Cybersecurity and Data Quality in Cloud Computing: A Research Framework

Hongjiang Xu(✉)

School of Business, Butler University, 4600 Sunset Avenue, Indianapolis, IN 46208, USA
hxu@butler.edu

Abstract. In the cloud computing environment, cybersecurity and data quality capacities and vulnerabilities can have impact on could computing performance. Cloud computing resiliency addresses risks and capabilities in order to make cloud computing stronger and less susceptible to disruptions. Cloud computing provides many opportunities, however, it also presents some cybersecurity and data quality issues. In this paper, we propose a research framework for cybersecurity and data quality in the cloud computing environment.

Keywords: Cybersecurity · Cloud Computing · Data Quality · Risks · Capabilities

1 Introduction

More and more systems are operating in the cloud computing environment. Cloud computing brings many benefits as the same time presents many challenges and issues. Particularly in regards to cybersecurity. Organizations' cybersecurity and data quality capacity and vulnerability will likely to have impact on how their systems can operate in the cloud computing environment.

Cybersecurity has some unique features compare to traditional IT security. The effectiveness and efficiency of traditional IT security protection mechanisms are being reconsidered, as the characteristics of cloud computing deployment model differs widely from the traditional architectures (Ramachandra, Iftikhar, & Khan, 2017; Zissis & Lekkas, 2012). Cybersecurity have impact on cloud computing performance (Xu & Mahenthiran, 2021).

Ensure data quality (DQ) is one of the primary job for information systems. The output and decision making will be impacted by poor quality information from the system. There are many measurements for information quality (Strong, Lee, & Wang, 1997; Xu, Horn Nord, Brown, & Daryl Nord, 2002). Systems operate in cloud computing cannot achieve overall effectiveness without good quality of data (Almutiry, Wills, Alwabel, Crowder, & WaIters, 2013), such as cloud-based health information systems, and cloud ERP.

Taking all of this into consideration, this paper aims to answer the following research question: What is the influence of cybersecurity and data quality on cloud computing resiliency? To do that, in the next sections we provide a theoretical background of from the fields and propose a research framework.

M. Papadaki et al. (Eds.): EMCIS 2022, LNBIP 464, pp. 201–208, 2023.
https://doi.org/10.1007/978-3-031-30694-5_15

2 Theoretical Background

2.1 Cybersecurity

Cybersecurity is a critical aspect for cloud computing and supply network. When more and more computing and supply chain network, data storage, and transactions moved from the traditional local hosted hardware and software to the cloud, the cyber space, there are potentially many cybersecurity threats and vulnerabilities.

One the cybersecurity concerns is that the large amount of data stored in the cloud, including critical information, which would attract highly skilled hackers who would want to steal the information for unauthorized users for financial gains (Srinivasamurthy, Liu, Vasilakos, & Xiong, 2013). The cybersecurity is even more critical when a business has sensitive information such as intellectual property, trade secrets, and personally identifiable information about their customers, employees, and suppliers that make security breaches a significant cost to the firms (Kamara & Lauter, 2010). Cybersecurity concerns are one of the major barriers to the adoption of cloud computing (Chen & Zhao, 2012). Therefore, to manage costs, organizations must learn to manage the cybersecurity and privacy risks (Kamara & Lauter, 2010), and learn how to deal with cybersecurity threats and try to manage and reduce the cybersecurity vulnerabilities.

Cybersecurity in the cyber space works differently than the normal IT security due to the potential threats coming from the cyber space, which makes it harder to *prevent, detect and respond to the cyber-attacks.* However, many of the general IT security theories still apply. Such as one of the basic and major security concerns is data security, it is also true in cybersecurity. Cybersecurity requires high level of protection of information.

There are many reasons for the vulnerability of cybersecurity, such as unauthorized access or breach into the system, capacity to store data in comparatively small space, complexity of code, negligence (Ani, 2011). There are also many technologies organizations can implement to help ensure cybersecurity. Such as: 1. Vulnerability scanners. 2. Intrusion prevention system. 3. Intrusion detection system. 4. Network and application firewall (Razzaq, Hur, Ahmad, & Masood, 2013).

2.2 Data Quality

The quality of information in any type of the systems is as important as the security for the information. As the data quality control theory of Garbage-in garbage-out (GIGO) is true for all information systems. Cloud computing is not an exception. There are many factors that impact data quality of the system. Those factors are in few categories: information systems characteristics, data quality characteristics, organizational factors, stakeholders' related factors and external factors (Xu, 2013).

