

Benefits of construction data risks management in the construction industry

Ornella Tanga Tambwe, Clinton Ohis Aigbavboa and
Opeoluwa Akinradewo

*CIDB Center for Excellence, Faculty of Engineering and the Built Environment,
University of Johannesburg, Johannesburg, South Africa*

Construction
data risks
management

Received 15 November 2022
Revised 20 March 2023
21 May 2023
Accepted 9 June 2023

Abstract

Purpose – Data represents a critical resource that enables construction companies' success; thus, its management is very important. The purpose of this study is to assess the benefits of construction data risks management (DRM) in the construction industry (CI).

Design/methodology/approach – This study adopted a quantitative method and collected data from various South African construction professionals with the aid of an e-questionnaire. These professionals involve electrical engineers, quantity surveyors, architects and mechanical, as well as civil engineers involved under a firm, or organisation within the province of Gauteng, South Africa. Standard deviation, mean item score, non-parametric Kruskal–Wallis H test and exploratory factor analysis were used to analyse the retrieved data.

Findings – The findings revealed that DRM enhances project and company data availability, promotes confidentiality and enhances integrity, which are the primary benefits of DRM that enable the success of project delivery.

Research limitations/implications – The research was carried out only in the province of Gauteng due to COVID-19 travel limitations.

Practical implications – The construction companies will have their data permanently in their possession and no interruption will be seen due to data unavailability, which, in turn, will allow long-term and overall pleasant project outcomes.

Originality/value – This study seeks to address the benefits of DRM in the CI to give additional knowledge on risk management within the built environment to promote success in every project.

Keywords Data management, Construction industry, Data risks

Paper type Research paper

1. Introduction

Van Besouw and Bond-Barnard (2021) mentioned that projects are growing more technically complicated, and there is a rising demand to accomplish them in the required time and cost frame. The key reasons behind this include competitive pressures and

© Ornella Tanga Tambwe, Clinton Ohis Aigbavboa and Opeoluwa Akinradewo. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>

The authors would like to thank the National Research Foundation (NRF) for funding this research study.



construction stakeholder expectations. [Adekunle et al. \(2022a, 2022b\)](#) and [Hendriyati et al. \(2022\)](#) stressed that one of the ways to stimulate project achievement and gain a competitive edge is through data management (DM). The construction industry (CI), according to [Tanga et al. \(2021a\)](#) and [Zha \(2023\)](#) is a sophisticated field that deals with a lot of data that comes from both on- and off-site and needs to be stored, kept carefully and distributed among all project members to enable a good project lifecycle. This same sector requires both the fourth industrial revolution tools building information modelling (BIM, cloud storage) to monitor the enormous amount of data that is exchanged among stakeholders, as well as data risks management (DRM) to stand and fight the data-related issues that come not only with the implementation of Industry 4.0 (cyber-attacks) but also with some financial risks, and human and natural disasters ([Zhao, 2023](#); [Rehman et al., 2022](#)). Although internet-related risks tend to dominate ([Tanga et al., 2022a](#)) in the present digitised world, there is a need to assess the benefits of all types of risks to promote more construction projects' success leading to more businesses. Several studies have talked about security risks associated with data in the sense of cyber-attacks ([Tanga et al., 2022a](#)), particularly in cloud computing ([Chen and Zhao, 2012](#)), DM risks ([Tanga et al., 2022b](#)) and supply chain risk management ([Pham et al., 2022](#)). Furthermore, [Tepeli et al. \(2021\)](#) focused on the development of multidimensional modelling to diminish risks in strategic and complex construction projects. Consequently, the research objective set for this study is to assess the benefits of DRM in the CI with a view to give additional knowledge on risk management within the built environment. This will keep professionals in the CI abreast of the advantages of using DRM in this digitalised world.

Construction project execution from inception to completion is strongly reliant on data for monitoring purposes. However, data usage also entails various risks such as loss, theft, corruption or misuse that can jeopardise the success of project delivery ([Sui Pheng et al., 2019](#)). Therefore, managing data risks is a crucial aspect of construction management that has not received adequate attention in the literature. While various studies focused on risk management in the CI, there are no research studies published on DRM specifically in the CI context. The novelty of this research lies in the identification and evaluation of the benefits of construction DRM in the CI. The study fills a gap in the body of knowledge by exploring the advantages of managing data risks and how it can enable the success of project delivery. Additionally, the study was conducted during the COVID-19 pandemic, which adds to its originality, as it sheds light on the benefits of DRM during a time when remote work and data access have become critical for project success.

