OPERATIONS AND SUPPLY CHAIN MANAGEMENT
Vol. 10, No. 3, 2017, pp. 130 - 140
ISSN 1979-3561 | EISSN 2759-9363

Can Improved Transparency Reduce Supply Chain Risks in Cloud Computing?

Olusola Akinrolabu
Department of Computer Science,
University of Oxford, UK
Email: olusola.akinrolabu@cs.ox.ac.uk *(Corresponding Author)*

Steve New
Said Business School,
University of Oxford, UK
Email: steve.new@sbs.ox.ac.uk

ABSTRACT

As organisations move sensitive data to the cloud, their risk profile increases due to the integrated supply chain utilised in cloud computing. The risk is made visible in situations where a cloud offering is federated, with customer data located in multiple datacenters, under the control of multiple providers and sub-providers in different jurisdictions. This problem is further exacerbated by the disposition of cloud providers to keep details of suppliers, data location, architecture, and security of infrastructure confidential from the cloud customers. As such, the shallowness of transparency amongst cloud providers makes it difficult for customers to assess the risk of cloud adoption. In this study, we report on our research into finding out how much customers know about their supply chain. We evaluate the transparency of cloud providers based on their published information and determine the resultant risk of limited visibility of the supply chain. In the course of the research, we identified eight transparency features, which, at a minimum, cloud providers should make available to their current or prospective customers, which we argue had no adverse impact on the competitiveness or profitability of the provider. The study concludes that ultimately, cloud supply chain transparency remains a customer-driven process.

Keywords: *cloud computing, supply chain, transparency, trust, risk, ERM*

1. INTRODUCTION

Cloud computing is an innovative shift from the traditional hardware outsourcing and independent software provider models. The cloud technology allows for the provisioning of Information Technology (IT) resources “as a service”, and offers this cloud service on a pay-per-use model (Leimeister et al., 2010; Sunyaev & Schneider, 2013). The utilisation of cloud services affords organisations, especially the smaller firms, access to compute-intensive applications, hardware resources with no upfront cost, a platform for innovation and IT scalability (Marston et al., 2011). Due to the use of distributed computing in cloud computing, there exists, an inherent concept of a supply chain where each member of the chain does what they know how to do best (Pohlman, 2010). The five characteristics of cloud computing (on-demand self-service, broad network access, resource pooling, rapid elasticity & measured service), as articulated in the NIST definition, further highlights the importance of supply chain in cloud offerings (Kaliski-Jr & Pauley, 2010). Similarly, the IT infrastructures that host cloud services can be hosted with multiple processors and subcontractors along a cloud chain, who belong to different legal entities and may be located in various jurisdictions. However, a layered cloud service involving multiple sub-providers will invariably pose a higher risk than a service hosted by a single provider (Weber & Staiger, 2014). Therefore, the risk of adopting a cloud service increases with the degree of in/outsourced hosting that makes up the service.

When organisations move their business processes to the cloud, their risk profile changes, and becomes a combination of their risks and a subset of their cloud service provider (CSP) risk, leading to many unknowns (Cayirci et al., 2014;Chan et al., 2012). Without sufficient management insight (due diligence) into the procurement of cloud services, a small investment in a BAU cloud application could have a significant impact on an organisation’s security posture (Chan et al. 2012). The abstraction of the cloud, the dynamism of the supply chain and the fundamental lack of transparency of cloud providers further exacerbate the risk organisations face when they adopt cloud computing. The lack of visibility into cloud supply chain makes it difficult to determine how data is treated when in the hands of sub-providers, given the limited insights customers have into sub-provider location, compliance, jurisdiction and processes (Raj Samani, 2011). Likewise, historically, providers have been circumspect about supply chain visibility, for the genuine risk of industrial espionage, sabotage, malicious attack or even reputational damage (New & Brown,2012). As such, there seems to be a distinct lack of supply chain transparency amongst CSPs, and this is setting back cloud adoption.

Transparency allows customers to verify that their trust in the CSP is not misplaced (Vijayan, 2015). According to Kaliski-Jr and Pauley (2010), an increased level of trust improves disclosure, reduces the demand for legislation, and reduces perceived risk. Albert S. & Rajeev (2015) hold the view that improved visibility of the supply chain helps customers to determine the trustworthiness of a cloud service a priori, based on its profile and security assurances. Transparency also encourages an alliance between customers and provider, allowing CSPs to focus their resources on providing services their customers want, and likewise benefitting more from an increased market share (Wisner, Tan, & Leong, 2008). According to the Business Dictionary (2016), transparency is the minimum degree of disclosure to which agreements, dealings, practices, and transactions are open to all for verification. Gavan Egan, vice-president of Verizon Terremark Europe, said, "Transparency is the biggest challenge in moving to the cloud and not security" (Ashford, 2013). Werff et al. (2014) highlight the advantage of cloud trust built on the knowledge of CSPs processes, architectures, and visible controls over the trust based on pure calculation. Some of the inherent cloud computing risks which can be addressed by supply chain transparency include loss of governance, malicious insiders, regulatory compliance, legal and jurisdictional risks, isolation failure due to multi-tenancy, data segregation and long-term viability(CSA, 2013;Brodkin, 2008).

In this paper, we investigate the extent of supply chain information CSPs share with their customers and suggest steps that providers can take to improve the transparency of their supply chain, to allay the growing concern amongst cloud consumers, who leverage cloud resources for their business-as-usual (BAU) and strategic goals. We argue that since the purpose of every cloud supply chain is to achieve high quality and responsive service offered at a low cost to the customer, the goal could be facilitated through increased visibility into the vulnerability of the chain, which helps to foresee challenges and enable proactive response, increasing both efficiency and profitability. Previous studies into the cause of limited transparency in computing technologies including the cloud, found the cost of provenance to be a major obstacle. Fisher et al. (1997) put forward the view that investing in supply chain efficiency for innovative and short lifecycle products, leads to a decrease in margin. Although the research of Pearson et al. (2012) identified the general desire for secrecy amongst CSPs especially those involved in the development of encryption-based proprietary security, New & Brown (2012) were able to establish a case for the genuine risks that can result from supply chain transparency. Many providers of innovative technologies fear that greater visibility into their chain could reduce their exclusivity or set back their market position, especially in the event of continuous supply chain disruption (New & Brown, 2012). While we recognise the cost implication and risk of espionage that is synonymous with the transparency of the supply chain, we investigate the level of information customers require to be able to assess their risks adequately and implement controls to protect their company sensitive information and intellectual property.

