Issues in Information Systems
Volume 24, Issue 2, pp. 275-281, 2023

DOI: https://doi.org/10.48009/1_iis_2021_124

Cybersecurity and data quality's impact on cloud ERP

Hongjiang Xu, *Butler University, hxu@butler.edu*
Mark Hwang, *Central Michigan University, hwang1m@cmich.edu*

Abstract

Cloud Enterprise Resource Planning (CERP) systems have become increasingly popular in recent years. The data quality in any type of the systems is important, from traditional systems to cloud based systems. It is particularly critical for CERP systems because of the highly integrated nature of CERP systems. Cybersecurity is a critical aspect of CERP. When more and more data storage, transactions are moved from the traditional local hosted hardware and software to the cloud, the cyberspace, there are potentially many cybersecurity threats and vulnerabilities. In this research, we will explore the capabilities of data quality and cybersecurity's impact on the use and benefits of CERP systems, as well as the potential negative effects of data quality and cybersecurity vulnerabilities on the CERP performance outcomes. We propose a research model for cybersecurity and data quality's impact on CERP.

Keywords: cybersecurity, data quality, cloud ERP

Introduction

Cloud Enterprise Resource Planning (CERP) systems have become increasingly popular in recent years, offering organizations the ability to manage their business processes and data in cloud computing environment and a centralized and efficient manner. However, the benefits of CERP have proven elusive. For example, a recent PwC survey found that only about 10 percent of the respondents witnessed significant business benefits realized at the companies they worked for (PwC, 2023). It is not surprising that some organizations are considering bringing some of their data and applications back to traditional systems (Linthicum, 2023). The quest for finding the success factors for the use and benefits of CERP continues. In this paper, we will focus on the effect of data quality and cybersecurity on the use and benefits of CERP.

Data quality (DQ) refers to the usefulness of the data and information, and could include DQ dimensions such as, accuracy, completeness, timeliness, consistency, and reliability of the data. Poor data quality can have a range of negative effects, including decreased business performance, increased costs, and decreased trust in the system. On the other hand, high-quality data is essential for the effective functioning of CERP systems, enabling organizations to make informed decisions and improve their business processes.

Data security refers to the measures in place to protect sensitive information from unauthorized access or misuse. For the cloud computing environment, it includes both traditional data security, and cybersecurity. In the context of CERP systems, data security is particularly important due to the sensitive nature of the information being stored and processed, as well as the increasing threat of cybercrime. Poor cybersecurity can lead to data breaches, which can have significant financial and reputational consequences for organizations.

Therefore, in this research, we will explore the capabilities of data quality and cybersecurity's impact to the use and benefits of CERP systems, as well as the potential negative effects of data quality and cybersecurity vulnerabilities to the CERP performance outcomes. Our aim is to provide organizations with a better understanding of the critical role that data quality and cybersecurity play in the success and measurements of CERP systems' performance, and to highlight the need for organizations to prioritize these issues.

Data Quality

The data quality in any type of the systems is important, from traditional systems to cloud based, from small, medium to large systems. It is particularly critical for CERP systems because of the highly integrated nature of CERP systems. As one of the very basic of the data quality control theories of Garbage-in garbage-out (GIGO) is true for all types and sizes of information systems.

Cloud ERP is not an exception. There are many factors that impact data quality of the system. Those factors are in a few categories: information systems characteristics, data quality characteristics, organizational factors, stakeholders' related factors and external factors (Xu, 2013).

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

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

- Accessibility DQ: 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: operational data production problems, changing data consumer needs, incomplete data, poor relevancy, distributed computing: inconsistent representation, and little value added, leading to data utilization difficulty (Strong et al., 1997).

Data Security

Cloud security is a broad topic that encompasses governance, risk management, and compliance (GRC) and controls (Al-Anzi et al., 2014). Data security has been a major challenge since the early days of cloud computing (Liu et al., 2020a, Liu et al., 2020b). It remains a top concern even with the widespread use of CERP. For example, Şener et al.,(2016) found that security and privacy as the most significant technological factor in cloud ERP adoption decisions. Nguyen and Luc (2016) similarly found perceived risk having a significant effect on the intention to use, which in turn had a significant effect on business benefits of CERP.