The study is structured in various sections. The succeeding Section 2 gives a theoretical literature background on DRM and its identified benefits. Following this, Section 3 is the research methodology part, which focuses on the approach adopted to carrying out the research. Subsequently, Section 4 discussed the findings of the study, after which the two final sections including Section 5 and 6 dwelt on the conclusions and recommendations in line with the findings as well as the practical implications of the research respectively.

2. Theoretical background of data risks management

[Adekunle et al. \(2022a\)](#) put forward that information, data or document management is the process of creating, gathering, storing, distributing, retrieving, managing, monitoring and finally disposing of project or organisation data or information in a timely and accessible manner. This is to have complete control of project data, and enhance collaboration, therefore, any negligence from workers or absence to any of the DM results in data risks

(Cains *et al.*, 2021). Data risks incorporate both threats and vulnerabilities that can be natural, environmental, intentional or intentional actions from employees, cyberattacks, technical problems (software not responding), thus anything that can affect data. Among the threats, are unauthorised access to the information system, software and maintenance errors, human and natural disasters, manipulation of data, espionage, loss of support services, wrong data entry, vandalism and theft, terrorism, user error, earthquakes, loss of electricity supply, information leakage, all of which have affected many sectors, including the CI. The vulnerabilities include cybersecurity negligence on the physical (hardware, employee), internet and software level such as inadequate control of physical access, lack of backup system, uncontrolled use of information, non-protection of hardware, unmotivated, lack of workers training, uncontrolled download from the internet among others (Sultanate of Oman Information Technology Authority, 2017; Cains *et al.*, 2021; Talha *et al.*, 2019; Tanga *et al.*, 2022a; Zhao, 2023; Erfani *et al.*, 2023). All these can be cured via the installation of a DM process.

The DM process involves data governance (DG), which is the procedure of generating key performance indicators (KPIs), objectives and strategies, principles, policies, standards and rules to have control over project data. This involves identifying the decision-making bodies, decision rights, authority and responsibility to ensure that compliance is achieved (Yebenes and Zorrilla, 2019). Staunton *et al.* (2021) explained that DG is a method that aims to allow data to be used as wished while simultaneously preserving the data and the data subject. Therefore, this is the centre of DM because it enables data security in a long run. Data security and confidentiality management are not excluded from DM because they are means of protecting data from both physical theft and internet theft (Nourani *et al.*, 2022). This requires the use of closed-circuit television (CCTV), employment of security guards, data identification, locked file cabinets, data backup and control access through a strong password, which has to be updated more often. Also, the use of artificial intelligence (face recognition and fingerprint) with its fast fraud detection capabilities, as well as breach prediction will help to have continuous control of the system access (Nourani *et al.*, 2022; Nyamuchiwa *et al.*, 2022). Firewalls, encryption, virtual, antimalware and intrusion prevention systems are also used in data security (Staunton *et al.*, 2021). Data privacy and safety refer to sustaining the data's availability, integrity and confidentiality, as needed by the organisation (Zhang and Yuan, 2016). Staunton *et al.* (2021) stressed that data quality checking is another DM process. During this sub-element of DM, data quality is entitled to dimensions such as credibility, timeliness, completeness and accuracy constitute a part of management because the organisation receives all types of data (unstructured, structured and semi-structured), which includes data relevance, credibility, accuracy, efficiency, completeness, portability, traceability, consistency, availability, accessibility, confidentiality, compliance, precision, understandability, recoverability, timeliness and reliability. Data accuracy is defining whether the recorded or documented values are in accordance with the real value of data. In other words, this is ensuring the correctness (precision) of data. The timeliness of data is simply referring to the update of the measured values of the current work at hand. Furthermore, data completeness makes sure that no values are missing in the recorded value and also the breadth and depth are appropriate. Finally, the credibility of data reflects the source's and its content's trustworthiness (Khatri and Brown, 2010; Yebenes and Zorrilla, 2019). This step is very important because organisations receive all types of data unstructured, structured and semi-structured received during construction project executions.

