Stakeholders in the cloud computing value-chain

A socio-technical review of data breach literature

David Kolevski
School of Computing and Information Technology
University of Wollongong
NSW, Australia
Email: dk616@uowmail.edu.au

Katina Michael
School for the Future of Innovation in Society
Arizona State University
Phoenix, Arizona
Email: katina.michael@asu.edu

Roba Abbas
School of Management, Operations and Marketing
University of Wollongong
NSW, Australia
Email: roba@uow.edu.au

Mark Freeman
School of Computing and Information Technology
University of Wollongong
NSW, Australia
Email: mfreeman@uow.edu.au

2020 IEEE International Symposium on Technology and Society (ISTAS) | 978-1-6654-1507-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/ISTAS50296.2020.9462169

***Abstract*—This paper is about stakeholders in the cloud computing value-chain. Early cloud computing literature focused on the technical aspect of the technology and viewed the provider and customer as essential value-chain stakeholders. The more users that use cloud services, the potential for data breaches increases. The review of the literature was carried out using a social-technical approach. Socio-technical theory encapsulates the social, technical and environmental dimensions of a system. The outcomes of the search indicated that there are two pertinent stakeholder types: operational and non-operational. Operational stakeholders include cloud providers, customers, enablers, resellers and third-party providers. Non-operational stakeholders include regulators, legislators, courts, non-government organisations, law enforcement, industry-standard bodies and end-users. The end-users are critically important in the cloud value-chain in that they rely on online services for everyday activities and have their data compromised. The cloud value-chain presents that cloud services encapsulate more than just technology services. The paper considers the complex stakeholder relationships and data breach issues, indicating the need for a better socio-technical response from the stakeholders within the value-chain.**

Keywords—stakeholders, cloud computing, data breach, ecosystems, value-chain, socio-technical, operational, non-operational, end-users, literature review

I. Introduction

The last decade has seen the rapid adoption of cloud computing services from everyday users (i.e. end-users) and businesses (i.e. cloud consumers). Traditional enterprise networks that were managed by internal information technology (IT) departments have been superseded by data centres storing and processing end-user and business data. Earlier cloud computing studies focused on the promise that outsourcing storage and processing requirements to the cloud (i.e. cloud providers) would achieve beneficial attributes. However, the simplistic representation of cloud stakeholders does not portray the unique, complex and interactive nature of cloud services. For example, the cloud resembles the cloud consumer (i.e. business) and the cloud provider and ignore the end-users that utilize the service. Take, for instance, Microsoft's Azure cloud service, the millions of cloud customers offering storage, e-mail and office-suite applications to their end-users is often not factored. The aim of this paper is to review the stakeholders within the cloud computing model using a socio-technical approach. The value chains of emerging technologies have been previously studied. Abbas [1] and Abbas et al. [2] conducted a value chain analysis of location-based services using socio-technical systems theory in the discovery of the interplay between direct and indirect stakeholders and users. This paper will use a similar approach but applied to cloud computing.

II. Defining Ecosystems and Value-Chains

Before defining cloud computing in the context of an ecosystem or value-chain, it is important to understand the level of interaction between stakeholders. In its broadest definition, a digital ecosystem is "an interactive system established between a set of active agents and an environment within which they engage in common activities" [3]. In a later study, the term cloud computing ecosystem has emerged with the aim of exploring the roles of actors (i.e. organizations or institutions) and their service offerings [4]. Floerecke and Lehner [5] define a role as a "set of similar services offered by market players to similar customers." While the term ecosystem is coupled with the intention that actors define their own "space", the cloud environment cannot function and be operational without a supporting ecosystem. Briscoe and Marinos [6] state that cloud computing systems are open systems that include virtualized resources. The authors also outline three agents (vendors, developers and end-users), with each potentially having multiple roles. While Briscoe and Marinos [6] present an earlier encapsulation of cloud ecosystems, they outline essential agents within the business ecosystem context.