To help us understand what CSPs think of supply chain transparency, we developed a fictional story of a Software-as-a-Service (SaaS) provider, who suffered a downtime as a result of a power outage at their CSP's Internet service provider (ISP). With respondents assuming the role of incident managers of the SaaS provider, we asked them to provide answers to two questions namely: i) what questions should the SaaS providers ask their infrastructure provider? ii) How much information on its supply chain should the CSP be willing to share? The novelty of this paper is to examine what information CSPs currently share with their customers, its effect on cloud adoption, and how CSP transparency can be improved. Using the transparency features identified during the case study and subsequent interviews with CSPs, we carried out a systematic comparison among twenty-five SaaS vendors based on their supply chain transparency. We present our findings in the result section of this paper.

The remainder of the paper is structured as follows: Section 2 reviews the literature concerning supply chain risks, transparency and cloud computing. Section 3 then describes our research question (RQ) and methodology. Section 4 continues by presenting our SaaS comparison result and discussion of our findings. Finally, we conclude the paper in Section 5 and present ideas for future research.

2. LITERATURE REVIEW

Since this paper focuses on understanding how improved supply chain transparency can reduce cloud computing risks, we should begin by describing some of the core terms starting with cloud computing. Amongst the plethora of definitions for cloud computing, we present that of Leimeister, et al. (2010), who defined cloud computing as an “IT deployment model, based on virtualization, where resources, in terms of infrastructure, applications and data are deployed via the internet as a distributed service by one or several service providers”. These services are scalable, on-demand and can be priced on a pay-per-use basis”. Wisner et al. (2008) define a supply chain as the series of companies that make products and services available to consumers, including all the functions enabling the production, delivery, and recycling of materials, components, end products and services. Also, according to FT Lexicon (n.d.), supply chain transparency captures the extent to which information about the companies, suppliers and sourcing locations is readily available to end-users and other businesses in the supply chain. Lastly, a risk is defined in ISO 27005 (2011), as the effect of uncertainty on objectives. Wisner et al. (2008) also describe supply chain risk as the likelihood of an internal or external event that causes a disruption or failure of supply chain operations, causing potential reductions in service levels, product quality, and sales, with an increase in costs.

There appears to be very little studies that have directly addressed the effect of supply chain transparency in reducing cloud computing risks. Although, we are aware of the efforts of leading organisations such as CSA, National Institute of Standards and Technology (NIST) and European Network and Information Security Agency (ENISA), who have published studies, surveys and recommendations addressing cloud computing risks. Cloud computing risks range from high, medium and low risks, and these risks are dependent on organisation, cloud model and service provider offering. Some of the typical cloud computing risks include i) disruptive force ii) multi-tenancy liability iii) lack of transparency iv) high–value cyber attack targets and v) risk of data leakage (Chan et al., 2012).Although, majority of these risks are not likely to be mitigated by contractual clauses with the CSP, many cloud customers, particularly SMBs, in embracing the cloud's economies of scale and flexibility advantages, end up blindly trusting the CSP and accepting the risk to run their entire enterprise in the public cloud due to the small up-front capital investment requirements.(Chan et al. 2012; Gadia 2011).

Felici & Pearson (2015) identified the effect of multi-tenancy, abstraction, automation, data duplication, data access from multiple locations and sub-processing as positive cloud features that could potentially set back data protection. Weber & Staiger (2014) in observing the complex liabilities of the cloud, emphasise the increased risk associated with a layered cloud service involving multiple sub-providers when compared to another with a single provider. This complex service provision eco-system may not be visible to an enterprise outsourcing their data processing to a CSP (Pearson et al., 2012). Cayirci (2015) explored the complexity involved with CSPs complying with the legal systems when they deliver cloud services over the Internet to global customers. They identify the frustrations and the near impossibility of cloud providers to satisfy all the applicable laws in these jurisdictions, which is a reason for some deciding not to comply or avoid doing business in some jurisdictions. Microsoft (2015) in identifying the top five deliverables customers want from their CSP, explained how the complexity and scope of standards and regulations evolve with the increase in an organization’s cloud adoption. It becomes more challenging for an organisation to be assured of its compliance with regulations, as its data moves within the cloud supply chain. Pearson et al. (2012) recommend the application of a “chain of accountability” whereby members of a cloud ecosystem ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs.

According to Weber & Staiger (2014), the move to the cloud consists of two decisive factors: risks associated and benefits to be gained. Chan et al. (2012) recognise the need for organisations to account for cloud computing risks in their enterprise risk management (ERM) programs. They recommend that as a prerequisite for cloud adoption, organisations should have a strong governance model, a sound reporting structure, an understanding of internal IT skills and most importantly a clearly defined risk appetite. The effectiveness of risk management greatly depends on the extent to which it succeeds in becoming a part of an organisation's culture (ENISA, 2006). Along similar lines, CERT-UK (2015) uses examples of security compromises to illustrate the need for a broad, inclusive approach to risk management within a supply chain, stressing that it helps organisations to map their cyber security dependencies and vulnerabilities. The ISO21000 highlights transparency and inclusivity as part of the principles for a successful risk management (Verbano & Venturini, 2013).

Felici & Pearson (2015) recognise an in-depth connection between accountability, trust and risks, whereby accountability enhances trust and trust help change consumers and providers’ perception of risk. According to CERT-UK (2015), cyber security risk management within the supply chain is primarily an issue of trust. Wisner et al. (2008) in identifying obstacles that often prevent the integration of supply chain listed the lack of trust, silo mentality and lack of visibility. According to ISACA & CSA (2015), this trust is built mainly on provider's reputation, and through visible controls, the service provider has implemented. This trust can be established based on performance, predictability and helpfulness of the CSP (Werff et al., 2014). The A4Cloud in their research work, focus on accountability as the most crucial prerequisite for the control of corporate and private data processing in the cloud, and they claim CSPs should be held accountable for how they manage personal, sensitive and confidential information in the cloud(Pearson et al., 2012).