From the discussion above, every organisation in the world, including the CI using the internet or not is exposed to data risks (Tanga *et al.*, 2021a; Zhao, 2023). Thus, it is important

to put in place a DRM system to fully reap benefits from digitalised business processes. The benefits are discussed as follows.

2.1 Promotes efficient financial management and reduces damage

To prevent the many cyberattacks that occur on online platforms, it is necessary to have different strategies and methods, as well as to understand how cyber attackers operate. These strategies or methods can help minimise, prevent and avoid the effects of cyberattacks on organisations (Dhillon, 2015; Bada and Nurse, 2020). Furthermore, the protection of private information on online platforms through various cybersecurity techniques in every industry in the world, including the CI must be a priority to avoid the consequences of these attacks. Some of these can be damages such as the loss of confidential information through a data breach, data leakage, usurpation, financial fraud, destruction of company reputation and image, sabotage, crash and computer freezing and reduction (Warren *et al.*, 2016; Bamigboye *et al.*, 2017; Arcuri *et al.*, 2017; Adekunle *et al.*, 2022a; Yaqoob *et al.*, 2021). Thus, it is necessary to have DRM measures in the construction companies to prevent money loss.

2.2 Reduces hardware and software damage

Tanga *et al.* (2022a) pointed out that construction companies may find it difficult to access saved papers or data, and take longer to recover the file resulting in the deadline missing which can be due to technical problems or cyberattacks. All of this can accumulate to the point where the company's software and hardware are destroyed, making it difficult to access the information, especially in the case of cyberattacks. This can happen when attacks like printed circuit board tampering, viruses and intellectual property infringement are coupled and not addressed and recognised (managed) in time. The reason why hardware is related to cybersecurity is that it has been used for a long time as a reliable component that supports the whole computer system. Furthermore, it is also considered an abstract layer, the main goal of which is to run the different instructions passed from the software layer (Preneel and Takagi, 2011). Thus, the hardware is linked to the software, and one of the key objectives of cybersecurity is the protection of software.

2.3 Promotes data privacy and protection

The adoption of cybersecurity is a valuable tool that responds to the data protection criterion, which is the safety of private data of all persons without exception, government and businesses. This implies that cybersecurity opposes the cybercriminals' mission, which is to manipulate personal data and penetrate government and business infrastructure (Yaqoob *et al.*, 2021). The mission of hackers involves finding a susceptible single point of susceptibility and data leakage to destabilise the good functioning of a system or project (Yaqoob *et al.*, 2021). Cybersecurity prevents private data of persons, government or construction business data misuse and prevents criminal activities by providing different security techniques and methods (Bamigboye *et al.*, 2017). Thus, adopting DRM is a good solution for the protection of data and keeping the privacy of confidential data.

2.4 Minimises dispute risk and promotes company reputation

Phishing is an electronic attack method where the intruder or hacker tries to falsify and steal the private information of legitimate users by imitating communications in an automated

fashion from a public or trusted company to steal private credentials (Attia *et al.*, 2016; Tanga *et al.*, 2022b), This may happen between client and contractor which can lead to misunderstanding, conflict and disputes (Dada, 2013; Rehman *et al.*, 2022). Thus, it is essential to make sure that DRM is applied to secure company information. In addition, Tepeli *et al.* (2021) stressed that when it comes to a company strategy, brand image (reputation), financial potential and economic viability, a department and a specific technique are needed throughout the project's life cycle to manage all types of risks. These risks do not exclude data risks.

2.5 Provides an appropriate risk approach to various attacks

The institute of engineering technology (2014) and Tanga *et al.* (2022a) emphasised that there needs to be effective cybersecurity by implementing appropriate mechanisms to deal with various attacks. These mechanisms involve strategies, such as security awareness and policies, business processes support, as well as technical solutions. Developing an appropriate data risk approach to responding to a cyberattack in a construction organisation will simplify its reaction to cyberattacks and save time and money, reduce stress and project failures (The institute of engineering technology, 2014; Tanga *et al.*, 2022b). After developing a data risk approach, it is important to ensure that the members of the construction organisation should carry out continuously, systematically, consciously and deliberately risk management across the whole project lifecycle. This will help the team to know that a cyberattack is likely to occur and remind them of the preparation in place to stop it from happening or to recover from an attack (Warren *et al.*, 2016; Tepeli *et al.*, 2021). Therefore, developing a good data risk approach will help the construction company to manage cyberattacks quickly, prevent unwanted money loss and decrease unnecessary stress.