More recently, a 2022 survey of 140 corporations found that 65 percent of the companies were using CERP while the rest were not (Panorama, 2023). The top three reasons cited by non-users were security breach, followed by data loss and connectivity issues. The same factors were investigated using a sample of small- and medium-sized firms in India. Compliance was found a significant factor in successful CERP implementation, but security and network issues were not (Gupta, and Misra, 2016).

A more recent survey found that a dedicated organizational unit in charge of GRC that has a close working relationship with the cloud vendor is a distinctive characteristic of "cloud-powered companies" that are reaping business benefits from CERP (PwC, 2023).

Cybersecurity

There are many types of cyber-attacks would make the CERP vulnerable. One of the cybersecurity concerns is that the large amount of critical data stored in the cloud, which would attract highly skilled hackers who would want to steal the information for unauthorized users for financial and other types of gains (Srinivasamurthy et al., 2013).

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 cyberspace works differently than the normal IT security due to the potential threats coming from the cyberspace, which makes it harder to prevent, detect and respond to the cyberattacks. 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. In fact, cybersecurity requires an even higher level of protection of information, as in the cyberspace, there are additional cyber related vulnerabilities and threats that are not of concerns for a local based traditional system.

The fight between cyberattacks and cybersecurity prevention, detection, and response is like a never-ending war between the intrusion and protection of the integrity of the data and systems. There are many causes for vulnerabilities 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 can be implemented to help ensure cybersecurity. Such as: 1. Vulnerability scanners. 2. Intrusion prevention system. 3. Intrusion detection system. 4. Network and application firewall (Razzaq et al., 2013).

The Research Model

The purpose of this research is to investigate the effect of data quality and cybersecurity's capabilities and vulnerabilities on the use and performance of CERP. We hope the findings from the study will help companies realize the potential benefits of CERP more effectively. The proposed research model is shown in Figure 1.

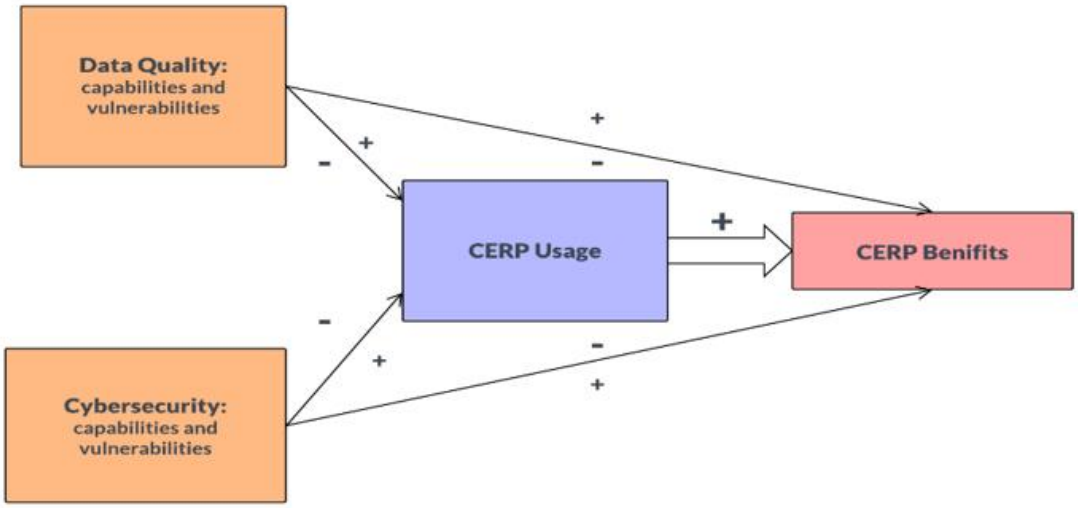

Figure 1: Data Quality and Cybersecurity's Impact on the Use and Benefits of CERP

CERP System Usage

ERP systems can be used for a range of different business functions, including accounting, procurement, human resources, inventory management, production, and project management. In general, ERP systems are designed for use by a range of different users across an organization, from executives and managers to line-level employees. However, the specific usage of an ERP system can vary widely based on the user's job function and level within the organization. Nevertheless, the aggregate usage of an ERP system is an important indicator of systems success, and factors that enhance or inhibit usage have been extensively investigated.