The integrated supply chain in cloud computing, whereby standardised cloud services are built on existing sub-provider services, calls for an increased transparency to help identify potential failure or disruption points in the supply chain, and establish a likelihood/probability of their occurrences. Wisner et al., (2008) observe the dynamic boundaries of supply chain and the difficulty of providers to coordinate supply chain beyond the 2nd tier, while Tom Ridge, CEO of risk management firm Ridge Global, is of the opinion that supply chains especially those involving multinational companies, need to be inspected down to the second, third, and fourth tiers (Wisner et al., 2008). However, Boyens et al. (2015) and New & Brown (2012) share a fundamental premise concerning the increase in the cost of doing business with providers that allow increased level of visibility into their security and supply chain practices. Another important argument put forward against visibility, is one of liability, whereby you become more liable the more you know about your supply chain (New, 2009).

According to Chopra & Sodhi (2004), most companies develop plans to protect against recurrent, low-impact risks in their supply chains, and all but ignore the high-impact, low-likelihood risks. For example, when big cloud providers are asked about what will happen should they lose one of their primary datacenters to terrorism, the response they give leads one to believe such risk is not in-scope. It is pertinent for organisations whose critical data reside in the cloud to develop a robust threat model to help identify and prioritise the supply chain risks (Charney & Werner, 2011). Chopra & Sodhi (2004) present the view that understanding the variety and interconnectedness of supply chain risks would assist risk managers in developing a tailor-balanced and effective risk-reduction strategy for their organisations, but argue that perhaps the biggest challenge companies face is mitigating supply-chain risks without eroding profits. According to Charney & Werner (2011), any framework needed to mitigate supply chain risk must promote transparency by all parties.

Two important themes emerge from the studies discussed so far; there is an inherent risk in cloud computing due to its dynamically complex supply chain, and also, the process of managing cloud computing risks can be improved through visible controls and improved transparency. Therefore organisations adopting cloud computingneed a broad and inclusive ERM to accommodate the risks associated with the cloud. In our study, we take a look at the nature of information customers need to have about their CSP and its' supply network that can assure that the risk of adopting the cloud service can be operationalized. Likewise, we investigate the level of information on the supply chain that a sample of cloud providers currently share through their websites and how much they are willing to tell their prospective or current customers if probed for details.

3. METHODOLOGY

Our methodology to address the effect of transparency in reducing cloud supply chain risk was to engage in a field research. Qualitative methods (case study, and interviews) were chosen to allow for a deeper insight into supply chain risks as we get to look at the issues from different perspectives, including both customer and providers in our study. We set out to determine how providers could offer a more transparent service to assist customers with mitigating their risks, while still maintaining their intellectual property and competitive advantage. Our research adopted the use of a case study, as it is a well-established approach to explorative investigation. We developed the case study for a fictitious company (Payworq) who experienced an outage due to their CSP's Internet Service Providers (ISPs) service failure. The questions that followed the case study contained aspects of our four main research questions, which are as follows:

1. *What information should cloud customers ask CSP about its supply chain?*
2. *How much should CSP be willing to share with their customers?*
3. *What are the risks of customers not knowing enough about the supply chain?*
4. *How can transparency be improved in cloud computing?*

The respondents to the case study were made up of SaaS, PaaS and IaaS vendors who either owned their hosting infrastructure or partnered with one of the top four cloud IaaS providers. They included CEOs of start-up CSPs, technical directors, and business development executives representing service providers, cloud brokers and cloud equipment manufacturers. As a supplement to our case study, we chose to interview cloud providers on their thoughts on supply chain transparency and its associated risk in cloud computing. The Cloud Expo event at the Excel Centre in London between the 12th and 13th of April, 2016, provided us with the opportunity to interact with a broad range of cloud providers. We approached about 40 of the exhibitors, but only 15 of them granted us an audience, with the majority of the interview conducted on the promise of anonymity. The interviews were organised around a set of predetermined open-ended questions, with other issues emerging from the response provided by the interviewee. Moreover, the semi-structured nature of the interviews enabled us to engage the cloud providers in further conversations around their cloud offering and supply chain while also giving us an opportunity to assess their transparency.

From our analysis of participants' response to the Payworq case study and interviews, we gathered some transparency features that could be useful in comparing cloud providers, based on the information they published on their websites. We examined twenty-five SaaS vendors, which were conveniently sampled from a list of the top 200 UK public cloud computing providers identified by Cloudscape (Bilderbeek, 2014). Cloudscape categorised SaaS providers under seven main headings including an eight catchall category, "other". Out of the seven main categories, we compared SaaS providers in five different cloud service category namely: online workspace, finance/ERP, human resource management (HRM), customer relationship management (CRM), and collaboration (Bilderbeek, 2014).

The University of Oxford ethical approval committee, under Ref No: R44459/RE001 approved this research work involving external participants. The research plan described the use of the qualitative method of research (case studies) and the recruitment of participants to take part of the survey. Other details around the anonymity of participants' data were requested and approved by the board. All participants were presented with a consent form describing the purpose of the study, its ethics committee approval, and their ability to withdraw their data at any time. We also assured the participants that their data would be stored securely following the University of Oxford ethical standards.

4. FINDINGS AND DISCUSSION

In this chapter, we discuss the results obtained from our case study, interviews, and cloud provider website comparison. The participants for each of the methods used in this research volunteered themselves to participate. We utilised different recruitment strategies for each stage of the research. For the case study, some of the respondents were sent emails with a link to the google form used for the case study, while we approached the other participants directly during the cloud expo event, where we also conducted the interviews. The individual research activities are discussed in the following sections with emphasis on our research questions. After which, we summarise the chapter with the findings of our work.

4.1 Case Study

We sent the case study (see Appendix 1) to a total of 47 contacts, which were made up of SaaS and IT industry experts, but only 12 of them responded, all of who were male, giving us a response rate of 25.5% over the three-month period. The twelve responses received were of good standard, judging from the level of analysis of the case study that was carried out by each of the respondents. The two questions that accompanied the case study connect back to our research objective of finding out the effect of transparency in reducing the supply chain risks in cloud computing. The questions are as follows:

1. *What information should Payworq ask for? Cloud computing services are often sold on the idea that customers do not need to know the exact detail of the operations of their Cloud Service Provider’s operations: but is this a good idea?*
2. *How much should A400 be prepared to tell? Providers are often reluctant to reveal too much about their operations - even to customers. What are the issues about being completely transparent about your operations?*

In practice, the information a customer can ask CSPs outside the information readily available to them from provider websites, and marketing document cannot be easily estimated. Large customers are known to be able to get CSPs to respond to their request for information (RFI), because of their higher purchasing power. However, the same cannot be said of SMBs, who according to Raj Samani (2011) get little cooperation, let alone answers when they submit questionnaires to large corporations. Interestingly, according to a World Bank research, SMBs accounts for 95% of existing businesses and their products and services make-up around 49.8% of the global economy (BCSG, 2015).