2.6 Enhances integrity, confidentiality and availability

According to Buch *et al.* (2017) and Bhushan *et al.* (2021), cybersecurity (DRM) is intended to guarantee that the company's properties are secured, and the assets of users are achieved and preserved against relevant security dangers in cyberspace. Other aims of DRM are to ensure data availability, integrity, as well as confidentiality. The institute of engineering technology (2014) developed these aims by emphasising the word "integrity" in the management of data and noting that it involves computer-based systems and electronics' trustworthy operations, their software, all connected business processes, data authenticity and assurance, the legitimacy of transactions and their retention, their authentication, as well as non-repudiation. "Confidentiality" incorporates the monitoring and approval of access to the company's data or information. "Availability" includes information, data, processes and systems availability, whenever needed for protected and reliable design, as well as building project execution procedures and delivery. Moreover, it also covers reliability and resilience at the same time. The need to manage and improve from a series of failures is a perfect example of reliability and resilience (The institute of engineering technology, 2014; Zhang and Yuan, 2016; Tanga *et al.*, 2022a). Additionally, Tanga *et al.* (2022b) the lack of education or training can lead employees to compromise a computer programme or even share security measures secrets with outsiders who can easily steal and destroy the company's data. In addition, they can also click on a link sent to them via email, thus compromising the data integrity, confidentiality and availability. Thus, DRM is paramount for project data protection.

2.7 Enables a safe and productive construction environment

According to [Adekunle et al. \(2022a\)](#) and [Erfani et al. \(2023\)](#), the need of every construction company is to satisfy the client this can be achieved through improved services and information or DM. This is justified by the fact that the use of DRM will allow the continuous application of 4IR tools that are known to improve productivity on construction sites. This will encourage the organisation not to fear cyber risks and other human-related risks leading to stressful consequences such as exposing private workers and project information. In, addition DRM also protects the physical construction site, including the people working in it and data through the use of security cameras, security guards' agents, as well as locks ([Nyamuchiwa et al., 2022](#)).

2.8 Guarantees safety of project data

Construction projects involve the need for constant effective communication among different stakeholders to ensure better progress of work. Because this communication is often done using information communication technology (ICT) tools such as emails, BIM and excel sheets, it makes the CI a target for cyber attackers ([Attia et al., 2016](#); [Adekunle et al., 2022b](#)). [Yaqoob et al. \(2021\)](#) put forward that data challenges such as data traceability, flexible access, transparency, data provenance, trust, audit, security and privacy are encountered in many organisations. Fortunately, if companies decide to adopt DM through the use of blockchain due to its immutability nature, all the cited challenges are solved at once. [Al-Ajmi and Makinde \(2018\)](#) emphasised that DRM are necessary for the CI because it enables managers to detect, evaluate, analyse, monitor and respond to and track attacks on time. If threats are not detected in time on a construction project, it could give rise to a lot of exposure to the project's lifecycle, thereby affecting personal data ([Buch et al., 2017](#)).

2.9 Promotes good quality information

[Bishop \(2003\)](#) and [Adekunle et al. \(2022b\)](#) noted that with the numerous data attacks and the absence of DM, it is hard to maintain good data quality and competitive advantage. As intruders delete, modify or steal the data contained in the information system they directly affect the quality of data in terms of completion and accuracy ([Bishop, 2003](#); [Bendovschi, 2015](#)). [Adekunle et al. \(2022a\)](#) explained that in the construction environment, handling information or data is a better way to enable accurate and reliable choices in appropriate time. These choices are based on the quality of the data. According to [Khatri and Brown \(2010\)](#), data or information is of good quality when it is complete and free of modifications and deletion or other data-twisting processes. For [Tanga et al. \(2022a\)](#), data quality is an important aspect of DRM in every organisation, including construction projects for better project outcomes.

2.10 Promotes trust in project data

According to [Khalfan et al. \(2007\)](#) and [Yaqoob et al. \(2021\)](#), trust among stakeholders about project data is necessary for a successful project outcome. [Karlsen et al. \(2008\)](#) agreed with [Yaqoob et al. \(2021\)](#) that trust is a crucial tool when a group of people is working together, whether in the health care or construction sector because it promotes the communication of important information, as well as determines if a team is willing to allow others to contribute to their decision-making and even ensure that the intruder is not inside the team. For [Beslin and Reddin \(2004\)](#), the key to teamwork success is to win trust. All types of data need to be protected from any manipulation to prevent severe consequences that could harm the company. Because the intruder aims to manipulate the exchange of information between two individuals who believe there is no intermediate person between them, this can destroy trust among stakeholders.

