectures, under different service and deployment models, the security challenges that cloud computing presents are formidable, particularly in the public cloud, where infrastructure and computational resources are owned and operated by third parties who deliver the services via a multi-tenant platform [45].

The use of public cloud means that organisation's data and applications are managed outside their *trust* *boundary*, with the service provisioning potentially requiring a dynamic supply chain. The supply chain is the core of every cloud service delivery, and it consists of a globally-distributed and dynamic collection of people, processes and technologies that encompass various software and hardware components [21]. The security of a cloud service strongly depends on the cloud provider (CP) and its supply chain, their implemented processes and the infrastructure in place. While not all cloud security problems are new, cloud computing introduces a new set of risks, changing the probability of success for a threat source and increasing the impact of an attack [35]. Evidence also suggests that many of the cloud risks are systems risks, where the greater the threat of a failure along the supply chain, the more likely it is for the cloud service to fail [22]. However, the variety of parties involved in cloud service delivery makes it difficult for cloud stakeholders to assess their cloud risks. This new attack surface presents system administrators, cloud customers (CC), co-tenants, and external attackers with the opportunity to launch malicious or unintentional attacks [12]. As such, cloud risks require new risk assessment solutions.

Nevertheless, we acknowledge that assessing and managing cloud risks can be a challenge since significant portions of the computing services are under the control of external parties. Cloud consumers find it difficult to determine the location of their data and third parties involved in its processing, due to the complex ecosystem of suppliers involved in cloud delivery. Several lines of evidence have suggested that this limited cloud supply chain visibility is the reason why some cloud customers engage in simple risk assessment based on qualitative methods to ensure compliance, while others choose to blindly trust their cloud providers without verifying the existence of security controls [24, 72, 8]. Improving cloud risk assessments, therefore, calls for a more transparent supply chain and the visibility of security controls.

Therefore, seeing that few studies have investigated the effect of supply chain risks in cloud computing, or looked into assessing cloud risks from a supply chain perspective, we surveyed cloud professionals to understand the industry practices with regards to cloud risk assessment and their level of awareness of cyber supply chain risks. Administering the survey to a wide range of cloud professionals, many of whom are experienced security and risk experts, we sought to find out the conventional risk identification/assessment methodologies employed within their environment, and identify factors that could improve cloud risk assessment. We present our findings in the result section of this paper.

The remainder of the paper is structured as follows: In Section 2 we present the relevant background and literature on cloud computing, supply chain and risk management. Section 3 presents the cloud supply chain, introducing the five elements of every cloud supply chain and our proposed risk assessment model, Cloud Supply Chain Cyber Risk Assessment (CSCCRA). Section 4 presents our survey results on cloud risk assessment and supply chain risks, and Section 5 concludes the paper.

2 Background and Literature Review

Cloud computing, in its simplest sense, could be referred to as a computing resources management model. It is a method for pooling and distributing hardware infrastructure resources on a massive scale [49]. Cloud computing fosters innovation and is described by Kushida et al. as simultaneously being an innovation ecosystem, a production platform and a global marketplace [49]. However, while some of this innovation is novel, others have fundamentally been transformed from an existing service and relabelled as a cloud service. The efforts of the non-traditional outsourcing companies like Amazon and Google are seen to have led the introduction of the new cloud business models, offering scalability, efficiency and flexibility on a pay-per-use basis [50].

Risk, which is a function of the likelihood of the occurrence of threat events and the potential adverse impact of the events [66], has remained an important topic in many discourses on cloud computing. In [5], a security risk assessment is described as a process aimed at examining possible threats and vulnerabilities as well as the likelihood and impact of them per the external and internal relative technology standards. The two broad categories of risk assessment are the Qualitative and Quantitative risk assessment methods [66]. Despite the incentives for cloud stakeholders to take a proactive and continuous approach to address information security risks, not least for legal and compliance requirements, there has been no reliable evidence that cloud providers devote their attention to assessing and mitigating security risks. Shameli-Sendi and Cheriet [69] also note that the existing risk assessment frameworks have been unable to cope with the challenges introduced by cloud computing. This is perhaps due to the dynamic nature of the cloud infrastructure and services, the lack of physical control, the absence of a well-structured risk cloud management framework and the lack of trust in cloud providers [55].

Cloud risks are associated with the processes, procedures, and practices used to assure the confidentiality, integrity, security, resilience, and quality of cloud services [15]. These risks increase with the on-demand, automated, and multi-tenanted cloud, where customers and providers are rapidly changing, technology advancing, and data and services regularly exposed to new threats. Cloud supply chains increasingly depend upon integrated and interoperable IT systems for efficient management, and there exists multi-level networked relationships among a heterogeneous group of organisations, many of which are small and medium-sized enterprises (SMEs) [38]. The vulnerability of these SMEs to cyber attacks is magnified into the supply chains, where they represent the weakest links, making them a 'soft' target for cybersecurity breaches [51]. Recent studies, particularly the Verizon Enterprise report [19], also showed that 92% of the cybersecurity incidents occurred among small firms with inadequate security systems controls. To further complicate the matter, organisations lack clarity, understanding, and awareness of their suppliers' dependencies or reliance on second, third or fourth parties for cloud service delivery [21].

While the cloud faces some of the threats applicable to any information system, it increasingly faces unique threats and vulnerabilities. Cloud services are exposed daily to new attack scenarios, which can be heightened by vulnerabilities of the cloud provider (employees, facilities, systems), the cloud technology (interfaces, API) or even other cloud co-tenants [55]. Many pieces of research have looked into the assessment of cloud risks both quantitatively and qualitatively, and have listed the typical challenges of risk assessment to include: (a) lack of appropriate historical data, (b) lack of trust in the cloud service providers (CSP) and the data provided for risk assessment, (c) the dynamic supply chain of infrastructure and services, (d) immature offering from CSPs, and (e) the lack of visibility of security control [55][30][27][5].

According to Jenks [46], there is a gap between the processes needed to manage cyber risks in cloud computing, and the implemented solutions. Our reflection on literature identified a significant number of reports addressing the existence of supply chain security risks in cloud computing, but only a few recommended solutions to these risks [58][54]. There is limited information on how cloud threats apply to real-world scenarios or the attack vector used, and the result of those events [23]. Boyson [17] discussed a recent study by Symantec, where, based on Symantec's network monitoring across 157 countries, they found supply chain to be their latest threat vector, and attributed this to the increased attacks on their contractors and subcontractors who are often in possession of a valuable intellectual property. The importance of continuous risk evaluation is more evident in cloud computing than traditional IT, primarily due to the dynamism of the cloud supply chain. This has led leading organisations and standards such as the Centre for the Protection of National Infrastructure (CPNI) [36] and ISO21000 to include the visibility, transparency and inclusivity of third-party risks as crucial elements of effective risk management.

The primary challenge of assessing cloud risks is that the data needed to estimate the impact and likelihood of risk scenarios or events are either unavailable or inadequate [29]. Power [62] suggests that reputational risk hinders this level of transparency, and the existing industry approaches to promote transparency through security certification, cloud provider self-assessment and third party audits, have been flawed by their occurrence on a yearly basis and due to customer's lack of trust [44]. The cloud industry's lack of transparency is characterised in the Cloud Security Alliance's (CSA) report on cloud outages between 2008 and 2013, where they listed 172 unique cloud computing outage incidents for the period, and at least 43 incidents (25%) had no information on the root-cause of the outage [48]. Cloud customers are often in the dark during cloud service adoption, unable to distinguish between cloud services based on security features or processes implemented by the cloud providers. Nevertheless, Werff et al. [75] in their compelling analysis of cloud trust, highlighted the advantage of customer's trust built on the knowledge of provider's processes, architectures, and visible controls over the trust based on pure calculation.

Together, these studies provide evidence to support the dynamic supply chain of cloud services, the inherent risk in the supply chain, and the need for cloud stakeholders to accept some degree of risk. While there are various unaddressed issues with cloud computing risk and risk assessment, there is a core element of trust, which seems to inhibit cloud adoption, consequently calling for a more transparent supply chain. The transparent supply chain would require cloud providers to provide valuable information to customers on how their sensitive data is protected, giving the customers the opportunity to question, test, and probe the security and privacy of their data. In this ideal situation, enterprises have the information they need to engage in a comprehensive risk assessment of their cloud services and can make optimal decisions about where and how to outsource the processing of their data. As ISACA/CSA [43] rightly puts it, 'transparency into the adequacy of the system of internal controls provides trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk'.

2.1 Existing Approaches to Cloud Risk Assessment

There is a relatively small volume of published studies that have looked into cloud computing risk assessments both from the academic and industrial communities. The current state-of-the-art in cloud risk assessment is presented in the works of Alturkistani et al. [5] and Drissi and Benhadou [27], where the authors classified the current cloud risk assessment approaches into five and seven categories respectively. Apart from the traditional risk assessment standards, frameworks and guidance documents which are predominantly qualitative, other cloud risk assessment models have been proposed and developed over the years, and we present here a cross-section of these studies.