To ensure high quality information, the measurements of quality of data need to be understood and used. Information quality problem pattern concept has been used to measure date quality in different type of systems (Xu et al., 2002). DQ problem patterns include:

- Intrinsic DQ pattern: multiple sources of same data, questionable believability, judgement involved in data production, questionable objectivity, poor reputation, and little added value, leading to data not used.

- Accessibility DQ pattern: lack of computing resources, poor accessibility, access security, interpretability and understandability, concise and consistent representation, amount of data, and timeliness, leading to barriers to data accessibility.
- Contextual DQ pattern: operational data production problems, changing data consumer needs, incomplete data, poor relevancy, distributed computing: inconsistent representation, and little value added, leading to data utilisation difficulty (Strong et al., 1997).

2.3 Cloud Computing

Cloud computing is one of the trends in the recent years, and many more businesses are joining it, but the theory for data quality and cybersecurity management in cloud computing is still weak. Many businesses are moving toward cloud by force or try to follow the new development, or catch up with their peers and competitors, without fully understand the implications of such action. Many risks associated with cloud computing, especially the data quality and cybersecurity issues need to be understood, and studied. The capacity of the cybersecurity might have impact on the cloud computing's performance (Xu & Mahenthiran, 2021).

The effectiveness and efficiency of traditional IT protection mechanisms are being reconsidered, as the characteristics of cloud deployment model differs widely from the traditional architectures (Ramachandra, Iftikhar, & Khan, 2017; Zissis & Lekkas, 2012). Cloud computing has three deliver models, which are infrastructure as a service (IaaS) that is multi-tenant cloud layers are provided by the service provider and shared with contracted clients, cloud platform as a service (PaaS) where the cloud provider provisions not just the operating system but also provides a development stack (e.g., a database), and cloud software as a service (SaaS) model that provides the complete application stack (e.g., cloud based accounting system) (Ramachandra et al., 2017). And these three delivery models can be deployed either as a private cloud, public cloud, or hybrid cloud. Currently, it is generally believed that small and medium size firm users (SMEs) require services more in the area of offering infrastructure and SaaS, because they do not have the necessary skills, time or resources to setup an application ecosystem and manage it (Khan & Al-Yasiri, 2016). There needs to be research that systematically examining the system development life cycle (SDLC) for cloud consumers to incorporate various technological advancements to improve security at a very fundamental level. Additionally, research need be done in regards to what are the impact of cybersecurity and information quality on cloud computing resiliency.

Cloud computing resiliency addresses risks and capabilities in order to make cloud computing stronger and less susceptible to disruptions. Cloud computing provides many opportunities, however, it also presents some cybersecurity and data quality issues.

3 The Research Framework

In order to prevent and reduce cybersecurity threats and vulnerabilities, there are a few areas of cybersecurity that we are interested in investigating: cyber data security in cloud computing, budget and investment for cybersecurity, security policy, and the human

aspect of information security. Cloud computing is defined as applications delivered as services over the Internet and data centers provide those services (Armbrust et al., 2010). Cybersecurity is one of the major concerns, as cloud computing enables the migration of system processing and data storage to the cloud, which increased the number of potential cyberattacks (Drew, August 2012). Therefore, it is important to understand the security and privacy risks in cloud computing and develop appropriate solutions for it to be successful (Takabi, Joshi, & Ahn, 2010). Security is implicit within the capabilities of cloud computing. There are many issues and concerns regarding cybersecurity. For example, one of the cybersecurity concerns for cloud computing is who is responsible for the security: is it solely the storage provider's responsibility, or it is also on the entity that leases the storage for its applications and data? (Kaufman, 2009).

3.1 Research Questions

In this paper, we propose a research framework on cybersecurity and data quality's impact on the resiliency of cloud computing. In particular, the objectives of the study is try to answer the following research questions:

(1) Does a higher level of awareness of the cybersecurity issues in firms lead to better cybersecurity risk management policies for cloud computing,
(2) Does better cybersecurity policies lead to higher level of cloud computing resiliency,
(3) What are the impact of cybersecurity and data quality vulnerabilities to cloud computing resiliency?

