Research on the Capability Maturity Model of Data Security in the Era of Digital Transformation

Zimeng Gao[1], Fei Xing[1(✉)], and Guochao Peng[2]

[1] Suzhou Institute of Trade & Commerce, Suzhou 215009, China
921820868@qq.com
[2] Sun Yat-sen University, Guangzhou 510000, China

Abstract. Digital transformation has become the trend of enterprise operation in the digital economy era. In this context, data security has become the focus of academic research and industrial circles. This paper aims to develop an enterprise data security capability maturity model in the era of digital transformation. Firstly, systematic literature review (SLR) was used to build up the hierarchical model of enterprise data security, which consists of three first level indicators and twelve second level indicators. Secondly, expert interview was used to develop the capability maturity model of data security with five different maturity levels. In the end, a series of suggestions was put forward to improve enterprise data security, namely: 1) Daily maintenance is required for computer and network security; 2) Physical safety protection to avoid safety accidents caused by environmental factors; 3) Establish a complete monitoring and automatic response mechanism; 4) Enterprise data disaster tolerance measures can systematically ensure security.

Keywords: Data security · Capability maturity model · Digital transformation · Recommendation

1 Introduction

With the rapid development of digital economy, enterprises comply with the development trend of digital economy and use emerging technologies to carry out digital transformation. Enterprise digital transformation is essentially the integration of unified digital technologies across a business. From startups to multinationals, these technologies change and optimize the way a company deploys and manages its everyday operations [1]. As a result of digital transformation, the operation mode of enterprise is changing stupendously. One of the most obvious changes is to enhance the data collection in the process of enterprise digital transformation [2]. Specifically, many enterprises have accumulated a lot of data about consumers, but the real advantage comes from analyzing these data to promote enterprise business development. Therefore, digital transformation provides a mechanism to capture the right data and fully integrate it to achieve a higher level of business insight.

A. Moallem (Ed.): HCII 2023, LNCS 14045, pp. 151–162, 2023.
https://doi.org/10.1007/978-3-031-35822-7_11

In the wave of digital transformation, data security has become a hot topic of concern in academia and industry due to the rapidly growing amount of data. Manita et al. (2020) considered that 'He who gets the data gets the world' [3]. Mergel et al. (2019) assumed that data is the 'gold' or 'oil' in the development of digital transformation, which is becoming the core asset of enterprise [4]. Since the significance of data security in enterprise digital transformation, there are many research results exploring it. On one hand, one of the most popular research fields are about the advantages brought by digital transformation from a macro perspective [3, 5]. Academic researchers have demonstrated the huge benefits that digital transformation brings to enterprise through theoretical and empirical studies. Besides, case analysis of digital transformation in different fields has also been investigated by academic scholars [6, 7]. On the other, researchers have made a lot of investigations in data security, mainly from the view of technology, such as tools [8], platforms [9].

However, it is worth noting that the research of studying the data security of enterprise digital transformation is scarce. Particularly, current literature and studies showed that most studies in this field focus on the advantages of digital transformation and technical angles of data security [9]. There is little research studying the combination of data security in era of digital transformation, especially in terms of data security capability maturity. Enterprise can effectively understand their data security protection capabilities in their process of digital transformation through the development of data security capability maturity model. Therefore, this paper aims to identify the indicators that affect the data security and maturity levels.

The rest of the papers is structured as follows. First, systematic literature on digital transformation and capability maturity model are presented. Subsequently, research methods namely systematic literature review and expert interview are introduced. Then, we will discuss the hierarchical model enterprise data security and capability maturity model. In the final, several suggestions on how to improve enterprise data security are put forward.

2 Literature Review

2.1 Related Studies on Digital Transformation

The digital transformation, otherwise called 'digitalization' is defined today rarely in the literature. Our literature review showed that the digital transformation is defined as a social phenomenon or cultural evolution [2], and for enterprise as an evolution of their business or operation model. In fact, it is perceived as a fundamental transition of society, driven by digital technologies such as big data, machine learning, deep learning, and even artificial intelligence. These so-called digital technologies are deeply rooted in their culture and daily practices. In this context, enterprise need to adapt themselves by changing their business pattern.