QUIRC, which stands for Quantitative Impact and Risk Assessment Framework for Cloud Security, is presented in [68]. QUIRC is a quantitative risk assessment model that operates based on six key security objectives, similar to Microsoft's STRIDE [57]. QUIRC uses the Federal Information Processing Standard (FIPS) model (LOW, MEDIUM, HIGH) for the potential impact definition and assigns scores to the threat scenarios affecting these six security objectives (SO). It employs a modified wide-band Delphi method to scientifically collect numerical estimates for the impact of events and the degree of confidence in the probability values, to arrive at a consensus on the value of a risk. In [69], Shameli-sendi and Cheriet proposed a risk assessment model for cloud computing based on fuzzy multi-criteria decision-making technique and uses expert opinions to weigh the impact of threat on the confidentiality, integrity and availability of an IT asset. The proposed framework is quantitative, iterative, and follows an incremental approach that is capable of providing cloud consumers with a predictable lifecycle security process for the development, adoption, and continual improvement of their cloud security solution. Similarly, Liu and Liu [53] proposed an information security risk assessment model based on analytic hierarchy process (AHP) for cloud computing environments. Using the integrated method of risk analysis, they combine qualitative and quantitative analysis methods and complement it with expert experience and objective facts to perform a comprehensive cloud risk assessment.

SECCRIT (SEcure Cloud computing for CRitical Infrastructure IT) is a cloud risk assessment model, developed to assist organisations in determining the risk associated with the adoption of a particular cloud service [11]. In support of an organisations' decision-making, they define an extension to existing asset-driven risk assessment processes. They take the assessment result of a non-cloud deployment and augment it with risks associated with cloud deployment scenario. In a similar approach to SECCRIT, Cayirci et al. [18] designed the cloud adoption risk assessment model (CARAM), a qualitative and relative model that helps cloud customers with assessing the various business, security and privacy risks in the cloud. It is based on existing frameworks of organisations such as European Union Agency for Network and Information Security (ENISA), CSA, and Commission Nationale de l'informatique et des Liberts (CNIL). It is proposed as a ranking algorithm that matches cloud customer requirements with cloud provider services, with each CP given a risk score based on their response to the Consensus Assessments Initiative Questionnaire (CAIQ). The EU-funded project OPTIMIS [26] also developed a risk assessment method that applies to different cloud stakeholders at various stages of the cloud service provisioning lifecycle. The risk assessment framework shows how supply chain transparency assists cloud providers in assessing the risks of their infrastructure provider (IP), stressing the importance of past service level agreement (SLA) performance, geographical location, security compliance, business stability and general infrastructure, in assessing the risk of the infrastructure provider. Zalazar et al. [76] developed a security and compliance ontology for cloud service agreements, which can help consumers to evaluate security risks of a cloud service and to make a decision on whether to adopt the cloud service.

In all the studies reviewed here, there was a distinct lack of consideration for the risks inherent in the complex, dynamic, and interdependent supply chain, and how it could affect the frequency of a threat or the impact of such threat on a cloud asset. We hypothesise that this could be due to the lack of transparency of cloud providers or the limited visibility customers have into the security controls implemented by the providers. Likewise, none of the studies reviewed expressed the value of risk in financial terms, an approach which is known to help with presenting a clear picture of risk to decision-makers and help justify significant security investments [67][9].

With these highlighted gaps, we identify the need for researchers to look into the problem of supply chain risks in cloud computing, with the view of improving cloud risk assessment through the transparency of the supply chain. Currently, no other study has addressed this problem, and neither has there been a solution that proposes the application of a quantitative probabilistic method to cloud risk assessment, presenting the value of risk as a dollar value. We believe such cloud risk assessment approach will provide organisations with an objective risk result, that is consistent, easy to understand by the decision makers and encourages the mitigation of cloud risks to an acceptable level. Based on the complexity of the cloud supply chain, we identify a need to discover members of the supply chain, particularly the first tier suppliers, as part of determining the probable source of cyber risk to the cloud service. Likewise, we identify a requirement to model cloud risks quantitatively, using mathematical simulations which according to Burtescu [28] is suited to events that are uncertain over time. Combining this model with a decision support tool would make it applicable to scenarios in which the perception of an event is different from one individual to another.

3 The Cloud Supply Chain

Cloud supply chain can be defined as a complex system of two or more parties that work together to provide, develop, host, manage, monitor or use cloud services; with each facing internal and external risk factors and influences that make it uncertain whether and when they will achieve their cloud service objectives. The term 'cloud supply chain' was coined out of more traditional terms such as IT supply chain and cyber supply chain. Lindner et al. reckon the application of supply chain concept to cloud computing to be innovative and suggest the possibility of a new research field [52]. They proceed to define cloud supply chain as two or more parties linked by the provision of cloud services, related information and funds. The cloud supply chain is an end-to-end process, that is not limited to the delivery of services but includes other aspects such as market mediation, security, billing, legal, performance monitoring, accountability and QoS [60][52][74][73]. Organisations that provide or use cloud services operate in a complex dynamic environment, involving multiple supply chains, and need to feel confident that providers further down that chain are accountable for how they manage personal and confidential data [31]. All actors within the cloud supply chain exchange services for money and add value to other actors' offering through the refinement of services that ultimately fulfil customer needs [50].

Cloud computing signals the move of an organisation's IT system from an integrated supply chain to a dynamic one. Cloud computing transforms the traditional hardware-based outsourcing of data centres and the delivery of software products off-the-shelf to 'as-a-service' products (IaaS and SaaS respectively) [50]. The supply chain of such offering is inherently complex and consists of globally-distributed and dynamic collections of people, process and technologies [59]. The automated provisioning of cloud resources makes it difficult for consumers to identify the physical location of their data. Due to the dynamism of the cloud supply chain, it is unpredictable and highly volatile [52], but some of these concerns can be neutralised by the flexibility of a resilient architecture [70][25]. Abbadi and Lyle identified the advantages of a dynamic cloud, such as resilience and scalability, but also acknowledge its introduction of new security, logging and auditing challenge [1]. Similarly, Pearson argues that a dynamic supply chain enables businesses to strike a balance between the opportunities that drive economic growth and the downside risks of disruptive events within the chain [61].

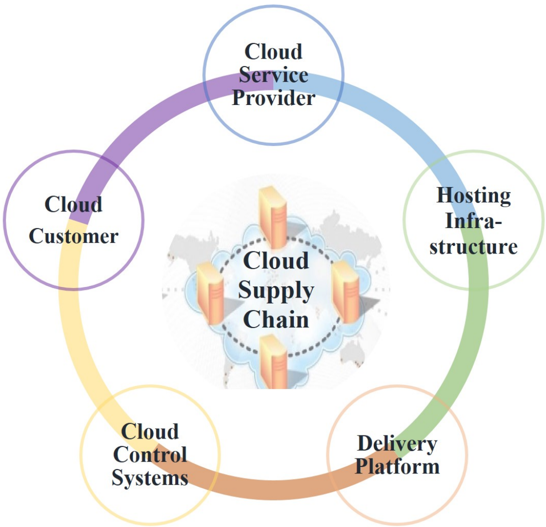

Figure 1: The Cloud Supply Chain

Boyson et al. [16], define cyber supply chain as 'the entire set of key actors involved with/using cyber infrastructure: system end-users, policy-makers, acquisition specialists, system integrators, network providers, and software/hardware suppliers'. Taking a cue from the definition, we briefly describe how the main actors involved in the delivery of a cloud service perform their role in what we termed the 'five cloud computing supply chain elements', as shown in Figure 1

The five key elements of a cloud supply chain can be listed as follows:

1. **Cloud Service Provider (CSP):** The CSP is the entity directly responsible for making a cloud service available to the customer. The CSP is defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as a thrid-party vendor that provides application delivery, monitoring, hosting and other services through cloud computing [20]. The CSP is the first tier of the supply chain and is directly responsible for the provision of adequate SLA

level protection, compliance, data privacy, security, etc. for the cloud service. Cloud computing technologies rely on an agile model, which puts an added responsibility on CSPs to manage the dynamic supply chain [61]. However, the security responsibility of data hosted in the cloud is shared between the CSP and the cloud customer, but the ability for cloud customers to carry out their allocated responsibility is often hampered by a seeming lack of the CSP's transparency, especially around the visibility of currently implemented security controls [64][65][6]. Examples of CSPs are Amazon and Salesforce.