2.11 Reduces physiological impact

Each phase or stage of a building project has its function, scope, cost frame and timeframe. As a result, many types of risks, including data risks and uncertainties are seen during the several phases of a construction project. There is, therefore, the necessity of developing an effective and transparent project delivery mechanism that allows all stakeholders to track project progress, as well as address the risks in every aspect of the project (Deep *et al.*, 2021; Rehman *et al.*, 2022). The lack of a clearly defined scope of a construction project, which is then followed by design, contracting, execution and project handover, is another crucial feature of carelessness that is frequent nowadays leading to an uncompleted project or late delivery (failure). This will affect the daily mood, as well as provoke the variation of emotions in a negative way (Rosi *et al.*, 2019).

3. Research methodology

This study used a quantitative method to assess the benefits of DRM in the CI. The targeted population for this research work was professional involving electrical engineers, quantity surveyors, architects and mechanical, as well as civil engineers involved under a firm or organisation within the province of Gauteng, South Africa. They were chosen from their respective professional bodies based on their level of expertise and experience in contributing to the solution of this work's research objective. Online Google forms were adopted for sharing the questionnaire. The Google forms were sent to the email address and LinkedIn accounts of the respondents. This research project was approved by the Ethics and Plagiarism Committee (FEPC) of the Faculty of Engineering and the Built Environment at the University of Johannesburg. Additionally, the approval number was UJ-FEBE-FEPC-00246. A random sampling technique was used in this study because it assures that each component and group of people has an equal chance of being included in the sample. (Eiselen *et al.*, 2007). Furthermore, this research had a sample size of 115 professionals, however, only 81 professionals replied. Also, the same study evaluated the benefits of construction DRM in the CI using a five-point Likert scale. The five-point Likert scale was transformed into a mean item score (MIS) for the benefit of DRM in the CI. Statistical package for the social sciences was used to analyse the acquired data. The research objective was analysed using SD, MIS, exploratory factor analysis (EFA) and non-parametric test. The MIS was used to classify factors based on the opinions of the participants while descriptive statistics were used to analyse the demographic data of the respondents. The non-parametric test Kruskal–Wallis H was assessed to test the existing relationship or considerable variance in smaller respondent groups (Pallant, 2007). As adopted from the study of Tanga *et al.* (2022b), Kruskal–Wallis was carried out to determine significant differences between the opinions of each of the identified professional groups. This is important to ascertain and validate the views of the respondents because it applies to a wider variety of circumstances as opposed to a parametric test. If the p -value is smaller than 0.05, the evidence is null and greater than 0.05, it is valid. Moreover, the EFA served to compile data relating to how the group variables interacted with one another (Pallant, 2007). It was used to identify a measure's factor structure, as well as assess its internal consistency. Also, it can be used to reveal constraints that may or may not be visible in direct analysis. This was done in accordance with the previous study of Adekunle *et al.* (2022b). Prior executing the EFA, the suitability of the data for factor analysis (FA) was conducted. Also, Pallant (2007) emphasised that the correlation matrix should show coefficients r not less than 0.3 to assess the factorability of the variables. All the coefficients were above 0.3, according to a detailed analysis of the correlation matrix. Eiselen *et al.* (2007) noted that to proceed with EFA, the Kaiser-Meyer-Olkin (KMO) is also used to show the adequacy of the

distribution of values. The condition for a KMO measure of sampling adequacy value to be retained for FA, be equal or greater than 0.6 and Bartlett's test of sphericity should be statistically significant at p less than 0.05 (Pallant, 2007). The direct oblimin rotation was adopted because it allows for correlation between the latent factors as compared to varimax which constrains the correlation to be 0.00 (Eiselen *et al.*, 2007). An experienced statistician examined all the completed questionnaires to validate the quality of the items for the validity test and ensure that the measure is of high quality. Also, Cronbach's alpha was used in this study to measure reliability, and the results showed that the alpha value was 0.968, which was near the recommended value of 1.0 (Pallant, 2007).