However, it is biased that regard digital transformation simply as a business mode of the enterprise, because it affects other elements of an organization like culture, organizational structure, etc. In academic research, although there is no unified concept of enterprise digital transformation, important consensus has been reached on some key

elements [10]. On one hand, enterprise digital transformation is the reshaping of enterprise business activities through using advanced information technologies. Enterprise fully utilizes the new generation of digitalization and intelligence technologies to optimize the business process and management system and realizes the transformation of the organizational structure and the innovation of the business model by formulating a comprehensive enterprise digitalization strategy [11]. On the other hand, the core of enterprise digital transformation is to realize value co-creation. Enterprises can ensure their ability to obtain competitive advantages and sustainable growth in the fierce market competition by changing the operation mode [12].

2.2 Related Studies on Capability Maturity Model

The Capability Maturity Model (CMM) was first formally put forward by the Software Engineering Research Institute (SEI) of Carnegie Mellon University in 1991. It is used for the evaluation and improvement of software development process and software development capability [13]. It is an integrated model of system engineering and software engineering with organization. Academic researchers have applied the ideas and methods of CMM to the field of project management, such as enterprise information security maturity [13], enterprise intelligent manufacturing maturity [14] and enterprise intellectual property management maturity [15]. In addition to software management and project management, the basic ideas and methods of CMM can also be widely applied to the process management of other organizations like university, hospital, and governments, etc. As a result of this, the existing literature showed that CMM has been adopted and applied in a large number of organizations.

2.3 Related Studies on Data Security Capability Maturity Model

In the wave of enterprise digital transformation, data is becoming the core asset or even the 'lifeline' of enterprises. The importance of data security is self-evident. The data security capability maturity model standard, which focuses on the security of the six data life cycle processes of collection, transmission, storage, processing, exchange and destruction, providing a basic model framework for the maturity of the organization's data security capability [15]. The existing literature showed that the enterprise data security maturity model is mainly embodied in three aspects: security capability, capability maturity level and data security process [16]. In the dimension of security capability, the existing research mainly uses organizational construction, institutional processes, technical tools, as well as the safety awareness and related capabilities of data security personnel as the measurement indicators [16]. In terms of capability maturity level of enterprise data security, its maturity model is mainly divided into five levels. In the final, the data security process mainly focuses on the data life cycle process and the data security process dimension evaluation index composed of 11 general security process areas such as data security policy planning, authentication, and access control.

Existing researchers have conducted extensive and in-depth research on the maturity of enterprise data security and have achieved many research results. However, digital transformation enterprise has not taken into account, considering the unique features of the digital transformation enterprises, their maturity model construction is different

from other enterprises. At the same time, digital transformation enterprises are the development direction of enterprises in the digital economy era. Therefore, there is of great theoretical and practical significance to study the data security maturity model of digital transformation enterprises.

3 Research Methods

In this study, systematic literature review (SLR) and expert interview (EI) were adopted to develop the evaluation indicators and enterprise data security capability maturity model respectively.

3.1 Systematic Literature Review

Systematic Literature Review (SLR) is a research method based on the analysis of existing literature. Unlike traditional literature analysis, systematic literature analysis method follows a rigorous and systematic literature research route [17]. It uses clear definitions to identify evidence related to research issues (i.e., past research results), and screens the literature through quality evaluation criteria. The systematic literature analysis method mainly includes four research steps: defining the scope of literature inspection, querying the initial literature, selecting relevant literature, and analyzing the selected literature data [18].

Firstly, this paper mainly selects research documents in the field of data security and capability maturity model from Scopus, ScienceDirect, SpringerLink, Web of Science, Wiley Online Library, Google Scholar and two Chinese databases namely CNKI and Wan fang. Secondly, Boolean operators were used to link the search terms in the selected database through three fields of title, summary, and keywords, which produced the initial relevant literature. Thirdly, according to the principle of literature selection and exclusion, 317 articles were excluded from the original 809 articles through the repeatability of the title and the content of the abstract. In this case, a total of 492 papers were selected as the research samples of this paper. Finally, the selected literature was coded and analyzed to develop the evaluation indicators of capability maturity model of data security.