The response from our participants elicited a range of ideas. Over half of the replies contained the need for the cloud customer to have a high-level understanding of the architecture of the CSP's infrastructure. One of the participants commented: *“The underlying infrastructure* *provider should not be a secret, and CSP should be willing to share high-level details of their architecture and dependencies on third party providers".* Zhang et al. (2010) established a correlation between the security risk associated with a cloud delivery and its cloud architectures and security controls. Another interesting aspect of our respondent's feedback was the definition of service level agreement (SLA). Eight of the respondents requested the CSP to provide further details on their SLA with regards to the outage and onwards support. One respondent suggested Payworq to "*get an understanding of the CSPs uptime record as well as SLA, as this helps Payworq in setting their own SLA to their customers"*.

Some of the other information highlighted by the respondents are listed as follows:

- **Monitoring and Notification capabilities**: According to Lee Newcombe (2012), customers should trust their CSPs ability to implement adequate monitoring and event management to enable them to inform customers of events requiring their attention or action promptly. One respondent mentioned that*: "CSPs should concentrate on procedures for notifying clients of problems rather than detailed internal operations"*.
- **Certification and Audits**: Respondents encouraged Customers should ask CSPs for the professional and third-party certification of their operations. One respondent suggested that CSP audits should include independently verified audit reports such as theService Organization Control (SOC) 1 and SOC 2 Type II reports.
- **Security Controls:** In addition to the high-level architecture, the majority of case study participants believe customers need to know about security controls implemented by the CSP to protect their data. These controls include physical security, network security and application security.

On the subject of how much CSP should be willing to share with their customers, 75% of the respondents were in support of information sharing. Respondents suggested that *the CSP should be prepared to tell as much as the customer will understand*, which we felt was promoting information asymmetry and could be advantageous to larger organisations with more technical resources, and less so for SMBs. Although this idea is in line with that of Lamming et al. (2002), who proposed that the information sharing within a supply chain must be reciprocal, selective, and justified but not necessarily symmetrical. Another respondent referenced the notion of providing customers sufficient information to assess their risk, stating that: *"the exact topography and schematics do not need to be shared, but A400 should be prepared to discuss where their solution has a reliance on a 3rd party e.g. Rackspace, etc."*. In analysing the other responses received, we identified that about three of the respondents were against full disclosure of the CSPs supply chain, with one respondent asking *why A400 should provide details of their supply chain when most businesses do not*. Another perspective of supply chain transparency paradigm is that of trust. One of our participants in relating trust to the case study *believes that A400 needs to give Payworq enough information to build or retain trust otherwise they risk losing customers after such incident*. He went further to say that coupled with providing clients with high-level architecture, redundancy and security control information, CSPs can also share with their customers their process for choosing a supplier. All of this he claims gives the customer confidence in their cloud solution.

In summary, the case study gave us a good foundation in this exploratory research into the effect of transparency in reducing supply chain risks in cloud computing. We have been able to provide answers to two of our research questions, although we will continue to build on them in the subsequent sections. The participants' feedback on the information customers should be willing to ask their CSP provided us with some transparency features (security controls, architecture, SLA, DR/BCP, IT certification, technology partners), which we used in comparing CSPs on their supply chain transparency in the latter part of the study. Despite the limited number of participants, we feel the information gathered provides a good groundwork for future research on this topic.

4.2 Interviews

In this section, we discuss the findings of our data collected through in-depth semi-structured interviews with the cloud vendors. At the start of each interview, we asked our interviewees how much they knew about their supply chain? As expected, some of the providers who hosted their infrastructure, were quick to say they were their own supplier, but with a little more clarity on the definition of a supply chain, as defined by Wisner et al. (2008), we were able to correct this notion. However, the responses were mixed, with the larger organisations knowing more about their provider's, up to about the second tier or third tier in rare cases, and the smaller SaaS vendors not quite so. One of those interviewed was the CEO of an original equipment manufacturer (OEM) for a private cloud infrastructure, and in our conversation, we gathered that although the product was assembled in the UK, the components were sourced from a major supplier in China. When asked, if there was a contingency in place, the answer was affirmative, but he admitted that since *they lack the visibility into the 2nd, 3rd and 4th tier suppliers, there is no guarantee that both major supplier's arrangement are not dependent on similar sub-suppliers*. Furthermore, we gathered from some of the start-up firms that traceability most times comes at a premium, which they were not willing to pay.

When asked why some CSP did not prioritise supply chain risks or the general risks of cloud computing, the interviewees pointed out that although they thought about it, it is hard to assess a worst-case scenario. One respondent added that: *".... the fact that no major event resulting in multi-billion dollar loss has happened in the cloud does not mean one will not occur shortly, but we do not know any better"*. Which brings up an interesting observation by New & Brown (2012) concerning how the Japanese earthquake of 2011 changed the perspective of manufacturing organisations to supply chain risks. Perhaps, it will take a significant breach or downtime to one or several cloud giants before the cloud community can be awakened to the realisation of the complex commercial interdependencies that exist in cloud computing and its resultant risks, a point also echoed by Pearson et al. (2012). Some of our interviews led to the conversation on cloud insurance, which from what we gathered is beginning to take shape in the cloud computing industry. In 2013, MSPAlliance in partnership with Lockton Affinity, a large privately owned independent insurance broker, announced a new Cloud and Managed Services Insurance (Reuven Cohen, 2013). The uncertainty of the effect of cloud risks has led providers who retain liability as part of their customer contracts to reduce such liability by taking up an insurance contract (Weber & Staiger, 2014). Although outages are part of today's technology landscape, many cloud providers have built their reputation on the resilience of their service, and as such have attracted more risk adverse customers and are therefore in need of extra assurance or comprehensive protection (Reuven Cohen, 2013).