2. **Hosting Infrastructure:** The hosting infrastructure for the cloud includes the physical resources (servers, routers, firewalls, power, and cooling systems), infrastructure, and platform layers of the cloud architecture together with their associated technologies [77]. A cloud provider's approach to managing hosting infrastructures depends on their service or deployment model. For example, the IaaS provider will be required to decide on the server manufacturer, Internet Service Provider (ISP), Application Programming Interface (API) provider, and web platform solution, that meet their cloud needs, while the SaaS provider relies on an already coupled service from a PaaS or IaaS provider. Popular hosting infrastructure providers are Softlayer (a core of the IBM cloud) and Rackspace.

3. **Delivery Platform:** Cloud services are accessed through a myriad of devices including servers, desktops, laptops and mobile devices. Consumer services hosted in the cloud are mainly web-based, requiring no prior installations. Cloud services, particularly SaaS applications accessible via mobile devices, access back-end systems via APIs, making them prime targets for malicious attacks [2]. According to Belmans and Lambrette [10], the increase in demand for mobile applications has accelerated SaaS adoption, a development which Charney and Werner [21] suggests has mitigated some risks and introduced or compounded others. The increased numbers of parties, devices and applications involved in cloud service delivery, lead to an increase in attack surface and consequentially a higher threat of data compromise [78].

4. **Control Systems:** With the dynamic supply chain of cloud applications, there is a high tendency for the various moving parts involved in the delivery of the cloud service to spiral out of the provider's control. CSPs require a robust framework to verify their applications' security properties, backup, access control, monitoring and forecast demand. Establishing a proactive monitoring system often can help to identify a disruption before its cause is apparent [70]. Likewise, implementing security controls, such as firewalls and intrusion detection systems (IDS) help CSPs to protect customer data. Some of the control systems need to be provided by the focal CSP, while others are the responsibility of other third parties within the supply chain, but in all situations, the focal CSP needs to demand visibility to ensure compliance with customer requirements. A useful list of control systems required for the proper functioning of a cloud service includes vulnerability management, logging, audit, identification and authentication, access control, encryption, continuity and incident management [7].

5. **Cloud Customer:** According to Felici et al. [31], a cloud customer (individual/firm) is an entity that maintains a business relationship with and uses the services of a cloud provider. An individual cloud customer, in most cases, doubles up as the end-consumer or the cloud subject, while an organisational cloud customer could range from a cloud broker, cloud aggregator, or the end-user organisation. A cloud broker interfaces between the cloud service provider and the consumer, translating user requirements to appropriate cloud offerings [47]. Cloud aggregators like brokers combine a large number of small and modular services to present to customers as a value-added service tailored to consumer needs [13]. However, contrary to the traditional description of cloud providers, Bohm and Riedl [13] argue that there are only a few cloud providers while all others are brokers, who buy network capacity and resell it under the 'cloud provider' label. Similarly, Kushida et al. [49], maintain that datacentre outsourcing or owning a single datacentre does not make an organisation a cloud provider, but that the real power of the cloud is in its dynamic allocation of resources and the 'illusion' of infinite scale.

An important theme that emerged from the above description of the cloud supply chain is that the cloud consumer is the starting point of a service request and the endpoint of a service delivery. The customer eventually pays all value-adding activities within the cloud supply chain. With most cloud products available from different value networks, the loyalty of customers, providers and suppliers to one another would seem to be constantly in doubt. Cloud customers look to change providers, particularly after an outage to avoid a repeat situation.

Also, seeing that each member of the supply chain faces an ever-changing list of security threats, it is challenging for focal CSPs to provide security assurances.

3.1 A Novel Cloud Risk Assessment Model – CSCCRA

Reflecting on the gaps identified in our literature review, and building on our knowledge of the dynamic cloud supply chain, we propose the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, as shown in Figure 2. The CSCCRA model is the combination of a quantitative risk assessment method, decision support analysis, and supply chain mapping. The model looks to address the gap on how the lack of supply chain transparency and limited visibility of third-party vendors' security controls have contributed to the inadequate level of cloud risk assessment. Knowing that this can be a difficult undertaking, not least because of the unpredictable and chaotic cloud supply chain, we adopt the systems thinking approach to solving complex system problems as suggested by Ghadge et al. [33]. This method requires us to conceptualise and analyse the interdependencies of a cloud service during risk assessment while making use of modelling and simulation techniques to draw the result of the assessment. The CSCCRA model takes a cue from standards and guidance documents such as ISO 27005:2011 [42], ISO 31000:2009 [41], NIST 800-30v1 [66], and FAIR risk assessment [32]. The three main components of the CSCCRA model are as follows:

1. **Quantitative Risk Assessment:** The CSCCRA model goes beyond the IT industry norm to apply a quantitative assessment method to cloud risks for at least three reasons. First, the ability to express risks as the combination of the probability of an event and its consequences as per ISO Guide 73:2009 [28]. Second, the rigorous process that goes into the determination of risk factors [40], and third, its potential for increased objectivity through the use of controlled experimentation [32]. With uncertainty being the primary factor in risk analysis, the CSCCRA model makes use of a probabilistic estimate of risk factors, e.g. threat frequency, vulnerability and loss magnitude, representing the estimates as a distribution (e.g. PERT, Poisson), and inputting the values into a Monte Carlo simulation engine.

2. **Decision Support Analysis (Supplier Rating):** As a CSP-targeted solution, the CSCCRA model requires the cloud providers to be aware of their cloud service supply chain and have sufficient information about the processes, capabilities and offerings of their partners. We introduced decision support analysis to cloud risk assessment to address the notion of a distorted and incomplete process involved in cloud supplier selection. The decision support analysis involves decomposing the cloud service into its component objects and using a multi-criteria decision tool, rate all entities based on their observed behaviours, to identify weak suppliers easily susceptible to cyberattack or those with a high risk of failure. According to Ghadge et al. [33], identifying the potential weak spots in the supply chain through a dynamic model helps to capture its vulnerability and promote proactive mitigation of risks. The CSCCRA makes use of an improper linear model for decision analysis, helping CSPs to consider areas where the chain is weakest during risk factor estimation.

3. **Supply Chain Mapping:** Providing end-to-end supply chain visualisation while assessing cloud risk makes it amenable to analyse and explore areas of weakness, strengths and the potential risks to a cloud service while also supporting collaboration and decision-making within the chain [71]. Visualising the information flow of a cloud service through the supply chain helps to identify critical suppliers and single points of failure (SPOF) within the chain. The benefit of a graphical representation of the inherent risk in the supply chain helps to counter any documented biases in risk estimation and decision-making and is thought to have an impact in reducing the cognitive load involved in the evaluation of risk factors [34]. The CSCCRA model employs supply chain mapping during the decision support analysis stage of the risk assessment, to allow for continuous monitoring and visibility of the current state of cloud risk, and to enable a data-driven risk estimation, not one based on instinct.

4 Cloud Risk Assessment Survey

4.1 Survey Methodology

This survey was approved by the University of Oxford's Central Research Ethics Committee, under Ref No: R50232/RE001. The survey instrument was designed to be self-administered and was built using the Bristol Online Survey (BOS) tool [14]. The welcome page contained a brief introduction to the research, survey goals and the anonymity of data provided. We kept the survey anonymous to allow for an open and honest response from the respondents.

Four fundamental goals drove the collection and analysis of the survey data, and they are as follows:

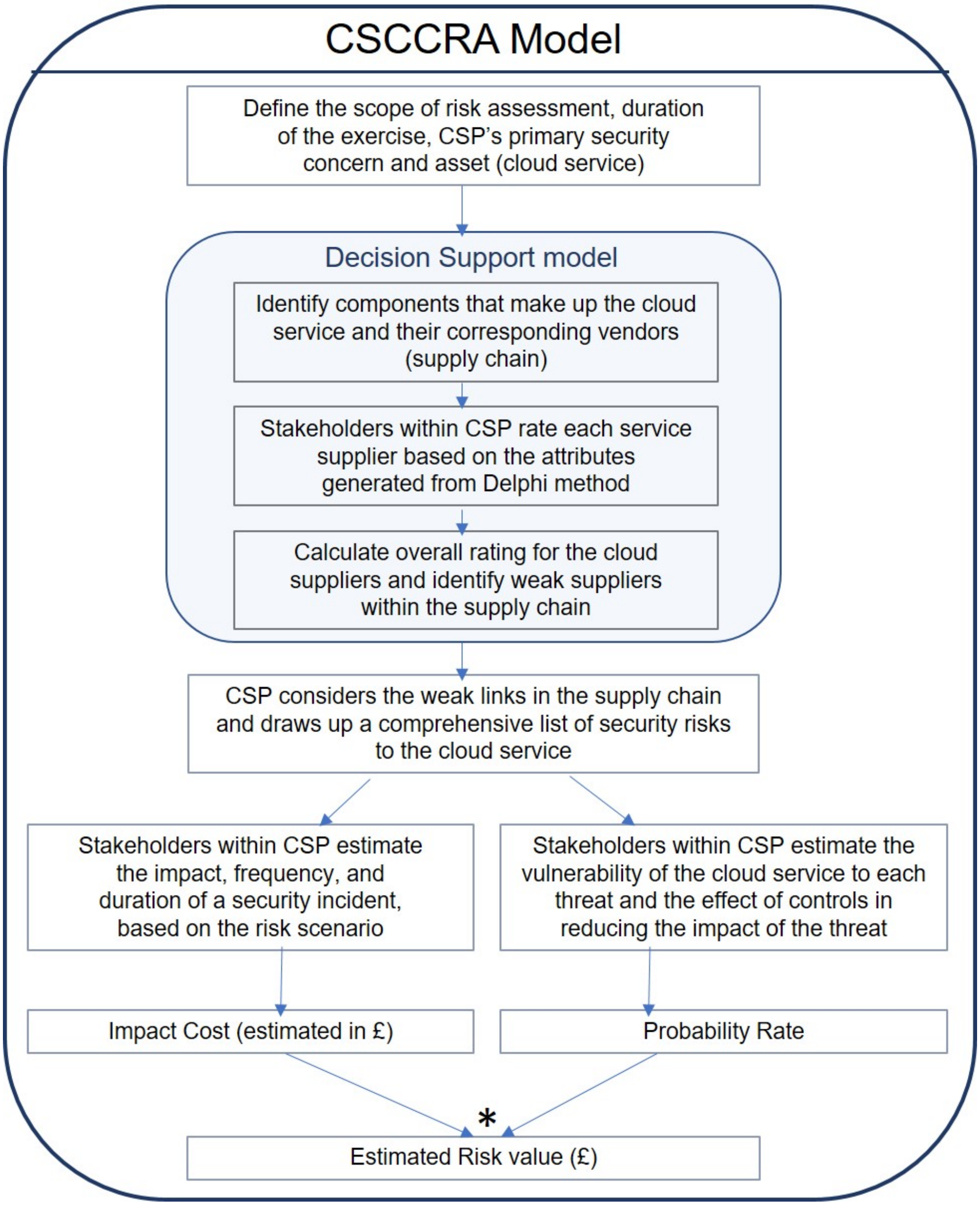
CSCCRA Model
Define the scope of risk assessment, duration of the exercise, CSP's primary security concern and asset (cloud service)
Decision Support model
Identify components that make up the cloud service and their corresponding vendors (supply chain)
Stakeholders within CSP rate each service supplier based on the attributes generated from Delphi method
Calculate overall rating for the cloud suppliers and identify weak suppliers within the supply chain
CSP considers the weak links in the supply chain and draws up a comprehensive list of security risks to the cloud service
Stakeholders within CSP estimate the impact, frequency, and duration of a security incident, based on the risk scenario
Stakeholders within CSP estimate the vulnerability of the cloud service to each threat and the effect of controls in reducing the impact of the threat
Impact Cost (estimated in £)
Probability Rate
*
Estimated Risk value (£)

Figure 2: The Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model

1. To understand the level of awareness cloud stakeholders have about supply chain risks.
2. To capture the decision-making process involved in cloud supplier selection.
3. To identify conventional risk identification/assessment methodologies employed within cloud provider and consumer environments.
4. To identify factors that contribute to the supply chain risks in cloud computing.

We administered the survey to a convenient sample of cloud stakeholders, considered to be experts, with information on how organisations approach cloud risks and the effect of the supply chain. These participants were recruited within the UK, mainly through the distribution of a survey recruitment calling cards during cloud conferences, and through collaborations with the Cloud Industry Forum (CIF) and the London Chapter of Information Systems Audit and Control Association (ISACA). The survey instrument [3] was administered to respondents between March and July 2017.

Because of the heterogeneous way in which firms perceive and manage risk, and the limited nature of the sample, the analysis of the survey is at this stage only descriptive. However, it does provide some insight into the range of approaches taken by firms.

4.2 Survey Result and Discussion

After careful analysis of the survey data, a total of sixty-two (62) respondents completed the questionnaire. The analysis of the data confirmed there was no missing information in these responses, as the Boston Online Survey (BOS) tool was designed not to proceed to the next page in cases where mandatory questions were left unanswered. The data that makes up the final dataset in this analysis is made up of fully completed forms. The frequency table, Table 1, shows a summary of the demography.

Having established the quality of the participants, we begin our analysis with the response of the cloud providers, followed by that of cloud customers, and conclude with the analysis of the general questions posed to all respondents.

4.2.1 Cloud Providers

A combined total of 22 cloud providers responded to the survey. The service provided by each of the respondents ranged from cloud security, email, monitoring, storage, Runtime/API, customer relationship management (CRM) and financial services. When asked if the respondents carried out a comprehensive risk assessment, the majority of the respondents answered yes, except for three participants. Sixteen providers estimated the level of comprehensiveness for their risk assessment to be in the region of 71% to 100%, while four rated themselves between 51-70%, and the remaining two were between 20-50%. The response of the participants to why they conducted risk assessment was not surprising, with the assurance of the security triad (availability, confidentiality and integrity) their top priority. Other suggestions including the identification of weak links in the supply chain, improved decision-making or better understanding of risk were lower on their priority list. Interestingly, we observed that on average each of the cloud providers relied on at least eight other suppliers for the delivery of their service.

While considering if the risk assessment process of cloud providers took into account supply chain risks, we asked the respondents to answer the question as “yes”, “partially” or “no”, and provide a percentage estimate. Their response showed that 18 of the 22 cloud providers somewhat considered their supply chain risks with varying degrees, while four did not consider supply chain risks at all. With the majority of the responses being positive, this feedback somewhat negates their response to the reasons for carrying out a risk assessment, where its use for monitoring weak links in the supply chain had a low response rate. However, in answer to the question on transparency with customers about their dependence on external providers, all but four cloud provider respondents, reported that they were transparent. Although we recall a recent outage of a major cloud provider that impacted the services of an anti-virus (AV) provider, alerting the AV provider and their consumers to their dependence on the cloud giant. So, the fact that over 80% of the cloud providers in this sample provide supply chain information up front does not necessarily guarantee that the information provided met the three criteria for transparent information identified by Hofstede [39], which are: (a) quality of data; (b) quality of format; and (c) quality of meaning.

In response to the question seeking to find out the three most important criteria cloud providers consider when choosing partners, the top three answers were: i) security of the cloud service ii) reputation of the vendor; iii) functionality of the service, see Figure 3. Also on the subject of the transparency of supply chain and its impact on risk assessment, the providers corroborated the results of our earlier research, acknowledging many of the identified transparency features [4] as essential components of a comprehensive risk assessment. When participants were asked for the largest risk to their cloud services, they listed several risks including human error, the introduction of new cloud feature, zero-day

Table 1: Relevant demographic and cloud computing data from respondents (N = 62)

Demographics		Frequency	%
Principal Industry	Manufacturing	1	1.61%
	Transportation	2	3.23%
	Government	3	4.84%
	Education / Research	4	6.45%
	Other (Media, trade, construction)	10	16.13%
	Finance (Banking, Insurance, etc.)	12	19.35%
	Information Technology/ Telecommunications	30	48.39%
Sector	Private	54	87.10%
	Public	8	12.90%
Company size	1 - 9	12	19.35%
	10 - 50	5	8.06%
	51 - 250	6	9.68%
	251 - 500	5	8.06%
	501 - 1000	6	9.68%
	1000+	28	45.16%
Cloud service model	IaaS	28	45.16%
	PaaS	12	19.35%
	SaaS	22	35.48%
Cloud role	Cloud Consumer (CC)	40	64.52%
	Infrastructure Provider (IP)	4	6.45%
	Cloud Service Provider (CSP)	12	19.35%
	Application Service Provider (ASP)	6	9.68%

attacks, data breaches, web application vulnerability, supplier change control, but the top on the list was the unavailability of the service.

With regards to their risk assessment process, ten cloud providers attested to carrying out a continuous risk assessment of their cloud service, two (monthly), while four each (quarterly and yearly), and the last two only after a security incident. According to Boyens et al. [15], the dynamic nature of the cloud calls for a continuous risk assessment, because while the current ‘check-box’ type risk evaluation system is good for regulatory compliance or adherence to standards, it is inadequate for the accelerated growth of cloud computing [43]. With regards to risk analysis methodology, 17 cloud providers indicated that they used both qualitative and quantitative methods, while five others opted for the qualitative approach. The follow-on question which asked for the specific risk assessment method highlighted the widespread use of qualitative methods, including weighted scoring and risk matrices which are considered ‘weak’ quantitative methods. According to Hubbard and Seiersen [40], one of the errors of assessing risk using a risk matrix is that of range compression, where a higher risk cell could contain a lower in comparison to another in a lower risk cell. As Figure 4 shows, only two provider respondents confirmed their use of a mathematical simulation.