3.2 Expert Interview

The expert interview is one of the most frequently used methods in empirical social research. It provides exclusive insights into expert knowledge and into structural contexts as well as change processes of action systems [19]. The aim of the expert interview is to discover the unknown, a person's 'insider knowledge'. Basically, expert interview will involve two or more people [20]. Mostly between the interviewer and the interviewee and the interviewer asks questions while the interviewee replies to them. Therefore, conducting expert interview helps the researcher get specific information about a specific study area.

In this study, a total of 12 experts were interviewed in the meeting room. Twelve experts come from different field such as computer, data science, enterprise management, information system, etc. Each interview lasted 40–60 min and all experts were booked in advance. Moreover, the expert interview data were analyzed through content analysis.

4 The Proposed Capability Maturity Model of Data Security

4.1 Hierarchical Model of Enterprise Data Security

After conducting the systematic literature review, hierarchical model of enterprise data security was built up, which consists of three first level indicators and twelve second level indicators. In general, data security capability of enterprise in the era of digital transformation was affected by three dimensions, namely platform risk, enterprise behavior and external risks. To be specific, platform risk mainly refers to information system defects, network protocol defects, physical environment defects, privacy security settings and hacker stealing. The risk of enterprise data storage platform will affect data security. Once there is a certain risk in the system, external hackers are easy to attack, resulting in data leakage. The existing literature showed 28% of enterprise data security problems are caused by system failures, including IT and business process failures.

Secondly, enterprise behavior refers to data security awareness, data security management system and data protection negligence. Data security awareness is one of the reasons that leads to the data leakage in the enterprise. Therefore, in order to improve enterprise data security capability, enterprises need to require internal personnel to abide by professional ethics, establish a prevention mechanism, and conduct regular safety training for employees. Lack of data privacy management system is also a major problem for the enterprise data security. Therefore, data privacy management system is also considered as the evaluating indicators to measure the capability maturity of data security in enterprise.

In the final, if platform risk and enterprise behavior are the internal evaluation index, external threat is the external dimension. In this paper, external threats primarily refer to destruction of intellectual property, policy impact, backward data security protection technology and data cross-border transmission protection. In details, data cross-border transmission protection refers to the enterprise is lack of security assessment and process control in the cross-border data transmission process, and the operation adopted is inconsistent with the internationally recognized transmission mechanism, that is, the enterprise does not have adequate security assurance in the data transmission process. The specific explanation of these indicators was demonstrated in Table 1 (Fig. 1).

Table 1. Enterprise data security evaluation indicators

First level indicator	Second level indicator	Description
Platform risk	Information system defects	Data security risk was caused by the incomplete software and hardware facilities of the computer, intentional destruction, and untimely updating, etc., leading to the difficulty in ensuring the database security

(*continued*)

Table 1. (*continued*)

First level indicator	Second level indicator	Description
	Network protocol defects	Defects of application, transport, network, data link and physical
	Physical environment defects	Defects of site selection, storage and surrounding environment
	Privacy security settings	Defects of various privacy security functions provided by the system for users in enterprise
	Hacker stealing	The enterprise is attacked by hackers due to the low security level of its cloud configuration, which leads to the theft of enterprise secret
Enterprise behavior	Data security awareness	The overall data security awareness of the enterprise, including the understanding of domestic and foreign data security regulations
	Data security management system	Relevant systems set by the enterprise for data security, including relevant training, confidentiality agreement, etc.
	Data protection negligence	Data loss or leakage due to negligence of enterprises in data security protection
External threats	Destruction of intellectual property	Threat and destruction of enterprise intellectual property rights caused by external behaviors
	Policy impact	Constraints and obstacles posed by domestic or foreign data security policies to enterprise data security behavior
	Backward data security protection technology	The data security technology used by enterprises is backward and it is difficult to resist external technical interference

(*continued*)

Table 1. (*continued*)

First level indicator	Second level indicator	Description
	Data cross-border transmission protection	The enterprise lacks security assessment and process control in the cross-border data transmission process, and the operation adopted is inconsistent with the internationally recognized transmission mechanism, that is, the enterprise does not have adequate security assurance in the data transmission process