For example, Salih and colleagues (2012) explored eight factors that contributed to user resistance in post ERP implementation. On the other hand, Salih and colleagues (2022) studied night factors that led to user acceptance of the use of ERP systems. Chang and colleagues (2008) examined several factors and found three to have a significant effect on ERP system usage. Similarly, Nwankpa (2015) found ERP system usage was a function of three factors. Tsai and colleagues (2010) examined the relationship between business process reengineering and the success of ERP implementation, with system usage as one of the success measures. Nguyen and Luc (2016) focused on the intention to use CERP and found it was related to several factors including system quality, information quality, and perceived risk.

System use or usage is an important systems success measure that is often included as a dependent variable in IS implementation studies. Another reason for examining system usage is its relationship with another commonly studied dependent variable, system benefits. The linkage between system usage and system benefits has been confirmed in many prior studies (e.g., Nwankpa, 2015; Ram et al, 2013). However, as mentioned previously, business benefits are hard to realize in practice (PwC, 2023). For example, an often-cited advantage of CERP is lower costs. However, companies are discovering that costs of CERP can be high and therefore are either repatriating back to their traditional systems (Linthicum, 2023) or forgoing CERP altogether (Panorama, 2023). In other words, even if some benefits such as cost savings cannot be linked to system usage, it is still important to show system usage as a standalone measure of systems success.

CERP System Benefits

System benefits are the beneficial outcomes realized from the use of a system. Organizational performance, business process performance and other terms have been used to describe various benefits, which can manifest in more efficient core business processes including sales, delivery, and customer service (Ram et al., 2013; Hasan et al., 2019). Efficiency in turn can result in lower costs and even higher revenue. System benefits can also be attributed to the use of cloud service providers rather than inhouse staff for systems development. Potential benefits include rapid development, lower development costs, greater availability and accessibility, and scalability (Elmonem et al, 2016).

The scope of an ERP implementation is also a factor in the realization of system benefits, with wider scope generally associated with greater benefits (Ha and Ahn, 2014). This can happen when more modules are implemented and hence more business processes are integrated, resulting in more efficiency in the system. A related factor is the degree of integration among the ERP and other systems both internally and externally to the organization.

Ram et al., (2013) found that system integration has a positive effect on organizational performance. As more modules are implemented or more systems are integrated with the ERP, the usage of the ERP increases, which further boosts system benefits. On the other hand, system benefits in some cases are not a direct result of system usage. For instance, a data breach can wreak havoc on the finances and reputation of the firm regardless how its ERP system was used. The perceived risk of CERP has been found an inhibitor of adoption (Chang, 2020; Nguyen and Luc, 2016). Consequently, the direct effect of security and data quality on system benefit should be examined, in addition to their indirect effect.

Methodology

The initial research model proposed in the paper will guide us through the development of a survey instrument to use for the next step of the study. We plan to conduct a large-scaled survey and use empirical data to investigate the validity of our research model. Results of data analysis can help to provide some insights and recommendations for practice. We will design the survey questionnaire based on the existing literature from the related fields as discussed in the previous sections. We will also have a pilot testing of the survey to help make necessary modifications to the instrument, before we send it out to the larger group of targeted respondents. The respondents would be IT professionals that have had experiences or knowledge of cybersecurity, cloud computing and CERP.

After data collection, we will performance statistical data analysis from the survey to see whether our proposed research model is supported. We will conduct descriptive and inferential data analysis.

Conclusion

The move to cloud computing offers organizations a chance to run their core business processes in the cloud. Using a CERP provides many potential benefits, but it also comes with multiple challenges. Inhibitors to the adoption and use of CERP can dampen the realized business benefits or even cause unexpected damages. Therefore, the effects of data quality and cybersecurity capacities and vulnerabilities on the CERP performance need to be understood. We developed an initial research model of the impact of data quality and cybersecurity on CERP. The next step of our research project is to design, develop a survey

questionnaire, and conduct a large-scaled survey of the professionals in the related fields. The analysis of the results will help us gain insight of all the components of our research model. Thus, our research will make theoretical and managerial contributions to the related fields of data quality, cybersecurity and CERP.

References

Al-Anzi, F.S., Yadav, S.K. and Soni, J. (2014). Cloud computing: Security model comprising governance, risk management and compliance. International Conference on Data Mining and Intelligent Computing (ICDMIC), Delhi, India, 2014, pp. 1-6, doi: 10.1109/ICDMIC.2014.6954232.