Alternately, the cloud computing literature has defined a set of stakeholders within the cloud value chain which interact to create business value and services. The cloud value chain is accountable for end-to-end support and service delivery and is situated at a higher abstraction level [7]. For example, rather than focusing on individual players within the cloud model, stakeholders are viewed as industry players, and a sudden stakeholder participant withdrawal would not compromise the representation of the cloud model [8]. The cloud value chain represents an end-to-end service that also combines the social, technical and environmental participants, particularly applicable to socio-technical systems. The cloud value chain allows stakeholders to be more accountable for their actions when a data breach

occurs. Therefore, cloud computing must be encapsulated using a generic value-chain to represent cloud data breaches issues. We proceed to present the cloud computing value-chain, a unique contribution to the literature.

A. The Generic Cloud Computing Value-Chain

In defining the stakeholders in the cloud computing value-chain, it is appreciated to review the relationships between stakeholders. As such, the value-chain presents a key component in understanding the dynamics of processing and storing end-user data. Fig. 1 presents two types of stakeholders, operational and non-operational. The figure also shows boundaries which are set for clarity and precedence of information flow.

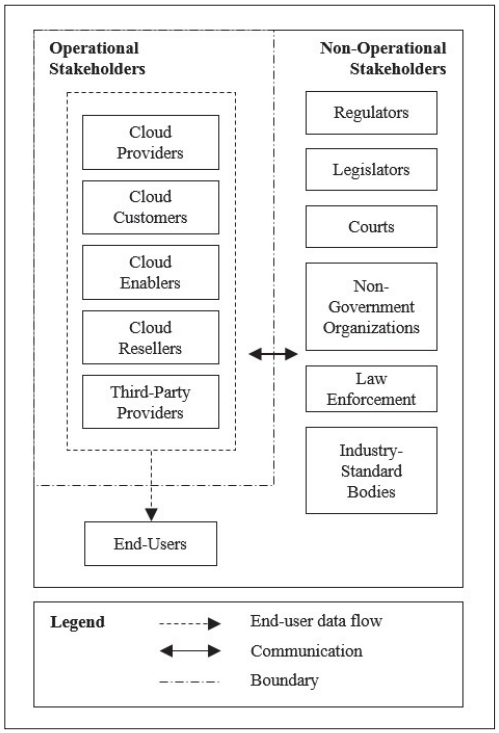

Fig. 1. Stakeholders in the cloud computing value chain

III. The Operational Stakeholders

This section will concentrate on the roles and responsibilities of operational stakeholders, particularly to cloud computing provisioning and administering. The roles of operational stakeholders in the context of delivering secure and sustainable data processing and storage facilities will be the common goal.

A. Cloud Providers, Customers and Enablers

In the context of cloud computing, cloud providers, customers, and enablers are an integral component of cloud service provisioning. In an early conceptualisation of cloud stakeholders, Buyya et al. [9] discuss that cloud providers (i.e. Amazon, Google and Microsoft) allocate service resources to cloud customers (i.e. enterprises). The focus here was on the interaction between the cloud provider and consumer and the advancements in cloud consumption. As more stakeholders participated in cloud computing services, so did the emphasis on cloud enablers and their role in delivering additional capacities to the cloud. For example, Martson et al. [8] embraced cloud providers and cloud customers but also embedded cloud enablers (i.e. CapGemini) and regulators in their cloud value-chain. While the latter study allowed for a more inclusive review of cloud stakeholders, they did not explicitly highlight end-users as stakeholders.

Several other studies have demonstrated that there are complexities associated with the cloud computing value-chain. Cloud computing services comprise a series of complex interactions with stakeholders collaborating to achieve the common goal of service consumption [10]. For example, we see the potential for complex interactions between stakeholders, integrated with unique environmental requirements [11]. We are also witnessing more cloud customers and end-users storing data through platforms such as social media, e-commerce, and other online services [12].

It is not until end-user data has been disclosed that anticipation of environmental implications is considered. These implications are magnified with cloud data breaches appearing on front-page news outlets and through court proceedings. The 2013 Target Corp. and 2017 Equifax, Inc. data breaches demonstrate not only the complex interactions between stakeholders but the impact of end-user's data, including personally identifiable information (PII) and financial information being disclosed [13] [14]. Regulators, legislators and the courts each have a role and responsibility to play in protecting end-user data now and into the future. Furthermore, it is imperative that through a cloud computing value-chain, privacy and trust relationships between stakeholders are established and maintained through secure provisioning and administering services.