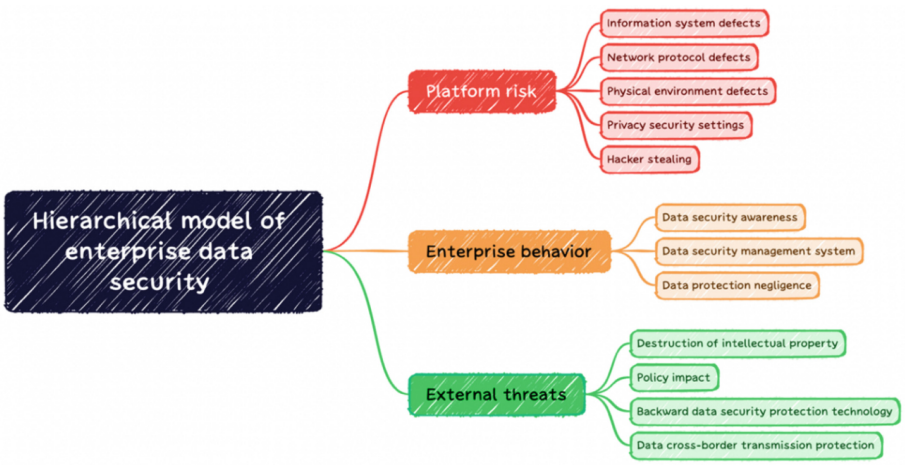

Fig. 1. Hierarchical model of enterprise data security

4.2 Capability Maturity Model of Data Security

The data was collected by expert interview, which contains of three categories of experts, namely computer science, enterprise management and information systems. Besides this, the collected interview data was analyzed through a thematic analysis. Consequently, the capability maturity model of data was developed, and it involves of five different maturity levels, namely planning level, informal implementation level, specification level, quantitative control level and leading level, the detailed explanation of capability maturity model of data security seen Table 2.

Table 2. Capability maturity model of data security

Name of level		Concept of level
Level 1	Planning level	The enterprise has realized the importance of data security and made a preliminary plan concentrate on data security, but no effective related work has been carried out
Level 2	Informal implementation level	Data security activities are being implemented, but these implementation activities are informal, and most of them are dependent on personal efforts and knowledge
Level 3	Specification level	The enterprise has invested on data security and some implementation activities are planned and tracked at the enterprise level
Level 4	Quantitative control level	The enterprise has established measurable data security management objectives. Enterprise can improve their actions through quantitative measurement
Level 5	Leading level	The enterprise has built up a smart data security management system, institutional processes and technical tools will continue to be adjusted independently to better adapt to business development

5 Recommendation

5.1 Daily Maintenance is Required for Computer and Network Security

The daily office and business activities of enterprise employees are inseparable from computers and networks, while Trojan viruses, harmful programs, security vulnerabilities, hacker attacks, etc. are all kinds of internal and external network threats. Therefore, it is difficult to guarantee the data security of enterprise in the era of digital transformation. Daily maintenance can be done from two dimensions.

Firstly, enterprise can improve the computer security protection capabilities. Nowadays, enterprise employees have recognized various risks from the network, but based on their past habits, they often ignore the impact on themselves, and even conflict with various security software and security measures [21]. The most simple and effective measures to protect computer security are to install enterprise antivirus software, update passwords regularly, update system patches regularly and other routine operations.

Secondly, enterprises can improve their network security protection capabilities. Common network security protection tools include firewall, network situational awareness, vulnerability scanning and intrusion detection system [22]. Firewall is the first barrier to prevent network sabotage. Network situational awareness equipment can help enterprises actively identify threats and risks in the company's network, and can cooperate with firewalls, intrusion detection systems, vulnerability scanning tools, etc. to

form a more three-dimensional network defense system to ensure the safe operation of enterprise networks and information equipment.

5.2 Physical Safety Protection to Avoid Safety Accidents Caused by Environmental Factors

Physical security protection is one of measures to protect data equipment and data system from earthquake, fire, flood and other environmental disasters and human error operation and destruction. In this paper, physical security protection contains of environmental safety protection and equipment safety protection.