4. Findings and discussion

4.1 Biographical data results

The results relating to the 81 respondents' educational qualifications revealed that few of the respondents have a doctorate degree representing 7%. This was followed by those with a diploma degree representing 14%, and honours' degree representing 17%. Moreover, the findings portrayed that most respondents have a bachelor's degree and master's degree with 32% and 30%, respectively. The research also showed that 12% of respondents were civil engineers, 27% were quantity surveyors and 7% were architects. Industrial, mechanical and electrical engineers each made up 1% of the respondents, while construction managers and project managers made up 20% and 14%, respectively. In total, 16% of respondents indicated that they were representing other people involved in the construction project. The respondents' years of experience indicated that out of all respondents, none of the respondents had more than 20 years of experience and 7% had between 16 and 20 years. In total, 14% had between 11 and 15 years of experience and 28% were in the industry with between 6 and 10 years of experience. Moreover, 37%, that is most of the participants, had between 1 and 5 years of experience and 14% had less than 12 months of experience in the CI.

4.2 Mean item score and non-parametric test for benefits of construction data risks management in the construction industry

The benefits of DRM were determined by examining the literature review, which identified 20 variables. The Kruskal–Wallis H test was run on the respondents' rankings of these variables to see whether or not the nine groups of respondents shared the same opinion. Table 1 presents the results of the study as reported by the respondents, revealing that “Enhances project and company data availability” was ranked first with MIS of 4.31, Kruskal–Wallis H of 20.787 and asymp. Sig. value of 0.008; “promotes confidentiality” was ranked second with MIS = 4.30; Kruskal–Wallis H = 18.581; asymp. Sig. value = 0.017; “enhances integrity” was ranked third with MIS = 4.24; Kruskal–Wallis H = 18.701; asymp. Sig. value = 0.017; “improves communication by preventing data modifications or deletion”. Additionally, “promotes data privacy and protection with different security methods” and “reduces hardware and software damage (crash and computer freezing)” were all ranked eleventh with MIS = 4.12; Kruskal–Wallis H = 21.324; asymp. Sig. value = 0.006, MIS = 4.12; Kruskal–Wallis H = 13.440; asymp. Sig. value = 0.098 and MIS = 4.12; Kruskal–Wallis H = 10.469; asymp. Sig. value = 0.234, respectively. Finally, “minimises dispute risk (reduces disputes among stakeholders due to data modification)” and “ability to submit tender” were the two lowest-ranked variables with MIS = 3.94; Kruskal–Wallis H = 23.822; asymp. Sig. value = 0.002 and MIS = 3.90; Kruskal–Wallis H = 10.143; asymp. Sig. value = 0.255, respectively.

The Kruskal–Wallis H test, revealed that there is a statistically significant difference in the respondents' opinions with regard to the following factors: “enhances project and

Benefits of construction data risks management in the construction industry	Mean	Kruskal–Wallis H	Asymp. Sig.	Rank	Construction data risks management
Enhances project and company data availability	4.31	20.787	0.008	1	
Promotes confidentiality	4.30	18.581	0.017	2	
Enhances integrity	4.24	18.701	0.017	3	
Promotes good information quality	4.21	13.610	0.093	4	
Promotes good reputation	4.21	25.888	0.001	4	
Trust about project data	4.21	21.745	0.005	4	
Enhances organisation’s competitive advantage	4.20	19.368	0.013	7	
Guarantees safety of project data	4.19	14.639	0.067	8	
Provides an appropriate risk approach to various attacks	4.19	24.148	0.002	8	
Prevents interruption of project timeline	4.15	8.735	0.365	10	
Improves communication by preventing data modifications or deletion	4.12	21.324	0.006	11	
Promotes data privacy and protection with different security methods	4.12	13.440	0.098	11	
Reduces hardware and software damage (crash and computer freezing)	4.12	10.469	0.234	11	
Promotes hardware and software protection	4.09	10.828	0.212	14	
Enables safe and productive construction environment (reduces loss of information risks)	4.09	9.651	0.290	14	
Eradicates time wastage by quickly handling cyber-attacks	4.07	15.388	0.052	16	
Efficient financial management (reducing unplanned expenses due to cyber-attacks)	4.00	26.325	0.001	17	
Reduces physiological impacts	3.95	16.168	0.040	18	
Minimises dispute risk (reduces disputes among stakeholders due to data modification)	3.94	23.822	0.002	19	
Ability to submit tender	3.90	10.143	0.255	20	