We develop two hypotheses for this question as following:

H1: Cybersecurity vulnerabilities have negative influence on cloud computing resiliency.
H2: Data quality vulnerabilities have negative influence on cloud computing resiliency.

(4) What are the impact of cybersecurity and data quality capabilities to cloud computing resiliency?

We develop two hypotheses for this question as following:

H3: Cybersecurity capabilities have positive influence on cloud computing resiliency.
H4: Data quality capabilities have positive influence on cloud computing resiliency.

3.2 Research Framework

We propose a research framework for cybersecurity and data quality for cloud computing resiliency as follows (Fig. 1):

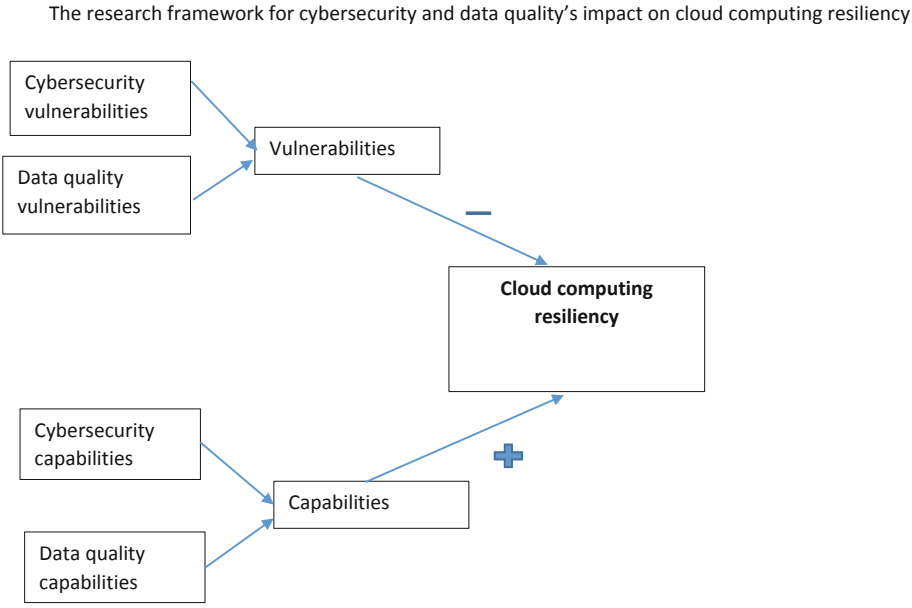

Fig. 1. The proposed research framework for cybersecurity and data quality for cloud computing resiliency

3.3 Proposed Items

To address the research questions, we propose a list of items to be used for assessment. Those items are based on the existing literature, and prior studies. Some of the other measurement items will come from established or tested instruments developed from the related research and practical fields.

Cybersecurity and DQ in Cloud Computing (Capability)

1. Cloud computing provider's ability to protect the *integrity* of my firm's data is high.
2. Cloud computing provider's ability to protect the *confidentiality* of my firm's data is high.
3. Sharing of cloud computing provider's server with other firms' is of great concern.

4. The cloud computing techniques provide sufficient security transfer channel during the process of mass data interchange.

Budget and Investment for Cybersecurity (Awareness)

1. More and faster digitization means an increase in digital attack surface and potential for harm to the business. For relatively high-likelihood, high-impact threats, do your company have adequate investments addressing these threats?
2. Regarding your organization's current cyber budget and processes, how confident are you with regard to the following?

    a. Includes process monitoring the effectiveness of our cyber program against the spending on cyber
    b. Linked to overall enterprise or business unit budgets in a strategic, risk-aligned, and data-driven way
    c. Allocated towards the most significant risks to the organization
    d. Focused on remediation, risk mitigation, and/or response techniques that will provide the best return on cyber spending
    e. Integrated with decisions on capital requirements needed in the event of a severe cyber event
    f. Adequate digital trust controls over emerging technologies for security, privacy, and data ethics

3. Have your company tested resilience plans for a wider range of threats?

Security Policy (Policies)

1. Are there appropriate Security Policy, Guidelines or Procedures established?
2. Is the existing Security Policy/Guidelines/Procedures adequately enforced?
3. Are users informed of their obligation with regard to the relevant laws, security policy and procedures before being granted access rights?
4. Is the use of strong/complex password policy enforced?
5. Is the use of two-factor authentication enforced for access control?

Human Aspect of Information Security (Vulnerability)
Do employees of the company do any of the following?