Equipment security mainly refers to protecting the information equipment and facilities of enterprises from being damaged and stolen, especially every piece of equipment in the data center is valuable. If equipment is stolen or damaged by people, the losses caused by them will even far exceed the purchase value of the equipment itself. Traditional defensive measures can play an effective role in prevention, such as controlling personnel access through fingerprint identification, swiping card access control and other technologies.

In addition to the factors mentioned above, the safety of the equipment is also affected by itself. Safety accidents caused by defects in the design and manufacture of electronic equipment or normal aging are not uncommon in enterprises [23]. Although the availability of its functions can be guaranteed through regular maintenance and clustered deployment, the equipment that is far beyond the normal service life or has problems should be resolutely eliminated to ensure that the equipment is always in good working condition.

5.3 Establish a Complete Monitoring and Automatic Response Mechanism

According to the research conducted by Xing et al., about 65% of all data security incidents are caused by human factors, so the biggest risk of enterprise information security management is the security of internal personnel [11]. Safety accidents will be caused by personnel's operation mistakes, weak sense of responsibility, lack of professional ability or failure to strictly comply with relevant safety systems and operation procedures [24]. There are even internal personnel who maliciously destroy and tamper with enterprise information systems, data, and equipment due to dissatisfaction, or steal confidential information to obtain illegal profits. In this context, enterprise must do a good preparation work in personnel security management.

First, it is necessary to formulate and improve various safety rules and regulations, including disciplinary mechanisms, according to the current situation and requirements of different companies, and strictly implement and implement safety responsibilities. Secondly, data security publicity and education and training are often carried out to eliminate the resistance of security management among employees and make security awareness deeply rooted in the hearts of the people in their daily work. Moreover, it is necessary to clearly divide the responsibilities of personnel, allocate the authority according to the principle of minimization, and follow the principle of multiple people present for key operations.

5.4 Enterprise Data Disaster Tolerance Measures can Systematically Ensure Security

Data disaster recovery refers to a systematic project to protect the data from natural disasters and man-made damage and reduce the impact of disaster events on information systems and business processes. In the practice of enterprise data protection, two important safeguards are needed, namely data backup and disaster recovery center.

Data backup refers to the process of copying all or part of data to other storage media through backup software and corresponding backup strategies to prevent data loss. Backup is the basis of disaster recovery [25]. Enterprises backup data such as databases, documents, and system applications. In this way, data can be recovered quickly when the information system is damaged or lost.

As soon as completing the backup of the important data of the enterprise, it is also indispensable to check the integrity and validity of the backup data regularly, because it can detect whether the backup strategy is successfully implemented and whether the data can be truly restored. The disaster recovery center is a redundant node that establishes one or more data centers outside the production environment for disaster recovery. When a disaster occurs, the disaster-tolerant node can take over the system and business without being damaged, so as to achieve the goal of uninterrupted business. It can be said that the substantive purpose of the disaster recovery center is to ensure business continuity.

6 Conclusions

Data security is related to the sustainable development of enterprises in the network era. Data security management is conducive to improving the competitiveness of enterprises and is also an effective integration in the process of enterprise digital transformation. To ensure the data security of enterprises, it is to achieve the organic combination of internal management and external prevention and control. This paper aims to develop the hierarchical model of enterprise data security and the capability maturity model of data security in the era of digital transformation through the combination of systematic literature review and expert interview. Subsequently, capability maturity model of data security with five different maturity levels is built up. In the end, in order to improve the data security capability of enterprises in digital transformation, a series of suggestions was put forward to improve enterprise data security, namely 1) Daily maintenance is required for computer and network security; 2) Physical safety protection to avoid safety accidents caused by environmental factors; 3) Establish a complete monitoring and automatic response mechanism; 4) Enterprise data disaster tolerance measures can systematically ensure security.