B. Cloud Resellers and Third-party Providers

Tschider [15] points out that cloud resellers and third-party providers are essential stakeholders in the value-chain in they allow cloud computing service integration between multiple cloud providers and have an extensive network of service resources. In this paper, resellers and third-party providers share similar characteristics, but each has their unique roles to play. For example, resellers could offer their cloud computing services to both cloud customers and end-users and typically have a one-to-many stakeholder relationship. On the other hand, third-party providers have many-to-many relationships with cloud providers and cloud customers. They offer system integration services and as more complex infrastructure continues to be developed, so does the need for this service offering. Similarly, Kandira, Mtsweni and Padayachee [16] note that third party providers play a significant role in provisioning between different cloud services. In a later study, Bouchaala et al. [17] state that third-party providers also play a role in carrier services network operations. The studies highlighted that resellers and third-party providers should be viewed at a higher level of abstraction and focus on system integration.

IV. The Non-Operational Stakeholders

This section will focus on the non-operational stakeholders and their role in ensuring cloud computing services are relevant, secure and transparent to others within

the value chain. These stakeholders are central to the guidance and support to others within the value chain.

A. Regulators and Legislators

Regulators may not be the ideal stakeholder when adopting emerging technologies, but they allow regulation to direct secure and transparent methods of data interchange. It is also foreseeable that technology outpaces other aspects of regulatory intervention. However, it is the role of the regulator to intervene when technology does evil to the users, through no fault of their own. This generally occurs post-technology development, and we are at a stage where cloud computing services are reaching a tipping point in data breach cases. Adrian [18] examines the role of regulators in cloud computing services and data breach cases and states that they play an important part in protecting end-user data. Similarly, King and Raja [19] determine that, along with privacy and security experts, regulators are key players within the cloud domain. Regulators intend to provide cloud providers and other relevant cloud stakeholders a framework to conduct cloud computing services [20].

Another relevant stakeholder is legislators and their focus on defining and constructing laws. They resemble and form a government within a particular jurisdiction (i.e. council, county, state and federal governments). Newman [21] examines the U.S. Congress' failed attempts in passing data breach notification (DBN) legislation. Similarly, Tschider [15] reviews U.S. state DBN legislations and notes that difficulty in passing comprehensive legislations lies within legislators. The studies portray the constrain in developing relevant legislation for cloud computing services within the U.S. Legislators play a critical part in constructing data protection laws within the cloud value-chain.

B. Courts

Several studies highlight the role of the courts within the cloud value-chain. In one study, Braunstein [22] reviews a U.S. Supreme Court case, *Clapper v. Amnesty International, 568 U.S. 398*, in that the court determined the plaintiff (i.e. end-user) did not sustain sufficient injury and did not have Article III standing. Similarly, Mank [23] reviews several high-profile data breach cases in the U.S. district and circuit courts, including P*isciotta v. Old National BanCorp., 499 F.3d 629* and *Galaria v. Nationwide Mutual Insurance Co., 663 F.3d 384*. The two data breach cases introduced a mixed response, in that the former case granted in favour of the plaintiff, while the latter case, denied the plaintiff Article III standing. As such, the role of courts in data breach cases bring a sense of uniqueness and end-user empowerment. However, the significant point in defining the court as a stakeholder is that end-users affected by a data breach go to courts for outcomes.

C. Non-government Organisations, Law Enforcement and Industry Standard Bodies

Other studies highlight non-government organisations (NGOs), law enforcement and industry-standard bodies as important stakeholders providing guidelines on privacy and security requirements. NGO's are neither part of nor controlled by governments and typically share the best interest for improving the needs of the end-users. Concerning law enforcement, agencies provide breached organisations (e.g. cloud customers or cloud providers) guidance on the investigative processes. Berghel [14], and Manworren, Letwat and Daily [13] state that law enforcement thus can participate in investigations and provide resources; otherwise, the breached entity does not hold. It is important to note that industry-standard bodies define, develop and coordinate technical standards that organisations can adopt [24].