As Figure 4 indicates, the quantitative risk assessment methodologies are not common within the cloud industry, despite their obvious benefits, including their ability to maintain internal and external consistency with the meanings and proportionality of the values used for risk estimation. We made this observation also as part of our literature review, so to further establish our findings, we asked cloud providers how the value of risk was expressed within their organisation. Sixteen of those surveyed responded that they used impact/likelihood rating, nine represented risk using its monetary value, five used probability distributions and three expressed risk value using time. In [32], Freund and Jones described one of the advantages of using quantitative over qualitative methods to be its ability to decompose

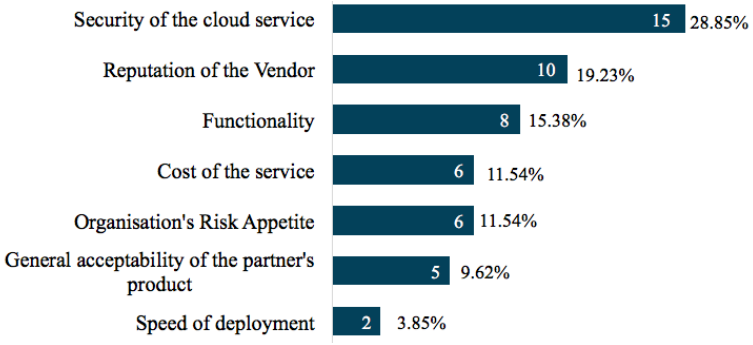

Figure 3: Three most important criteria providers consider when choosing suppliers

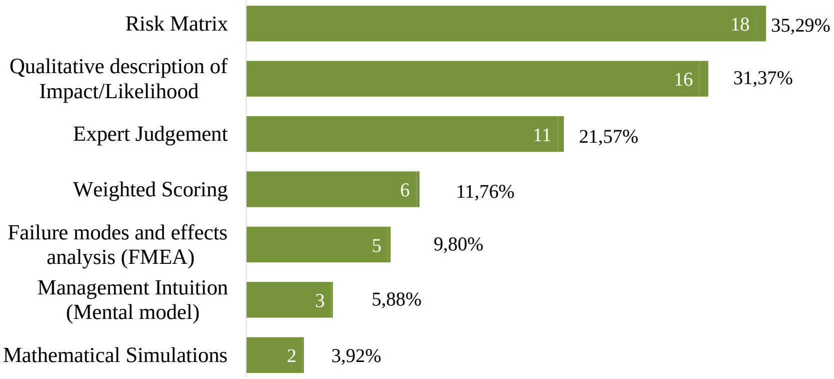

Figure 4: Risk assessment methods most commonly used within provider organisations

the relevant risk loss scenarios. Such rigour does not seem to apply to the subjective selection of impact and likelihood ratings, further disqualifying the application of qualitative risk assessment in assessing the risk of the dynamic cloud supply chain.

4.2.2 Cloud Customers

A total of 40 cloud consumers responded to the survey, each of whom are subscribers of at least one SaaS application. Of the 40 cloud customer respondents, 15 were from SMEs (1-250 employees), and 25 were from larger organisations. On the subject of the comprehensiveness of cloud risk assessment, 34 of the respondents indicated they followed a thorough process. Also, 19 respondents confirmed to accounting for their provider's supply chain risks in their risk assessment, while 15 partially considered their supply chain, leaving six respondents who did not consider supply chain risks. It is however not clear to what extent the provider supply chain risks were accounted for since it requires having knowledge of third parties and the impact these suppliers could have on the cloud service. Following careful analysis of the respondents who claimed to account for their providers' supply chain in their risk assessments, 25 of them were consumers of email and productivity tools from cloud giants such as Microsoft and Google. On the face of it, it is possible that these respondents erroneously believe their cloud providers are the only member of their supply chain, which is rarely the case. That said, a minor difference between the provider and consumer responses came when we asked the consumer respondents the important reasons for carrying out a cloud risk assessment. Their top three options for conducting risk assessments were: i) ensuring confidentiality of the cloud service (34), ii) ensuring availability of the cloud service (30), iii) better understanding of risk (28), see Figure 5 for more information.

There was a positive correlation between the provider and consumer responses on the need to have relevant supply chain information to conduct a comprehensive cloud risk assessment. Nevertheless, a more significant concern for cloud customers was the possibility of their provider going out of business or being locked-in to a long-term contract. On the subject of risk analysis methodology, 19 cloud consumer respondents used both quantitative and qualitative models, while 14 used only qualitative, with the last seven respondents using neither of the methods, preferring to use expert judgements on

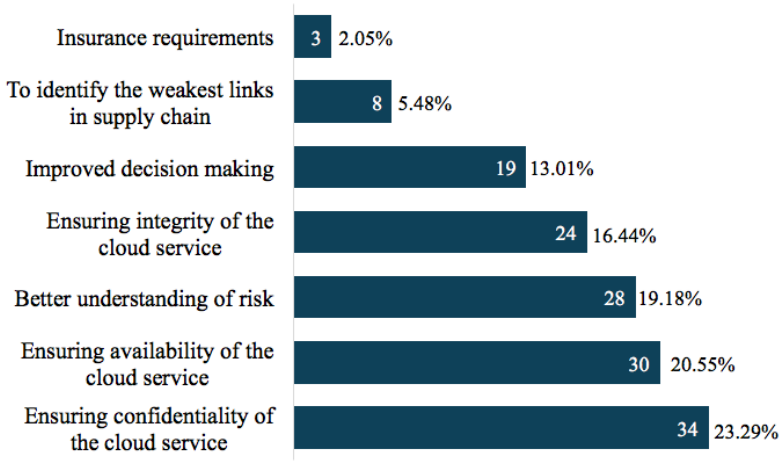

Figure 5: Cloud consumers' most important reasons for carrying out cloud risk assessment

a 'need-to' basis. Similar to cloud providers, the use of risk assessment as a decision-making support tool was common also to cloud consumer organisations, and their most common method was also the **qualitative description of impact/likelihood**, selected by 34 of the 40 respondents. This method seems to be popular across the IT industry, together with other techniques such as the risk matrices (28 of 40) and expert judgement (22 of 40), see figure 6. None of the consumers surveyed used mathematical simulations, which was not shocking, considering the arguments of Freund and Jones [32] and Power [63], on how the bias of regulatory organisations like the National Institute of Standards and Technology (NIST) and COSO against quantitative risk assessment, influenced the use of more qualitative assessment methods within the IT industry.

As a final question to the cloud consumer respondents, we asked if in the last year they have had a supply chain related security incident, which was not a direct responsibility of their focal cloud provider, and nine of the consumer respondents answered in the affirmative. Of the nine responses, four had an availability related events, two were privacy-related, and the others were the loss of confidentiality and authentication issues. With this in mind, some of the countermeasures cloud consumer respondents listed as being in operation within their organisation, are tabulated verbatim in Table 2.

4.2.3 General Questions

In the concluding section of the survey, the combined group of respondents (62), were presented with a set of general risk and supply chain related questions to validate some of the knowledge we acquired from our review of the literature. The first general question required respondents to select what they believe constituted the top four hindrances to a more comprehensive cloud risk assessment, from a list of seven options, as seen in Figure 7. While we were not surprised with the choices of the respondents, their emphasis on the need for transparency in cloud computing is in agreement with our earlier work and also the study of [20], which established the extent to which cloud transparency could help to reduce the risk of cloud adoption. With cloud computing's survival based on a dynamic and complex supply chain, we argue that the transparency of cloud providers by way of providing reasonable visibility of controls and processes promotes better risk assessment. Also, we observed that some of the respondents raised the topic of cost and limited training, two factors often cited when SMEs are asked to conduct a quantitative risk assessment. One of the respondents in contributing to the list of hindrances to a comprehensive risk assessment noted the *"lack of awareness amongst suppliers about security risks and how to protect against them"*. The respondent stressed that the *"security standards in the cloud industry were too low"*. Another respondent also identified the hindrance of limited resources, saying *"there is a shortage of qualified experts to perform comprehensive risk assessment"*. Some of the other barriers named include *"Lack of adherence of cloud suppliers to assurance standards (e.g., CSA STAR programme)"* and *"the poor response rate of large CSPs to due diligence requests"*.