The issue of trust as earlier discussed in the literature review is one that is essential for cloud survival. Das & Teng (2001) were able to establish the linkage of trust and control with risk when dealing with strategic alliances. One of our interviewees pointed out that the situation of transparency and trust is a catch-22, saying, *"If I tell you, you might know my weakness. If Ido not say, you do not trustme."* According to Akkermans et al. (2004), there is a feedback loop, whereby the increase in trust leads to increase in transparency, which improves decision-making quality and improves supply chain performance. Also, one of the respondents cited the example of how his organisation adopted the "travail" method of transparency, suggested by Akkermans et al. (2004) to help their customers understand how much effort goes into securing their data.

In conclusion, we found out that the transparency of supply chain is a customer-driven process. Many of the CSPs confirmed that most customers do not ask for too much information about the cloud service or its supply chain but are more concerned with the cost. Also, we learnt that the reason many customers used AWS or Rackspace instead of the smaller public cloud providers was that, they paid less attention to where their data was stored or who had access to it, as long as the service was cheap. For the CSP, there is an incentive to establish trust with their customers, and this can happen when they can provide the needed information to them. The advice is for CSPs to start simple and get comprehensive if needed. Cloud providers who automatically update their service status, uptime and SLA targets on their web portal for their customers to see, are also challenging themselves to optimal performance. We identified the reason for the blur of vendor information sometimes for competitiveness and exclusivity, but also recognise that the transparency of cloud suppliers can also be leveraged for trust, as was the case with some of the start-ups we interviewed who branded their solution with Amazon AWS. Except for two interviewees, all others were in support of more transparency from the cloud providers, both through their online presence and in their day-to-day relation with their customers. Although this could cause a particular bias, considering they might consciously or unconsciously want their organisation to look good from the outside, more so as it related to security. Our opinion as a whole is that the interviewees were genuine in their views, and they were forward thinkers, who looked to make cloud computing secure for customers.

4.3 Cloud Service Provider Comparison

The growing trend in cloud adoption has seen a surge in the number of companies rolling out public cloud services, to meet their customers need. The many success stories of SaaS applications have demonstrated the relative ease at which start-up companies can launch a cloud service, with no upfront cost, and within few months' boast of a sizeable customer base. Our focus was to compare SaaS providers, whose services could potentially be bought online, by a new customer looking to adopt cloud services and who based his/her decision on the information available on CSPs website. Talluri et al. (2006) discussed how traditionally, vendor evaluations have been based on financial measures with less emphasis on other tangible or intangible criteria but how this trend has changed, leading to the use of methodological developments in vendor evaluation techniques. The methodological approach base vendor evaluation on the consideration of multiple measures that often included product and service-related attributes (Talluri et al., 2006). We applied this methodological approach in our comparison of CSPs and centred our comparison on eight transparency features, namely:

- Architecture
- Technology/Partners
- Datacenter location
- Security features
- IT-related compliance certifications
- Advertised Service Level Agreement (SLA)
- Disaster recovery/ business continuity
- Monitoring/Support

As we have discussed earlier in this study, trust in a cloud service can be enhanced based on the knowledge of the CSPs processes, architectures and visible controls, and this trust together with control reduces the perceived risk of a cloud service. Below is a tabular comparison of our 25 SaaS providers as conveniently sampled from the Cloudscape report (Bilderbeek, 2014).

Table 1 shows the results obtained from the comparative analysis of the 25 SaaS providers. Although this comparison is far from authoritative, considering our method of gathering the data, we believe it is a good start and could be developed further to establish the minimum level of information CSPs should publish on their website; thus boosting cloud transparency. We investigated various vendor evaluation techniques including simple weighted scoring methods, complex mathematical programming, and neural network models (Talluri et al. 2006). In the end, we chose to go with a simple numerical scoring system, where for every transparency feature a CSP published on their website, we gave them one point and did not give any point for missing features, assuming each element is equally weighted. From the data in **Table 1**, we can see that the CSPs in the finance/ERP sub-group scored the lowest points. One possible reason for this is the fact that the CSPs are vertical industry specific since they operate in the finance sector, where local knowledge and regulation is essential. Their websites only seem to make reference to cloud hosting for a technological advantage, and all other contents are geared towards promoting how the software works, pricing and other marketing information. In our analysis, CSPs in the online workspace sub-group were found to be the most transparent.

Table 1 Comparison of 25 Saas Providers Taken from Cloudscape

SaaS Cloud Provider comparison based on Transparency feature											
SaaS Cloud Provider	**Architecture (Yes/No)**	**Technology/ Partners (Yes/No)**	**Data center location (Yes/No)**	**Security features (Yes/No)**	**IT-related compliance certifications (ISO 27001, PCI-DSS, ITIL etc.) (Yes/No)**	**Other cloud offering (PaaS, IaaS & Others)**	**Private, Public, & Hybrid**	**Advertised Service Level Agreement (SLA) (Yes/No)**	**Disaster Recovery/ Business Continuity (Yes/No)**	**Monitoring/Support (Yes/No)**	**Scoring (No. of Yes) Maximum=8**
Online workspace sub-group											
CSP1	Yes	Yes	Yes	Yes	Yes	IaaS and PaaS	All	No	Yes	Yes	7
CSP2	Yes	Yes	Yes	Yes	Yes	IaaS	All	Yes	Yes	Yes	8
CSP3	No	Yes	Yes	Yes	Yes	IaaS and others	All	No	Yes	Yes	6
CSP4	No	Yes	Yes	Yes	Yes	IaaS and others	All	Yes	Yes	Yes	7
CSP5	Yes	Yes	Yes	Yes	Yes	N/A	All	Yes	Yes	Yes	8
Finance/ERP sub-group											
CSP6	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
CSP7	No	No	No	Yes	No	N/A	public	No	No	No	1
CSP8	No	Yes	Yes	Yes	Yes	IaaS	All	No	Yes	Yes	6
CSP9	No	No	No	No	No	N/A	public	No	No	No	0
CSP10	,No	No	No	No	No	N/A	public	No	No	No	0
Human Resources (HR) sub-group											
CSP11	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP12	No	Yes	No	Yes	No	N/A	public	Yes	No	Yes	4
CSP13	No	Yes	Yes	Yes	No	N/A	public	No	Yes	Yes	5
CSP14	Yes	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP15	No	No	No	No	No	N/A	public	No	No	No	0
Customer Relationship Management (CRM) sub-group											
CSP16	No	Yes	Yes	Yes	No	N/A	public	Yes	Yes	Yes	6
CSP17	Yes	Yes	Yes	Yes	Yes	N/A	public	No	No	Yes	6
CSP18	No	Yes	No	No	No	N/A	public	No	No	Yes	2
CSP19	No	Yes	Yes	Yes	No	IaaS	public	Yes	Yes	Yes	6
CSP20	No	No	No	Yes	No	N/A	public	No	No	Yes	2
Collaboration sub-group											
CSP21	No	No	No	Yes	No	N/A	public	No	No	No	1
CSP22	Yes	Yes	Yes	Yes	Yes	N/A	public	Yes	Yes	Yes	8
CSP23	No	Yes	Yes	Yes	No	N/A	All	Yes	Yes	Yes	6
CSP24	No	Yes	Yes	Yes	Yes	IaaS and PaaS	All	Yes	Yes	Yes	7
CSP25	No	Yes	Yes	Yes	Yes	N/A	Public	Yes	Yes	Yes	7