Source: Authors’ own creation

Table 1.
Mean item score and non-parametric test for benefits of construction data risks management in the construction industry

company data availability”, “promotes confidentiality”, “enhances integrity” and “promotes good reputation”. The variations in the opinion of the nine groups of respondents can be due to their points of view concerning these variables. For instance, “enhances project and company data availability” was ranked lower by mechanical engineers compared to the other eight groups while “promotes confidentiality” was ranked lower by industrial engineers. In addition, “enhances integrity” was ranked lower by quantity surveyors compared to the other eight groups while promoting a good reputation was ranked higher by architects and electrical engineers compared to the seven other groups. This test was conducted to discover the different opinions of construction professionals based on what they think of the benefits of DRM. However, there are professionals in the CI who use internet facilities and computers more than others. This will influence the way they view DRM.

The institute of engineering technology (2014) and Tanga *et al.* (2022a) opined that managing data risk enhances project and company data availability. The main aim of DRM is to ensure data availability, integrity, as well as confidentiality (Bhushan *et al.*, 2021). Data availability means that information systems, and processes are available whenever needed for safe, reliable and secure design, as well as building or facility project execution procedures and delivery (The institute of engineering technology, 2014). Construction professionals need DRM to preserve their project data from attackers and to guarantee the availability of data whenever required to avoid work execution interruption. This will enhance the project delivery output while strengthening the information system’s security. The institute of engineering technology (2014), Zhang and Yuan (2016), Talha *et al.* (2019) and Bhushan *et al.* (2021) argue that the management of risks promotes confidentiality.

Therefore, construction project parties need to adopt measures to manage data risk to have total control over individuals who can have access to the project's data.

According to Buch *et al.* (2017) and Tanga *et al.* (2022b), DRM enhances integrity. The institute of engineering technology (2014) stated that integrity in the management of data involves computer-based systems and electronics' trustworthy operations, their software, all connected business processes, data authenticity and assurance, the legitimacy of transactions and their retention, their authentication, as well as non-repudiation. Construction project parties should more pay attention to DRM for viable operation, as well as legal transactions during the project lifecycle to prevent failures and other severe consequences. Aljumaili (2016) and Tanga *et al.* (2022a) opined that DRM promotes good information quality, especially at the collection stage (Adekunle *et al.*, 2022b). According to Yebenes and Zorrilla (2019), good quality data is complete, meaning free of modifications and deletion or other data twisting processes. Professionals in various industries need DRM to be applied to avoid data modification that will spoil the quality of information and lead to client dissatisfaction, project failure and misunderstanding. White and Murray (2016), Arcuri *et al.* (2017), Adekunle *et al.* (2022b) and Van Besouw and Bond-Barnard (2021) posited that DRM via construction information systems and project management information systems promotes a good reputation. Cyber risk represents a big threat to both public and private organisations due to its impact on the information systems, stakeholders' confidence loss, reputation, financial losses economic success and overall performance (Arcuri *et al.*, 2017; Tepeli *et al.*, 2021; Yaqoob *et al.*, 2021). Most of the companies that have experienced data attacks have ended up with unfinished projects according to the contract's timelines and terms of conditions. The CI business is also based on reputation, meaning no client will contact or appoint a professional with a bad reputation concerning his or her past undertaken projects. Beslin and Hendriyati *et al.* (2022) posited that trust relating to the project data is key to the success of the project and this can be achieved through DRM as it can track all the data changes. If construction professionals apply different measures to protect their computers and information system, there will be no open door for intruders to operate and carry out cybercrimes. DRM are essential and beneficial to the CI because it keeps project data far from any manipulation which might destroy trust in project data. Good DRM will build trust among stakeholders.

4.3 Exploratory factor for benefits of construction data risks management in the construction industry

All the factors with eigenvalues above one are displayed on the steep slope of the plot, while the rest of the factors with eigenvalues inferior to one are represented on the gradual trail of the plot. Table 2 presents the number of benefit factors, as well as their respective eigenvalues. Based on the results presented in Table 2 only three clusters of factors fell under Kaiser's criterion with eigenvalues greater than one. Thus, the clusters were interpreted for this FA.