The next question we posed to the respondents was aimed at finding out their security priorities and in what order they were worried about the confidentiality, integrity and availability of their cloud service. Table 3 presents a breakdown of their responses. From Table 3, we can see that both providers and consumers prioritised

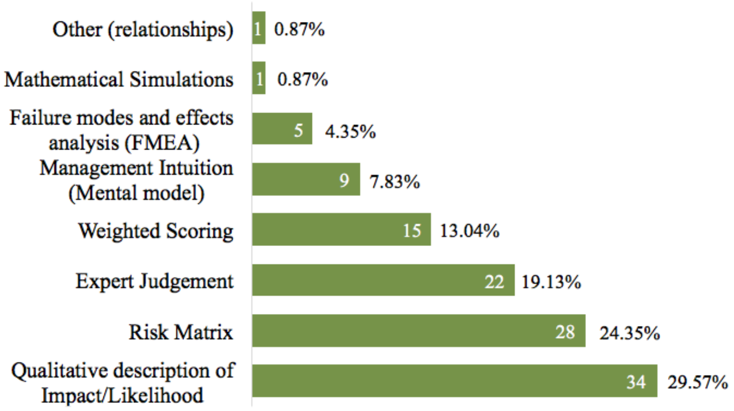

Figure 6: Cloud consumers' most commonly used risk assessment method for decision making

Table 2: Cloud consumer's threat mitigation

No.	Countermeasures for mitigating cloud threats
1	Comprehensive contract management and an exit clause/strategy
2	Detailed Auditing and Logging to identify baseline to know what normal traffic looks like and identify malicious behaviour
3	Encryption of sensitive data transmitted to provider
4	Due diligence in supplier selection at the time of new/incremental business award should identify the risks associated with potential suppliers and eliminate any where the risk is too high
5	Ensuring that credentials are not stored in an insecure manner
6	Backup, Redundancy and Up-to-date business continuity plans
7	Active Directory federation. Firewalls, Data Loss Protection
8	Local software capability to provide off-line services
9	Private Virtual Networks, Identity federation, encryption at rest and in transit, multi site hosting, DNS
10	E-mail continuity solution and Cloud Access Security Broker (CASB)
11	Monitoring of supplier compliance with security and data protection requirements specified in the contract
12	Use of strong password policies

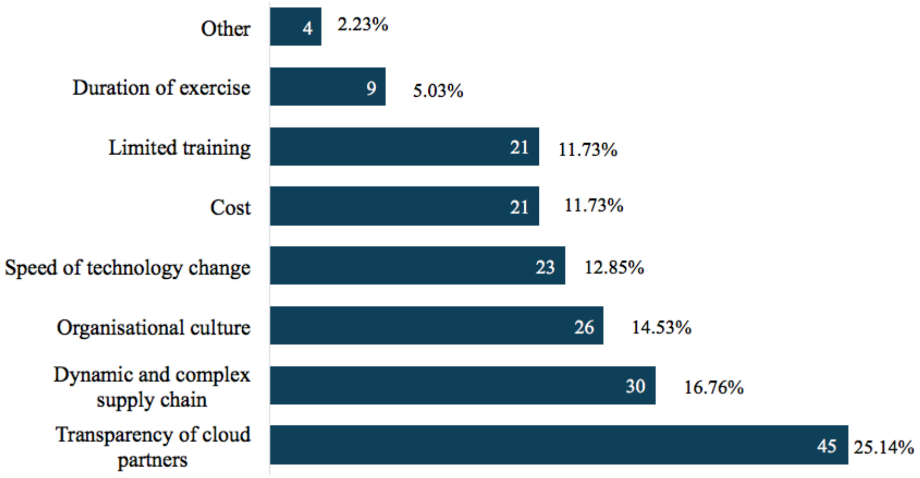

Figure 7: Hindrances to a more comprehensive risk assessment

Table 3: Security triad (CIA) order in which cloud stakeholders are worried about their cloud supply chain

Class	Security Concern	Order	Count
CP	Loss of Confidentiality	Low	6
CP	Loss of Confidentiality	Medium	6
CP	Loss of Confidentiality	High	10
CP	Loss of Integrity	Low	6
CP	Loss of Integrity	Medium	12
CP	Loss of Integrity	High	4
CP	Loss of Availability	Low	10
CP	Loss of Availability	Medium	4
CP	Loss of Availability	High	8
CC	Loss of Confidentiality	Low	6
CC	Loss of Confidentiality	Medium	8
CC	Loss of Confidentiality	High	26
CC	Loss of Integrity	Low	19
CC	Loss of Integrity	Medium	19
CC	Loss of Integrity	High	2
CC	Loss of Availability	Low	15
CC	Loss of Availability	Medium	12
CC	Loss of Availability	High	12

the availability and confidentiality of data over the integrity. This might be because they have solutions in place that can detect message integrity, solutions such as end-to-end data protection, and metadata checksumming. Nonetheless, the analysis of the result would seem to suggest that the loss of integrity is a medium priority for both cloud provider and customer organisations. Lastly, seeing that the CSA top 12 treacherous threats [37] was the result of a survey that compiled industry experts opinion on cloud threats, we decided to confirm which of the threats our respondents thought were supply chain related.

Our motivation is to have a validated reference guide for supply chain-related cloud security threats since the CSA survey is widely regarded as the most authoritative and up-to-date cloud survey. As shown in Figure 8, the respondents opined that the 12 threats are supply chain related, with varying level of popularity. This observation follows an earlier established claim by NIST [15], who suggested that the ICT supply chain threat agents are similar to the information security threats agents, citing insiders and cybercriminals as examples. The threats that many of those surveyed agreed on, include: data breaches, insecure interfaces and API, system vulnerabilities, malicious insiders, data loss, insufficient due diligence, Denial of Service(DoS) and shared technology vulnerabilities. Unsurprisingly, these were the threats we hypothesised to be supply chain related at the initial stage of our research, although we added insufficient IAM and, abuse and nefarious use of cloud services, which from Figure 8 have at least 19 of the 62 respondents agreeing with this choice. We hope to use this list of threats as potential causes of supply chain risks during the risk modelling stages of our risk assessment.

4.2.4 Summary

Together these results provide valuable insights into the level of awareness cloud stakeholders have on supply chain risks, cloud risk assessment and other cloud decision-making processes. The results broadly speak for themselves. Although there seems to be a good awareness of supply chain risk among cloud stakeholders, their approach to assessing the risk cannot be said to be keeping up with the dynamic growth of cloud computing. Conducting risk assessments on a yearly basis gives organisations a false sense of security, while the use of qualitative methods for risk assessment is not considered to be rigorous enough to help decompose and model cloud risks appropriately. Furthermore, there remains the all-important issue of cloud transparency, which as we have seen is a major component of cloud risk assessment.

One concern expressed regarding risk assessment, in general, was the challenge of small enterprises to conduct cloud risk assessment. These companies who usually do not have a dedicated IT team nor individuals with the specialised skill for IT risk assessment seem to rely on their cloud provider to take care of their valuable assets. In providing a final comment on the survey, one of the respondents said *'As a small*

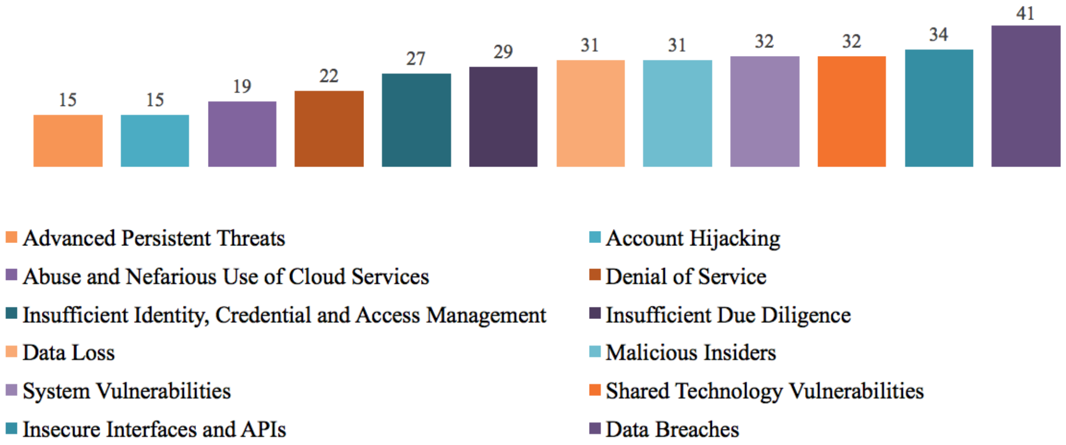

Figure 8: CSA's top 12 cloud computing threats that are supply chain related

company it is challenging to identify appropriate risk assessment due to lack of specialist staff. This means we are highly reliant on our cloud service provider to manage risk issues downstream and rely on our SLA for commercial management of our contractual expectations of service'. Perhaps, a good suggestion would be for cloud customers to trust but verify that their confidence in the cloud provider is not misplaced, which is only possible through a transparent supply chain.

5 Conclusions and Future Work

In this study, we set out to describe the supply chain of a cloud service and examine how acknowledging the inherent risk within the supply chain could bridge the risk assessment gap. The survey results showed a widespread use of qualitative risk assessment methods and identified the lack of cloud provider transparency as the top hindrance to a comprehensive risk assessment. Many of those surveyed had a good awareness of supply chain risks, and a majority of the respondents even confirmed that most of the Cloud Security Alliances top 12 treacherous threats had its origin in the supply chain. Nonetheless, awareness alone is not sufficient for the survival of the cloud, which is reliant on a dynamic, complex and often opaque supply chain. Therefore, the ability of cloud providers to provide reasonable visibility of controls and processes both of themselves and their third parties will contribute to the improvement of cloud risk assessment.