Internet use

- Installing unauthorized software
- Accessing dubious websites

- Inappropriate use of internet

Social networking site (SNS) use

- Amount of work time spent on SNS is too much
- No award of the consequences of SNS
- Posting about work on SNS

Incident reporting

- Reporting suspicious individuals
- Reporting bad behavior by colleagues
- Reporting all security incidents

Mobile computing

- Physically securing personal electronic devices
- Sending sensitive information via mobile networks
- Checking work email via free network

Information handling

- Disposing of sensitive documents
- Leaving sensitive material unsecured

4 Significance

There is limited research on cybersecurity data quality's impact on cloud computing resiliency in the cloud environment, thus our research objectives begin to address this gap.

From the existing literature, it is not clear if a firm that is not aware of its cybersecurity- threats can effectively manage authentication, authorization, data confidentiality, data integrity and non-repudiation concerns of a cloud user wanting to employ a cloud provider. Hence, the first objective of the study is to assess whether a higher level of awareness of the cybersecurity issues in firms lead to better risk management policies for cloud computing. Future research can include collecting data to further test and valid the proposed research framework. The other research objectives can be achieved by using the empirical data to answer the research questions, and test the research hypotheses.

The research framework proposed in this paper is going to make theory contributions by providing a theoretical model to fill the current research gap in cybersecurity and data quality's influence on cloud computing resiliency in cloud computing environment. As for the managerial implications, the future research that build on the research framework of this paper will provide findings that will help businesses to understand the cybersecurity and data quality issues better for cloud computing management, which many of the businesses and managers still have difficulty comprehend.

References

Almutiry, O., Wills, G., Alwabel, A., Crowder, R., WaIters, R.: Toward a framework for data quality in cloud-based health information system. Paper presented at the International Conference on Information Society (i-Society 2013) (2013)

Ani, L.: aCybercrime and national security: the role of the penal and procedural law. Law and Security in Nigeria, 200–202 (2011)

Chen, D., Zhao, H.: Data Security and Privacy Protection Issues in Cloud Computing. Paper presented at the 2012 International Conference on Computer Science and Electronics Engineering (2012)

Goud, N.: Cyber Attack on Tower Semiconductor. Cybersecurity Insiders. http://www.cybersecurity-insiders.com/cyber-attack-on-tower-semiconductor/ (2020)

Kamara, S., Lauter, K.: Cryptographic cloud storage. Paper presented at the Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization (2010)

Khan, N., Al-Yasiri, A.: Identifying cloud security threats to strengthen cloud computing adoption framework. Paper presented at the the 2nd International Workshop on Internet of Thing: Networking Applications and Technologies (IoTNAT'2016) (2016)

Ramachandra, G., Iftikhar, M., Khan, F.A.: A comprehensive survey on security in cloud computing. Procedia Comput. Sci. **110**, 465–472 (2017). https://doi.org/10.1016/j.procs.2017.06.124

Razzaq, A., Hur, A., Ahmad, H.F., Masood, M.: Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial ap- plications. Paper presented at the 2013 IEEE Eleventh International Symposium on Auton- omous Decentralized Systems (ISADS) (2013)

Schneier, B.: The US has suffered a massive cyberbreach. It's hard to overstate how bad it is. The Guardian. Available at: https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols (2020)

Srinivasamurthy, S., Liu, D.Q., Vasilakos, A.V., Xiong, N.: Security and privacy in cloud computing: a survey. Parallel Cloud Comput. **2**(4), 126–149 (2013)

Strong, D.M., Lee, Y.W., Wang, R.Y.: Data quality in context. Commun. ACM **40**, 103–110 (1997)

Xu, H.: Factor Analysis of Critical Success Factors for Data Quality. Paper presented at the AMCIS (2013)

Xu, H., Horn Nord, J., Brown, N., Daryl Nord, G.: Data quality issues in implementing an ERP. Ind. Manag. Data Syst. **102**(1), 47–58 (2002). https://doi.org/10.1108/02635570210414668

Xu, H., Mahenthiran, S.: Users' perception of cybersecurity, trust and cloud computing providers' performance. Inform. Comput. Secur. **29**(5), 816–835 (2021). https://doi.org/10.1108/ICS-09-2020-0153

Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Gener. Comput. Syst. **28**(3), 583–592 (2012). https://doi.org/10.1016/j.future.2010.12.006