With a mean score of 7.2, the five CSPs showed a clear understanding of their cloud architecture, provided detailed information about their cloud offering, and steps they took in securing customer data. Since most of the CSPs were also IaaS providers, we hypothesise that the reliance of other CSPs on IaaS providers, and the need for the vendors to stand out, have led to their increase in supply chain transparency.

On Architecture, the overall evidence of cloud architectures published on CSP websites was inadequate. However, we are not surprised by this trend, considering the level of abstraction that makes up most cloud architectures. Out of the 25 CSPs, we compared, only four of them provided details of their cloud architecture, three of which were IaaS providers whom we might expect to provide this information to their prospective IaaS and SaaS customer. With regards to SLA, again, the finance sub-group was the worst performing group of CSPs, with none of our compared CSPs having any SLA published. To verify this claim, we carried out searches using Google search techniques, looking for the word "SLA" on their websites and this did not yield any result. The online workspace and collaboration sub-group had excellent transparency scores for DR and monitoring capabilities. One of the many known advantages of using a cloud service was that a CSP could help customers with their incident response and disaster recovery as most CSP have this capability inbuilt into their service. While we believe on the average this is true; our data suggests that not all providers of cloud service prioritise disaster recovery. Our worst performing sub-groups for DR transparency were finance and CRM.

Lastly, we compared the SaaS providers based on their transparency of datacenter locations. Sixteen of the twenty-five vendors made mention of their datacenters and its location, with some more detailed than the others. A few of the CSPs just alluded to the fact that customer data was hosted in a Tier "x" datacenter in the UK, while others provided the location, and who owned the datacenters. We believe that, for customers to exercise their data controller rights over their data, they need to have visibility of that data, know where it is stored and how it is secured, and also policies and procedures surrounding its use.

In conclusion, and to answer our fourth research question, we assert that transparency is not a black or white situation, which is evident in our comparison, considering different organisations approach transparency in distinct ways. We discovered that SaaS providers who offered IaaS services were more transparent than regular SaaS vendors. Mainly, we found that vertical industry specific CSPs concentrate on their product and its functionality, and provide little detail on the supply chain and the security of the product. Our analysis of this vertical industry trend is in threefold, and one is that the SaaS providers do not have enough information on how their service is being provided and have completely outsourced technical control of the infrastructure to their IaaS provider. The second is that the CSP wrongly assumes that their customers are not interested in the security and availability of their data. Thirdly, it might just be that they omitted this information from their website, but are willing to share it with prospective customers at any point. We agree with Fischer-Hübner et al. (2014), on their suggestion that complex supply chain information should be provided in layers, and argue that the eight transparency features we identified can be used as a starting point for all CSPs. We believe that this information would not impede the CSPs competitive advantage, neither would it violate their intellectual rights.

5. CONCLUSIONS AND FUTURE WORK

In this study, we set out to determine the effect of transparency in reducing supply chain risks in cloud computing. Cloud computing is a combination of benefits and risks. The delivery of a cloud service is rooted in an inherently complex and dynamically formed cloud provider chain. This complexity of cloud supply chain, made up of sub-tiers of multiple suppliers, increases cloud risk in a way that makes it unlikely to be mitigated by contractual clauses with the CSP. We found out that although there was an incentive for cloud providers to be transparent with their supply chain, not least to gain the trust of their customers, some CSPs refrained from doing this for the sake of maintaining profitability, protecting intellectual property and competitive advantage. Some of the identified reasons for the vague information on supply chains include:

- CSPs are not aware of their supply chain beyond the first tier.
- Cloud customers favour the functionality and cost of a cloud service over its provenance.
- CSPs are uncertain about the quality and quantity of technical and supply chain information to share with their customers.

We mainly observed a lack of transparency among the CSPs that provided services for the vertical market such as financial industry and noticed that providers of infrastructure services (IaaS), provided more detailed information about their supply chain than the typical SaaS provider. This might be due to the diverse customer base of IaaS providers, which included both end-customers, as well as SaaS and PaaS providers. We established that an improved communication within the supply chain and transparency into the adequacy of the internal controls provided trust in operation, confidence, and adequate understanding of residual risk.

To address the quality and quantity of information CSPs should share with their customers, we identified eight transparency features (security controls, architecture, SLA, DR/BCP, IT certification, technology partners) that we firmly believe should be made available to prospective and current customers. We used these features to compare 25 SaaS providers cut across five cloud service categories and concluded that although each provider approached supply chain in a different way, customers develop confidence in the services of providers that were upfront with detailed information on these transparency features. We conclude that, although cloud supply chain is not a black or white situation, it is ultimately customer-driven and could soon become a competitive differentiator for cloud service providers, especially SMB providers.

Despite its exploratory nature, this study has gone some way towards enhancing our understanding of cloud provider chains and the thoughts and action of cloud providers concerning supply chain transparency. Whilst not conclusive, this study makes a significant contribution to addressing: (i) the nature of supply chain information CSPs can share with their customer while still maintaining their competitive advantage; (ii) the level of information vertical and horizontal market CSPs currently publish on their website; and (iii) the importance of the supply chain awareness and the visibility of third party risks to effective risk management. However, the major limitation of this study is its ability to generalise to the wider cloud provider community due to the number of respondents that participated in each of the phases.