Despite its exploratory nature, the evidence from this study suggests that the current approach to cloud risk assessment is unable to address the cloud risks. Furthermore, with an apparent lack of trust in cloud providers, cloud customers who set out to conduct risk assessments for decision-making, are constrained to carrying out qualitative and subjective assessments due to the limited transparency. While this study did not confirm if quantitative risk assessment would provide better results, it did partially substantiate the need for more rigour in cloud risk assessments and provide evidence on how this can be improved with supply chain transparency.

Therefore, to bridge the cloud risk assessment gap, we proposed the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model. The CSCCRA model which is currently being targeted at cloud providers would require each CSP to be aware of the logical and physical dependencies they have on their supply chain. The proposed model will combine quantitative risk assessment, decision analysis and supply chain mapping to provide a more iterative, incremental and inclusive approach to risk assessment. The model provides stakeholders with a unique capability for capturing the dynamic behaviour of risks within a cloud supply chain and objectively measure the overall risk value of the cloud service. The structured and systematic approach to the model would also aid decision makers in understanding their current security posture, how much security is required and why, increase the assurance on the effectiveness of security investments, and identify weak spots in the current supply chain.

Future research will focus on developing the model into a cloud risk assessment tool. The decision support and mapping tool will help address the problem of weak links in a supply chain, by identifying suppliers with an inadequate security posture, while the quantitative risk assessment model will make use of stochastic modelling to reduce the level of uncertainty and subjectivity in the cloud risk evaluation process. We aim to present the value of a risk as a dollar value and express the rate of risk occurrence or its impact as a probabilistic range. Once the system is developed and validated by academic and industry experts, we will look to verify its effectiveness by conducting real-world case studies with cloud providers. We hypothesise that the rigour involved in the risk assessment process would improve its accuracy and provide decision-makers with a clearer picture of their cloud risks.

ACKNOWLEDGMENTS

Olusola Akinrolabu's research is funded by EPSRC via the Centre for Doctoral Training in Cyber Security at the University of Oxford. The authors would like to thank the management of the Cloud Industry Forum and the London Chapter of ISACA for their help with sending the survey to their members. Also, we appreciate the assistance of the anonymous reviewers for their helpful and constructive comments.

REFERENCES

[1] I. Abbadi and J. Lyle, "Challenges for provenance in cloud computing," *USENIX Work. Theory Pract. Proven. (TaPP'11).*, 2011.

[2] Akana, "Api security: A guide to securing your digital channels api security," 2015. [Online]. Available: https://www.roguewave.com/resources/white-papers/api-security-guide-to-securing-digital-channels

[3] O. Akinrolabu, "Survey - supply chain cyber risks in cloud computing: The effect of transparency on risk assessment," 2017. [Online]. Available: https://oxford.onlinesurveys.ac.uk/supply-chain-cyber-risks-in-cloud-computing

[4] O. Akinrolabu and S. New, "Can improved transparency reduce supply chain risks in cloud computing?" *Operations and Supply Chain Management*, vol. 10, no. 3, pp. 130–140, 2017.

[5] F. M. Alturkistani and A. Z. Emam, *A Review of Security Risk Assessment Methods in Cloud Computing*. Springer International Publishing, 2014, pp. 443–453.

[6] Amazon Web Services Inc., "Amazon web services: Overview of security processes," August 2015. [Online]. Available: http://aws.amazon.com/security

[7] M. Auty, S. Creese, M. Goldsmith, and P. Hopkins, "Inadequacies of current risk controls for the cloud," *The 2nd IEEE Int. Conf. Cloud Comput. Technol. Sci.*, pp. 659–666, 2010.

[8] L. Badger, R. Patt-corner, and J. Voas, "Cloud computing synopsis and recommendations recommendations of the national institute of standards and technology," *Nist Spec. Publ.*, vol. 800, no. 146, p. 81, 2012.

[9] M. A. Bashir and N. Christin, "Three case studies in quantitative information risk analysis," *Proc. CERT/SEI Bus. Case Work. Mak. Bus. Case Softw. Assur.*, pp. 77–86, 2008.

[10] W. Belmans and U. Lambrette, "The cloud value chain exposed key takeaways for network service providers," *CISCO*, 2012. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/sp/Cloud-Value-Chain-ExposedL.pdf

[11] A. Bicaku, M. Tauber, S. Maksuti, and C. Wagner, "Seccrit - secure cloud computing for critical infrastructure it," *SECCRIT*, 2014. [Online]. Available: https://www.seccrit.eu/

[12] S. Bleikertz, T. Mastelić, W. Pieters, S. Pape, and T. Dimkov, "Defining the cloud battlefield: Supporting security assessments by cloud customers," *Proceedings of the IEEE International Conference on Cloud Engineering*, pp. 78–87, 2013.

[13] M. Böhm and C. Riedl, "Towards a cloud computing value network," *GI Jahrestagung Informatik*, pp. 129–140, 2010.

[14] BOS, "BOS online survey tool," 2017. [Online]. Available: https://www.onlinesurveys.ac.uk/

[15] J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, "Supply chain risk management practices for federal information systems and organizations," *NIST Spec. Publ.*, 2015.

[16] S. Boyson, "Building a cyber supply chain assurance reference model," *Supply Chain Manag.*, vol. 1, no. June, pp. 1–64, 2009.

[17] S. Boyson, "Cyber supply chain risk management," *Revolutionizing Strateg. Control Crit. IT Syst.*, vol. 34, no. 7, pp. 342–353, 2014.

[18] E. Cayirci, A. Garaga, A. S. De Oliveira, and Y. Roudier, "A cloud adoption risk assessment model," *IEEE/ACM 7th Int. Conf. Util. Cloud Comput.*, pp. 908–913, 2014.

[19] CERT-UK, "Cyber-security risks in the supply chain," 2015. [Online]. Available: https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf

[20] W. Chan, E. Leung, and H. Pili, "Enterprise risk management for cloud computing," *Comm. Spons. Organ. Treadw. Comm.*, 2012.

[21] S. Charney and E. T. Werner, "Cyber supply chain risk management : Toward a global vision of transparency and trust," 2011. [Online]. Available: http://download.microsoft.com/download/3/8/4/384483BA-B7B3-4F2F-9366-E83E4C7562D6/Cyber

[22] S. Chopra and M. S. Sodhi, "Managing risk to avoid supply-chain breakdown," *MIT Sloan Manag. Rev.*, vol. 46, no. 1, 2004.

[23] CISO Platform, "The notorious 9 in cloud security - ciso platform," 2014. [Online]. Available: http://www.cisoplatform.com/profiles/blogs/the-notorious-9-in-cloud-security

[24] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data protection-aware design for cloud services," *Proceedings of IEEE International Conference on Cloud Computing*, pp. 119–130, 2009.

[25] M. Dekker and G. Hogben, "Survey and analysis of security parameters in cloud SLAs across the European public sector," *ENISA*, pp. 1–36, 2011.

[26] K. Djemame, D. J. Armstrong, and M. Kiran, "A risk assessment framework and software toolkit for cloud service ecosystems," *Computing*, no. c, pp. 119–126, 2011.

[27] S. Drissi and S. Benhadou, "Evaluation of risk assessment methods regarding cloud computing," *The 5th Conference on Multidischiplinary Design Optimization and Applicaton*, no. June, 2016.

[28] Emil Burtescu, "Decision assistance in risk assessment - monte carlo simulations," *Informatica Economic*, vol. 16, no. 4, pp. 86–93, 2012.

[29] ENISA, "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools," June 2006. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/

[30] K. Fatema, V. C. Emeakaroha, P. D. Healy, J. P. Morrison, and T. Lynn, "A survey of cloud monitoring tools: Taxonomy, capabilities and objectives," *J. Parallel Distrib. Comput.*, vol. 74, no. 10, pp. 2918–2933, 2014.

[31] M. Felici, T. Koulouris, and S. Pearson, "Accountability for data governance in cloud ecosystems," *IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, pp. 327–332, 2013.

[32] J. Freund and J. Jones, *Measuring and Managing Information Risk*. Elsevier Inc., 2015.

[33] A. Ghadge, S. Dani, M. Chester, and R. Kalawsky, "A systems approach for modelling supply chain risks," *Supply Chain Manag. an Int. J.*, vol. 18, no. 5, pp. 523–538, 2013.

[34] D. Gresh, L. A. Deleris, L. Gasparini, and D. Evans, "Visualizing risk," in *Proceedings of IEEE Information Visualization Conference*, 2011, pp. 1–10.