References

1. Litvinenko, V.S.: Digital economy as a factor in the technological development of the mineral sector. Nat. Resour. Res. **29**(3), 1521–1541 (2020)
2. Verhoef, P.C., et al.: Digital transformation: a multidisciplinary reflection and research agenda. J. Bus. Res. **122**, 889–901 (2021)

3. Manita, R., Elommal, N., Baudier, P., Hikkerova, L.: The digital transformation of external audit and its impact on corporate governance. Technol. Forecast. Soc. Chang. **150**, 119751 (2020)
4. Mergel, I., Edelmann, N., Haug, N.: Defining digital transformation: results from expert interviews. Gov. Inf. Q. **36**(4), 101385 (2019)
5. Fenech, R., Baguant, P., Ivanov, D.: The changing role of human resource management in an era of digital transformation. J. Manage. Inf. Decis. Sci. **22**(2) (2019)
6. Piepponen, A., Ritala, P., Keränen, J., Maijanen, P.: Digital transformation of the value proposition: a single case study in the media industry. J. Bus. Res. **150**, 311–325 (2022)
7. Datta, P.: Digital transformation of the Italian public administration: a case study. Commun. Assoc. Inf. Syst. **46**(1), 11 (2020)
8. Thapa, C., Camtepe, S.: Precision health data: requirements, challenges and existing techniques for data security and privacy. Comput. Biol. Med. **129**, 104130 (2021)
9. Yang, P., Xiong, N., Ren, J.: Data security and privacy protection for cloud storage: a survey. IEEE Access **8**, 131723–131740 (2020)
10. Xue, L., Zhang, Q., Zhang, X., Li, C.: Can digital transformation promote green technology innovation? Sustainability **14**(12), 7497 (2022)
11. Xing, F., Peng, G., Wang, J., Li, D.: Critical obstacles affecting adoption of industrial big data solutions in smart factories: an empirical study in China. J. Glob. Inf. Manage. (JGIM) **30**(1), 1–21 (2022)
12. Gao, J., Zhang, W., Guan, T., Feng, Q.: Evolutionary game study on multi-agent collaboration of digital transformation in service-oriented manufacturing value chain. Electron. Commer. Res. 1–22 (2022)
13. Chapman, R.J.: Exploring the value of risk management for projects: improving capability through the deployment of a maturity model. IEEE Eng. Manage. Rev. **47**(1), 126–143 (2019)
14. Ge, J., Wang, F., Sun, H., Fu, L., Sun, M.: Research on the maturity of big data management capability of intelligent manufacturing enterprise. Syst. Res. Behav. Sci. **37**(4), 646–662 (2020)
15. Wu, J., Ma, Z., Liu, Z., Lei, C.K.: A contingent view of institutional environment, firm capability, and innovation performance of emerging multinational enterprises. Ind. Mark. Manage. **82**, 148–157 (2019)
16. Kim, S., Pérez-Castillo, R., Caballero, I., Lee, D.: Organizational process maturity model for IoT data quality management. J. Ind. Inf. Integr. **26**, 100256 (2022)
17. Xiao, Y., Watson, M.: Guidance on conducting a systematic literature review. J. Plan. Educ. Res. **39**(1), 93–112 (2019)
18. Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M.: Lessons from applying the systematic literature review process within the software engineering domain. J. Syst. Softw. **80**(4), 571–583 (2007)
19. Bogner, A., Menz, W.: The theory-generating expert interview: epistemological interest, forms of knowledge, interaction. In: Interviewing Experts, pp. 43–80. Palgrave Macmillan, London (2009)
20. Xing, F., Peng, G., Zhang, B., Li, S., Liang, X.: Socio-technical barriers affecting large-scale deployment of AI-enabled wearable medical devices among the ageing population in China. Technol. Forecast. Soc. Chang. **166**, 120609 (2021)
21. Kaufman, L.M.: Data security in the world of cloud computing. IEEE Secur. Priv. **7**(4), 61–64 (2009)
22. Kong, D., Dong, H., Li, H., Wang, Z., Li, J.: Research on situation analysis technology of network security incidents. In: Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, pp. 213–218 (2020)

23. Xing, F., Peng, G., Liang, Z.: Research on the Application of Blockchain Technology in the Cross-border E-Commerce Supply Chain Domain. In: Streitz, N.A., Konomi, S. (eds.) HCII 2022. LNCS, vol. 13326, pp. 99–109. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-05431-0_7
24. Fraga-Lamas, P., Fernández-Caramés, T.M.: A review on blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE Access **7**, 17578–17598 (2019)
25. Nabbosa, V., Kaar, C.: Societal and ethical issues of digitalization. In: Proceedings of the 2020 International Conference on Big Data in Management, pp. 118–124 (2020)