D. End-users

Perhaps, the least emphasis is given to the cloud customer's customer (i.e. end-user) as a vast number of studies only portray cloud providers and cloud customers as essential stakeholders in the value-chain. In this study, end-users are non-operational stakeholders. End-users, in effect, provide their information to initialise a service using the cloud customer's portal. They also use cloud services with or without knowing they are even using cloud services. As cloud services began to permeate government and private-sector businesses, end-users were not adequately defined, or at least discussed significantly, the way they use the technology. That is, what constitutes a cloud end-user and what role do they play in cloud value-chain.

It is not until studies focusing on data breaches or even in a greater extent, actual data breaches that have caused havoc or harm to end-users, will they be seen as important stakeholders that cannot be left out of the cloud value-chain. For example, Manworren, Letwat and Daily [13] summarize the 2013 Target Corp. data breach and explicitly define that end-users' are vulnerable to identity (ID) theft. Similarly, Berghel [14] summarises the 2017 Equifax Inc. data breach that caused havoc to over 147 million end-users. Braunstein [22], Rotenberg and Jacobs [25], and Kolevski and Michael [26] have examined data breaches and the implications it has had on end-users. They acknowledge that without the proper guidance and support from non-operational stakeholders, the data breach problem will likely continue to increase. The studies summarizing data breaches not only provide a glimpse into real-world scenarios, but they also factor end-users as essential stakeholders in the value chain.

V. Conclusion

This paper has given an insight into a more comprehensive cloud computing value-chain, incorporating operational and non-operational stakeholders. It also has scratched the surface concerning stakeholder engagement in cloud data breaches; however, there interactions and relationships are continually evolving. There are two principle outcomes. The first outcome is that cloud computing encapsulates more than technology stakeholders. As more cloud providers, customers and end-users adopt cloud services, the more transparent it has become that cloud computing is more than technology. Cloud computing services and the underlying systems encapsulate other important roles such as end-users, the driving force behind consumption and the tasks and processes required for functionality. The same cloud computing service designed to produce better performance, scalability and reliability is evolving, and with this, so has the social implications of the technology. The value-chain is adapting to the context, and the likes of NGOs, law enforcement, industry-standard bodies, regulators, legislators and the courts are responding. The second outcome is that end-users, e.g. consumers or citizens should be considered cloud computing stakeholders.

The more that data breaches occur, the more evident it is that end-users are part of the cloud computing value chain.

A. Future Research

Interestingly, there is an assumption that there are incremental changes to the value-chain, adding more and more stakeholders to the mix as new technologies and services emerge. Other stakeholders are not highlighted within the generic cloud value chain and literature but provide essential functions. Future studies can also focus on employees of cloud providers and other organizations that use cloud services. Investors, shareholders or owners of cloud computing companies are other stakeholders that could be considered valid in a given context. The open-source community is another important stakeholder due to most cloud instances running open source applications, as are citizen scientists known to utilize state of the art technologies. Given that most underlying cloud infrastructure hardware is sourced from dozens of countries, specialized hardware providers could also be considered valid stakeholders. These stakeholders hold important tasks for the operation of cloud services; however, each poses security issues that cannot be ignored.

REFERENCES

[1] Abbas, R, Location-based services (LBS) regulation in Australia: a socio-technical approach, thesis, University of Wollongong, 2012. https://ro.uow.edu.au/theses/3666.

[2] Abbas, R, Michael, K, and Michael, M (2014), "The regulatory considerations and ethical dilemmas of location-based services (LBS) : A literature review", Information Technology & People, Vol. 27 No. 1, pp. 2-20. https://doi.org/10.1108/ITP-12-2012-0156.

[3] Sabry, N & Krause, P 2012, 'A digital ecosystem view on cloud computing', in 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 1-6.

[4] Floerecke, S, Lehner, F & Schweikl, S 2020, 'Cloud computing ecosystem model: evaluation and role clusters', Electronic Markets.

[5] Floerecke, S & Lehner, F 2016, 'A Revised Model of the Cloud Computing Ecosystem', in Cham, pp. 308-321.