[35] B. Groubauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," *Softw. Reuse Emerg. Cloud Comput. Era*, no. April, pp. 204–227, 2011.

[36] P. C. Group, "Security for industrial control systems- manage third party risks," *CPNI*, 2015.

[37] T. T. W. Group, "Cloud computing top threats in 2016 – treacherous 12," *Cloud Security Alliance (CSA)*, no. February, 2016.

[38] T. Haselmann, G. Vossen, and S. Dillon, "Cooperative hybrid cloud intermediaries - making cloud sourcing feasible for small and medium-sized enterprises," *Open Journal of Cloud Computing (OJCC)*, vol. 2, no. 2, pp. 4–20, 2015. [Online]. Available: http://nbn-resolving.de/urn:nbn:de:101:1-201705194494

[39] G. J. Hofstede, "Transparency in netchains," in *Proceedings of EFITA Conference*, July 2003, pp. 17–29.

[40] D. Hubbard and R. Seiersen, *How to measure anaything in cybersecurity risk*. John Wiley & Sons, 2016.

[41] International Standards Organisation, "ISO 31000 - Risk management," 2009. [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm

[42] International Standards Organisation, "BS ISO / IEC 27005 : 2011 BSI Standards Publication Information technology - Security techniques - Information security risk management," 2011. [Online]. Available: http://www.iso27001security.com/html/27005.html

[43] ISACA & CSA, "Cloud computing market maturity," *AN ISACA CLOUD Vis. Ser. WHITE Pap.*, 2015.

[44] U. M. Ismail, S. Islam, M. Ouedraogo, and E. Weippl, "A framework for security transparency in Cloud Computing," *Futur. Internet*, vol. 8, no. 1, pp. 1–22, 2016.

[45] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," *Director*, vol. 144, no. 7, pp. 800–144, 2011.

[46] M. Jenks, "Critical infrastructure protection supply chain risk management," *FERC Docket No. RM15-14-000*, pp. 1–6, 2016.

[47] E. Kamateri, N. Loutas, D. Zeginisis, and J. Ahtes, "Cloud4soa: A semantic-interoperability paas solution for multi-cloud platform management and portability," *ESOCC*, pp. 64–78, Sep. 2013.

[48] R. Ko, S. Lee, and V. Rajan, "Cloud computing vulnerability incidents: A statistical overview," *Cloud Security Alliance*, March 2013.

[49] K. E. Kushida, J. Murray, and J. Zysman, "Cloud computing: From scarcity to abundance," *J. Ind. Compet. Trade*, vol. 15, no. 1, pp. 5–19, 2015.

[50] S. Leimeister, C. Riedl, M. Böhm, and H. Krcmar, "The business perspective of cloud computing: Actors, roles, and value networks," *Proc. 18th Eur. Conf. Inf. Syst.*, pp. 1–12, 2010.

[51] R. Lewis, P. Louvieris, and P. Abbott, "Cybersecurity information sharing: a framework for information security," *Proceedings of Twenty Second Eur. Conf. Inf. Syst.*, pp. 1–15, 2014.

[52] M. Lindner, C. Chapman, S. Clayman, D. Henriksson, and E. Elmorth, "The cloud supply chain: A framework for information, monitoring, accounting and billing," *2nd Int. ICST Conf. Cloud Comput.*, 2010.

[53] P. Liu and D. Liu, "The new risk assessment model for information system in cloud computing environment," *Procedia Eng.*, vol. 15, pp. 3200–3204, 2011.

[54] J. Luna, N. Suri, M. Iorga, and A. Karmel, "Leveraging the potential of cloud security service-level agreements through standards," *IEEE Cloud Comput.*, vol. 2, no. 3, pp. 32–40, 2015.

[55] T. Marianthi, T. Nikolaos, and G. Dimitris, "In cloud we trust: Risk-assessment-as-a-service cloud computing: A security perspective," *Trust Manag. VII*, vol. 401, pp. 100–110, 2013.

[56] P. Mell and T. Grance, "The nist definition of cloud computing recommendations of the national institute of standards and technology," *Nist Special Publication*, pp. 1–7.

[57] Microsoft, "The STRIDE threat model," 2002. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[58] G. Motta, L. You, N. Sfondrini, D. Sacco, and T. Ma, "Service level management (slm) in cloud computing - third party slm framework," pp. 353–358, June 2014.

[59] S. New, "Supply chain traceability and product provenance: challenges for theory and practice," *Supply Chain Management and Logistics in a Volatile Global Environment*, 2009.

[60] A. Pannetrat and J. Luna, *Accountability and Security in the Cloud*, M. Felici and C. Fernández-Gago, Eds. Springer International Publishing, 2015.

[61] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong, and J. Lopez, "Accountability for cloud and other future internet services," *Proc. 4th IEEE Int. Conf. Cloud Comput. Technol. Sci.*, pp. 629–632, 2012.

[62] M. POWER, "The risk management of everything," *J. Risk Financ.*, vol. 5, no. 3, pp. 58–65, 2004.

[63] M. Power, *Organized Uncertainty - Designing a world of risk management*. Oxford University Press, 2007.

[64] S. E. Ramgovind and E. M.M. Smith, "The management of security in cloud computing," *Proceedings of Inf. Secur. South Asia*, pp. 1–7, 2010.

[65] C. Rong, S. Nguyen, and M. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, 2013.

[66] R. S. Ross, "Guide for conducting risk assessments," *Spec. Publ. (NIST SP) - 800-30 Rev 1*, pp. 1–95, September 2012.

[67] R. Samani, B. Honan, and J. Reavis, *CSA Guide to Cloud Computing*. Elsevier, November 2014.

[68] P. Saripalli and B. Walters, "QUIRC: A quantitative impact and risk assessment framework for cloud security," *Proceedings of IEEE 3rd Int. Conf. Cloud Comput.*, pp. 280–288, 2010.

[69] A. Shameli-sendi and M. Cheriet, "Cloud computing : A risk assessment model," *Proceeding of Cloud Engineering Conference*, pp. 1–6, 2014.

[70] Y. Sheffi and J. B. Rice Jr., "A supply chain view of the resilient enterprise," *MIT Sloan Manag. Rev.*, vol. 47, no. 1, pp. 41–48, 2005.

[71] Sourcemap, "Sub-supplier mapping: Tracing products to the source with a supply chain social network," pp. 1–5, 2011. [Online]. Available: http://www.sourcemap.com/

[72] C. Tang and J. Liu, "Selecting a trusted cloud service provider for your SaaS program," *Comput. Secur.*, vol. 50, no. 1, pp. 60–73, 2015.

[73] M. V. Thomas and K. Chandrasekaran, "A trust-based approach for management of dynamic qos violations in cloud federation environments," *Open Journal of Cloud Computing (OJCC)*, vol. 2, no. 2, pp. 21–43, 2015. [Online]. Available: http://nbn-resolving.de/urn:nbn:de:101:1-201705194523

[74] A. Weiss, "Computing in the clouds," *netWorker*, vol. 11, no. 4, pp. 16–25, 2007.

[75] L. V. D. Werff, T. Lynn, and H. Xiaong, "Building trust in the cloud environment: Towards a consumer cloud trust label," *Proceedings of ICDS2014 Conference*, pp. 157–163, 2014.

[76] A. S. Zalazar, L. Ballejos, and S. Rodriguez, "Security and compliance ontology for cloud service agreements," *Open Journal of Cloud Computing (OJCC)*, vol. 4, no. 1, pp. 17–25, 2017. [Online]. Available: http://nbn-resolving.de/urn:nbn:de:101:1-2017100112242

[77] L.-J. Zhang, J. Zhang, J. Fiaidhi, and J. M. Chang, "Hot topics in cloud computing," *IT Professional*, vol. 12, no. 5, pp. 17–19, 2010.

[78] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

AUTHOR BIOGRAPHIES

Olusola Akinrolabu is a Cybersecurity DPhil student at the Department of Computer Science, University of Oxford. Olusola's research interests include cloud computing, information security risk management, supply chains and security compliance monitoring. His current research work is looking into the assessment of cyber supply chain risks in cloud computing.

Steve New is an Associate Professor in Operations Management at Said Business School and a Fellow in Management Studies at Hertford College, Oxford. Steve's expertise is in process improvement and supply chain management, with a particular focus on the application of the Toyota Production System in medical care, and in the development of an underlying theory of provenance, the foundation for understanding reputation and ethics within supply chains. Much of his work is interdisciplinary, and he collaborates extensively with colleagues from across disciplines.

Andrew Martin is a Professor of Systems Security and Director of Centre for Doctoral Training in Cyber Security at the Department of Computer Science, University of Oxford. Prof. Martin undertakes research and teaching in the area of Systems Security, in the University of Oxford. His recent research focus has been on the technologies of Trusted Computing, exploring how they can be applied in large-scale distributed systems, particularly cloud computing, mobile devices, and the Internet of Things.