For our future work, we would be expanding on our cloud comparison study to include PaaS and IaaS vendors, as well as increase the transparency features, with each feature having a different weighting that can be fed into an algorithm to calculate the overall transparency of a CSP. The inclusion of IaaS and PaaS providers in this comparison would be to investigate if indeed there is a pattern of supply chain transparency with the different service models, or perhaps it is ultimately down to the strategic decision of the management of each CSP. We will undertake a systematic random sampling of the UK cloud computing provider's directory, expecting to identify 100 cloud providers that we can assess. Furthermore, according to Fisher et al. (1997), there is a right supply chain for every product, from functional to innovative, as well as BAU and strategic. Therefore, we hope to develop a framework that can help providers formulate the best supply chain strategy for their offering, and determine the level of transparency applicable to each arrangement with a capability of improving their overall performance. We aim to investigate how different supply chain arrangements assist CSPs to offer secure and reliable services, introduce a steady stream of innovations, predict demand, maximise profit, and remain viable while meeting customer needs.

ACKNOWLEDGEMENTS

This research project has been possible thanks to a DPhil grant from the Engineering and Physical Sciences Research Council (EPSRC) and Kellogg College, University of Oxford.

REFERENCES

Akkermans, H., Bogerd, P., & Van Doremalen, J. (2004). Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics. *European Journal of Operational Research* 153 (2), pp. 445–456.

Horvath, A.S. and Agrawal, R., (2015). Trust in cloud computing. In SoutheastCon 2015 (pp. 1-8). Fort Lauderdale, FL, USA.IEEE.

Ashford, W. (2013). Transparency, not security, is biggest cloud challenge, says Verizon. Retrieved May 1, 2016, from http://www.computerweekly.com/news/2240185187/Transparency-not-security-is-biggest-cloud-challenge-says-Verizon

BCSG. (2015). The small business revolution: trends in SMB cloud adoption. Retrieved June 7, 2016, from https://www.bcsg.com/wp-content/uploads/2015/03/The-small-business-revolution-trends-in-SMB-cloud-adoption.pdf

Bilderbeek, P. (2014). CLOUDSCAPE – Top 200 UK public cloud computing providers, 2014. Retrieved May 5, 2016, from http://www.themetisfiles.com/2014/03/cloudscape-uk/

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Special Publication*, *800*(161), p.1.

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. *InfoWorld*, *July*, 2–3. Retrieved August 29, 2016, from http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf

BusinessDictionary. (2016). What is transparency? definition and meaning - BusinessDictionary.com. Retrieved August 27, 2016, from http://www.businessdictionary.com/definition/transparency.html

Cayirci, E. (2015). Models for Cloud Risk Assessment: A Tutorial. In *Accountability and Security in the Cloud*. Springer International Publishing. (Vol. 8937, pp 154-184).Available from: http://link.springer.com/10.1007/978-3-319-17199-9

Cayirci, E., Garaga, A., De Oliveira, A. S., & Roudier, Y. (2014). A cloud adoption risk assessment model. *Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014*, 908–913. http://doi.org/10.1109/UCC.2014.148

CERT-UK. (2015). Cyber-security risks in the supply chain, 10. Retrieved from https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf

Chan, W., Leung, E., & Pili, H. (2012). Enterprise risk management for cloud computing. *Committee of Sponsoring Organizations of the Treadway Commission*, 4.

Charney, S., Werner, E.T. and Computing, T., 2011. Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust. *Microsoft Corporation paper*, pp.6-8.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review*, 46(1), pp. 53 – 61.

CSA. (2013). Cloud Security Alliance Warns Providers of "The Notorious Nine" Cloud Computing Top Threats in 2013 : Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/media/news/ca-warns-providers-of-the-notorious-nine-cloud-computing-top-threats-in-2013/

Das, T. K., & Teng, B.-S. (2001). Trust, Control, and Risk in Strategic Alliances: An Integrated Framework. *Organization Studies*, *22*(2), pp. 251–283. http://doi.org/10.1177/0170840601222004

ENISA. (2006). *Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools*. Technical Department of ENISA Section Risk Management.

Felici, M., & Pearson, S. (2015a). Accountability and Security in the Cloud: *First Summer School, Cloud Accountability Project, A4Cloud*, Malaga, Spain, June 2-6, 2014, Revised Selected Papers and Lectures. In M. Felici & C. Fernández-Gago (Eds.), (pp. 3–42). Cham: Springer International Publishing. http://doi.org/10.1007/978-3-319-17199-9_1

Fisher, M. L., (1997). What is the Right Supply Chain for Your Product. *Harvard Business Review* 75, pp. 105 – 117.

FT Lexicon. (n.d.). Supply Chain Transparency Definition from Financial Times Lexicon. Retrieved May 11, 2016, from http://lexicon.ft.com/Term?term=supply-chain-transparency

Gadia, S. (2011). Cloud Computing Risk Assessment: A Case Study. *ISACA Journal* 4, 11–16. Retrieved from http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx

ISACA & CSA. (2015). Cloud Computing Market Maturity. *AN ISACA CLOUD VISION SERIES WHITE PAPER*, 1–12.

ISO 27005. (2011). BS ISO / IEC 27005: 2011 BSI Standards Publication Information technology — Security techniques — Information security risk management.

Kaliski-Jr, B. S., & Pauley, W. (2010). Toward Risk Assessment as a Service in Cloud Environments. *Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing*, 1–7.

Lamming, R. C., Caldwell, N. D., Harrison, D. A., & Phillips, W. (2002). Transparency in supply relationships: Concept and practice. *IEEE Engineering Management Review*, 30(3), pp. 70–76.

Lee Newcombe. (2012).*Securing Cloud Services: A pragmatic approach to security architecture in the Cloud*. IT Governance Publishing.

Leimeister, S., Riedl, C., Böhm, M., & Krcmar, H. (2010). The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks. *Proceedings of 18th European Conference on Information Systems ECIS 2010*, pp. 1–12.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems*, *51*(1), 176–189.

Microsoft. (2015). Trusted Cloud : Microsoft Azure Security, Privacy, and Compliance. Retrieved May 4, 2016 from http://download.microsoft.com/download/1/6/0/160216AA-8445-480B-B60F-5C8EC8067FCA/WindowsAzure-SecurityPrivacyCompliance.pdf.