[6] Briscoe, G & Marinos, A 2009, 'Digital ecosystems in the clouds: Towards community cloud computing', in 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies, pp. 103-108.

[7] Mohammed, AB, Altmann, J & Hwang, J 2010, 'Cloud Computing Value Chains: Understanding Businesses and Value Creation in the Cloud', in D Neumann, M Baker, J Altmann & O Rana (eds), Economic Models and Algorithms for Distributed Systems, Birkhäuser Basel, Basel, pp. 187-208.

[8] Marston, S, Li, Z, Bandyopadhyay, S, Zhang, J & Ghalsasi, A 2011, 'Cloud computing - The business perspective', Decision Support Systems, vol. 51, no. 1, pp. 176-189.

[9] Buyya, R, Yeo, CS, Venugopal, S, Broberg, J & Brandic, I 2009, 'Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility', Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616.

[10] Wang, L, Pires, LF, Wonbacher, A, van Sinderen, MJ & Chi, C 2010, 'Stakeholder interactions to support service creation in cloud computing', in 14th IEEE International Enterprise Distributed Object Computing Conference Workshops, Vitória, Brazil, pp. 173-176.

[11] Maxim, M 2015, 'The rights and obligations of the main stakeholders in cloud computing services', Perspectives of Business Law Journal, vol. 4, no. 1, pp. 190-203.

[12] Rastogi, N, Gloria, MJK & Hendler, J 2015, 'Security and Privacy of Performing Data Analytics in the Cloud', Journal of Information Policy, vol. 5, pp. 129-154.

[13] Manworren, N, Letwat, J & Daily, O 2016, 'Why you should care about the Target data breach', Business Horizons, vol. 59, no. 3, pp. 257-266.

[14] Berghel, H 2017, 'Equifax and the Latest Round of Identity Theft Roulette', Computer, vol. 50, no. 12, pp. 72-76.

[15] Tschider, CA 2015, 'Experimenting with privacy: Driving efficiency through a state-informed federal data breach notification and data protection law', Tulane Journal of Technology & Intellectual Property, vol. 18, no. 1, pp. 45-82.

[16] Kandira, M, Mtsweni, J & Padayachee, K 2013, 'Cloud security and compliance concerns: Demystifying stakeholders' roles and responsibilities', in 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), pp. 653-658.

[17] Bouchaala, M, Ghazel, C, Saidane, LA & Kamoun, F 2017, 'End to End Cloud Computing Architecture Based on A Novel Classification of Security Issues', in 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), pp. 303-310.

[18] Adrian, A 2013, 'How much privacy do clouds provide? An Australian perspective', Computer Law & Security Review, vol. 29, no. 1, pp. 48-57.

[19] King, NJ & Raja, VT 2012, 'Protecting the privacy and security of sensitive customer data in the cloud', Computer Law & Security Review, vol. 28, no. 3, pp. 308-319.

[20] Daly, A 2018, 'The introduction of data breach notification legislation in Australia: A comparative view', Computer Law & Security Review, vol. 34, no. 3, pp. 477-495.

[21] Newman, BV 2015, 'Hacking the current system: Congress' attempt to pass data security and breach notification legislation', University of Illinois Journal of Law, Technology & Policy, vol. 2015, no. 2, pp. 437-460.

[22] Braunstein, A 2015, 'Standing up for Their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing', Journal of Law and Policy, vol. 24, no. 1, pp. 93-130.

[23] Mank, BC 2017, 'Data breaches, identity theft, and Article III standing: Will the supreme court resolve the split in the circuits?', Notre Dame Law Review, vol. 92, no. 3, pp. 1323-1368.

[24] Borenstein, N & Blake, J 2011, 'Cloud Computing Standards: Where's the Beef?', IEEE Internet Computing, vol. 15, no. 3, pp. 74-78.

[25] Rotenberg, M & Jacobs, D 2013, 'Updating the law of information privacy: The new framework of the European Union', Harvard Journal of Law & Public Policy, vol. 36, no. 2, pp. 605-652.

[26] Kolevski, D & Michael, K 2015, 'Cloud computing data breaches a socio-technical review of literature', in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, pp. 1486-1495.