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

Chang, Y. (2020). What drives organizations to switch to cloud ERP systems? The impacts of enablers and inhibitors. Journal of Enterprise Information Management, 33, 3, 600-626.

Chen, D., & Zhao, H. (2012, 23-25 March 2012). Data security and privacy protection issues in cloud computing. Paper presented at the 2012 International Conference on Computer Science and Electronics Engineering.

Elmonem, M.A., Nasr, M.S., Geith, M.H. (2016). Benefits and challenges of cloud ERP systems – A systematic literature review. Future Computing and Informatics Journal, 1, 1–2, 1-9.

Gupta, S., and Misra, S. C. (2016) Compliance, network, security and the people related factors in cloud ERP implementation. International Journal of Communication Systems. 29(8), 1395– 1419.

Ha, Y., and Ahn, H.J. (2014). Factors affecting the performance of Enterprise Resource Planning (ERP) systems in the post-implementation stage. Behaviour & Information Technology, 33, 1065 - 1081.

Hasan, N., Miah, S.J., Bao, Y., & Hoque, M.R. (2019). Factors affecting post-implementation success of enterprise resource planning systems: a perspective of business process performance. Enterprise Information Systems, 13, 1217 - 1244.

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

Linthicum, D. (2023). 2023 could be the year of public cloud repatriation. InfoWorld. Available at https://www.infoworld.com/article/3684369/2023-could-be-the-year-of-public-cloud-repatriation.html

Liu, J., Shen, H., Chi, H., Narman, H.S., Yang, Y., Cheng, L. and Chung, W. (2020a). A low-cost multi-failure resilient replication scheme for high-data availability in cloud storage. IEEE/ACM Transactions on Networking, 29, 4, 1436-1451.

Liu, L., Chen, R., Liu, X., Su,J. and Qiao,L.(2020b). Towards practical privacy-preserving decision tree training and evaluation in the cloud. IEEE Transactions on Information Forensics and Security, 15, 2914-2929.

Nguyen, T.D., Luc, K.V.T. (2018). Information Systems Success: Empirical Evidence on Cloud-based ERP. In: Dang, T., Küng, J., Wagner, R., Thoai, N., Takizawa, M. (eds) Future Data and Security Engineering. FDSE 2018. Lecture Notes in Computer Science (), vol 11251. Springer, Cham.

Panorama. (2023) The 2022 ERP Report. Available at https://www.panorama-consulting.com/resource-center/erp-report/

PwC. (2023). PwC's 2023 Cloud Business Survey. Available at https://www.pwc.com/us/en/tech-effect/cloud/cloud-business-survey.html

Ram, J., Corkindale, D., and Wu, M. (2013). Implementation critical success factors (CSFs) for ERP: Do they contribute to implementation success and post-implementation performance? International Journal of Production Economics, 144, 1,157-174.

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, 6-8 March 2013). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. Paper presented at the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS).

Salih, S.H., Abdelsalam, S., Hamdan, M., Ibrahim, A.O., Abulfaraj, A.W., Binzagr, F., Husain, O., & Abdallah, A.E. (2022). The CSFs from the Perspective of Users in Achieving ERP System Implementation and Post-Implementation Success: A Case of Saudi Arabian Food Industry. Sustainability.

Salih, S.H., Hussin, A.R., & Dahlan, H.M. (2012). User resistance factors in post ERP implementation.

Şener, U., Gökalp, E., Eren, P.E. (2016). Cloud-Based Enterprise Information Systems: Determinants of Adoption in the Context of Organizations. In: Dregvaite, G., Damasevicius, R. (eds) Information and Software Technologies. ICIST 2016. Communications in Computer and Information Science, vol 639. Springer, Cham. https://doi.org/10.1007/978-3-319-46254-7_5

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

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

Xu, H, (2013) "Factor Analysis of Critical Success Factors for Data Quality" AMCIS 2013 Proceedings., Chicago, IL. https://aisel.aisnet.org/amcis2013/DataQuality/GeneralPresentations/1

Xu, H., Horn Nord, J., Brown, N., & Daryl Nord, G. (2002). Data quality issues in implementing an erp. Industrial management & data systems, 102(1), 47-58. doi:10.1108/02635570210414668

Yang, P., Xiong, N. and Ren,J. (2020), "Data security and privacy protection for cloud storage: a survey", IEEE Access, Vol.8 No.2,pp.131723-131740.