New, S. (2009). Supply Chain Traceability and Product Provenance: Challenges for Theory and Practice. In: Sweeney, Edward, (ed.) *Supply Chain Management and Logistics in a Volatile Global Environment. Blackhall Publishing Ltd., Dublin. ISBN 9781842181775*

New, S., & Brown, D. (2012). The Four Challenges of Supply Chain Transparency. *European Business Review*, 1–7. Retrieved from http://www.europeanbusinessreview.com/?p=4082

Pearson, S., Tountopoulos, V., Catteddu, D., Sudholt, M., Molva, R., Reich, C., Lopez, J. (2012). Accountability for cloud and other future Internet services. *CloudCom 2012 - Proceedings: 2012 4th IEEE International Conference on Cloud Computing Technology and Science*, 629–632. http://doi.org/10.1109/CloudCom.2012.6427512

Pohlman, M. (2010). Using the CSA Control Matrix and ISO 27017 controls to facilitate regulatory compliance in the cloud. *Cloud Security Alliance*. Retrieved from http://docbox.etsi.org/workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/EMC_CSA_POHLMANN.pdf

Raj Samani. (2011). Common Assurance Maturity Model, 1–2. Retrieved May 12, 2016 from http://www.fstech.co.uk/fst/FSTech_Conference_2011/Common_Assurance_Maturity_Model_Raj_Samani.pdf

Reuven Cohen. (2013). New Cloud Computing Insurance Attempts to Solve Cloud Liability Concerns For Service Providers. Retrieved from http://www.forbes.com/sites/reuvencohen/2013/04/24/new-cloud-computing-insurance-trys-to-solve-cloud-liability-concerns-for-service-providers/

Sunyaev, A., & Schneider, S. (2013). Cloud Services Certification. *Communications of the ACM*, 56(2), pp. 33–36.

Talluri, S., Narasimhan, R., & Nair, A. (2006). Vendor performance with supply risk: A chance-constrained DEA approach. *International Journal of Production Economics*, 100(2), pp. 212–222.

Verbano, C., & Venturini, K. (2013). Managing Risks in SMEs: A Literature Review and Research Agenda. *Journal of Technology Management & Innovation*, 8(3), pp. 186–197.

Vijayan, J. (2015). Cloud Security: Transparency Is Crucial for Service Providers. Retrieved May 9, 2016, from http://www.cio.com/article/2925773/cloud-security/cloud-security-transparency-is-crucial-for-service-providers.html

Weber, R. H., & Staiger, D. N. (2014). Cloud Computing: A cluster of complex liability issues. *Web Journal of Current Legal Issues* 20 (1), pp. 1–13. Retrieved from http://webjcli.org/article/view/303/418

Werff, L. Van Der, Lynn, T., & Xiaong, H. (2014). Building Trust in the Cloud Environment: Towards a Consumer Cloud Trust Label. *ICDS 2014: The Eighth International Conference on Digital Society* Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=icds_2014_6_40_10104

Wisner, J. D., Tan, K.-C., & Leong, G. K. (2008). *Principles of Supply Chain Management - A Balanced Approach*. Cengage Learning.

Zhang, X. Z. X., Wuwong, N., Li, H. L. H., & Zhang, X. Z. X. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. *2010 IEEE 10th International Conference on Computer and Information Technology (CIT),* pp. 1328–1334. http://doi.org/10.1109/CIT.2010.501

APPENDIX 1: CASE STUDY

Payworq Ltd offers payroll-processing software (PayFruit), which runs as Software as a Service (SaaS). Its move to the cloud was due to an increased demand for PayFruit, from small businesses and start-ups. Payworq needed an Infrastructure-as-a-Service (IaaS) provider to host its growing service, and it looked for the cloud service providers (CSP) from provider websites and attending exhibitions and trade events. Eventually, it selected A400 Ltd on its promise of flexibility, rapid scalability, redundancy, pay-as-you-use, and compliance with standards. Leveraging A400's expertise for hosting infrastructure services, Payworq could now focus on its core competency, which is software development.

Recently, PayFruit suffered a downtime for approximately four hours as a result of a power outage at the A400's Internet Service Provider (ISP). The situation was very damaging for Payworq; several of its customers were unable to pay their staff on time, and it now faces financial penalties.

As part of its incident management process, Payworq has arranged a meeting with A400 to try to ensure that this incident does not happen again. It wants to know more about the 'supply chain' of other providers, which may lie behind A400's offering. They want to follow this up with a comprehensive risk assessment of the benefits and vulnerabilities of their cloud solution.

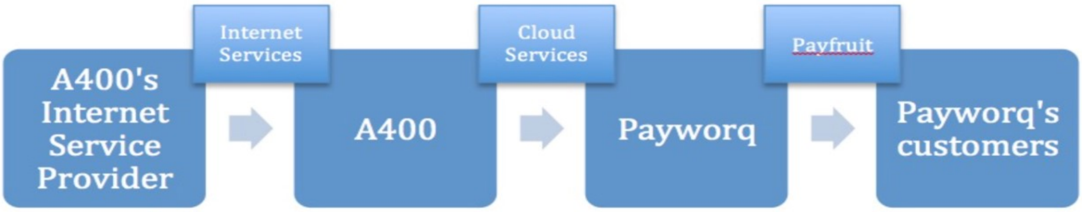

Figure 1 Payfruit Cloud Services Supply Chain.

Olusola Akinrolabuis a Cybersecurity DPhil student at the Department of Computer Science, University of Oxford. He obtained a BSc. (Honours) in Computer Science from Babcock University, Nigeria and also holds a Master's degree in Mobile and High-Speed Telecommunications Networks from Oxford Brookes University. His industry experience spans over 12 years, where he has worked in both computer network and security related roles. 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 effect of supply chain transparency in reducing cloud computing risks.

Steve New is an Associate Professor in Operations Management at Saïd 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. Steve completed his doctorate on the use of visual interactive modelling for decision support in manufacturing at Manchester Business School (MBS). He subsequently taught at the Manchester School of Management, UMIST (now merged with MBS), before joining Saïd Business School in 1996. He has taught extensively on a wide range of Executive Education and Degree Programmes, and previously served as Vice Dean of the school. Steve has published over 35 refereed articles, with most of his research focusing on supply chain management and quality improvement, with his work appearing in journals ranging from the *Harvard Business Review* to the *British Medical Journal*. Much of his work is inter-disciplinary, and he collaborates extensively with colleagues from across disciplines.