Table 3 shows the findings from the EFA clustering with the aid of the oblimin method of rotation. The choice of the oblimin method of rotation was based on the variables' relationship. According to the results in Table 3, the 20 variables of benefits of construction DRM in the CI are reported into three clusters.

Three-factors clusters were revealed after applying the EFA to identify the correlation patterns within the set of data retrieved. The values for the linear combination of variables measured are represented in the pattern matrix. The three emerged factors are discussed as follows.

Component	Total variance explained				Rotation sums of squared loadings ^a	
	Total	Initial eigenvalues % of variance	Cumulative %	Total	Extraction sums of squared loadings % of variance	Total
1	12.801	60.955	60.955	12.801	60.955	11.280
2	1.268	6.037	66.992	1.268	6.037	10.156
3	1.023	4.870	71.862	1.023	4.870	2.876
4	0.868	4.132	75.994			
5	0.772	3.675	79.669			
6	0.610	2.903	82.572			
7	0.501	2.386	84.958			
8	0.456	2.171	87.129			
9	0.359	1.710	90.880			
10	0.302	1.437	92.317			
11	0.279	1.327	93.644			
12	0.260	1.237	94.881			
13	0.238	1.133	96.014			
14	0.176	0.839	96.853			
15	0.163	0.775	97.628			
16	0.125	0.595	98.223			
17	0.121	0.576	98.798			
18	0.101	0.482	99.281			
19	0.091	0.432	99.713			
20	0.060	0.287	100.000			

Extraction method: principal component analysis

Note: ^aWhen components are correlated, sums of squared loadings cannot be added to obtain a total variance

Source: Authors' own creation

	Pattern matrix ^a		
	1	2	3
Enhances integrity	0.909		
Prevents interruption of project timeline	0.860		
Promotes good information quality	0.836		
Promotes confidentiality	0.832		
Trust about project data	0.738		
Enhances organisation's competitive advantage	0.711		
Ability to submit tender	0.705		
Enhances project and company data availability	0.616		
Provides an appropriated risk approach to various attacks	0.545		
Reduces hardware and software damage (crash and computer freezing)	0.517		
Promotes good reputation	0.465		
Eradicates time wastage by quickly handling cyber-attacks		0.917	
Promotes data privacy and protection with different security methods		0.896	
Improves communication by preventing data modifications or deletion		0.785	
Minimises dispute risk (reduces disputes among stakeholders due to data modification)		0.728	
Enables safe and productive construction environment (reduces loss of information risks)		0.634	
Guarantees safety of project data		0.483	
Promotes hardware and software protection		0.475	
Reduces physiological impacts			0.660
Efficient financial management (reducing unplanned expenses due to cyber-attacks)			0.498
Extraction method: principal component analysis			
Rotation method: Oblimin with Kaiser normalisation ^a			

Table 3.
Pattern matrix

Note: ^aRotation converged in 13 iterations

Source: Authors' own creation

4.3.1 Component one: work performance enhancement. The eleven items loaded in Component 1 among which the three top items were “enhances integrity” (90.9%), “prevents interruption of project timeline” (86%) and “promotes good information quality” (83.6%) while the two last items were “reduces hardware and software damage (crash and computer freezing)” (51.7%) and “promotes good reputation” (46.5%). The 11 items had an overall percentage of the variance of 60.955%.

According to [Attia et al. \(2016\)](#) and [Talha et al. \(2019\)](#), DRM enhances integrity. Integrity in the management of data involves computer-based systems and electronics' trustworthy operations, their software, all connected business processes, data authenticity and assurance, the legitimacy of transactions and their retention, their authentication, as well as non-repudiation ([The institute of engineering technology, 2014](#)). In alignment with [Zhang and Yuan \(2016\)](#), integrity was mentioned by 90.9% of respondents as a benefit of DRM as it stops intruders from data alteration. Thus, construction project parties should more pay attention to DRM to ensure the matching of data when communicating at any point in time, responsible operation, as well as legal transactions during to project lifecycle to prevent failures and other severe consequences. [Shi and Saleem \(2012\)](#), [Arcuri et al. \(2017\)](#) and [Tanga et al. \(2022a\)](#) posited that the practice of good DM will prevent the interruption of project timelines due to loss of data. Construction professionals need to follow all the regulations and practices of DRM to avoid work interruption which will hold them liable for non-compliance to the contract's timelines frame which will cost them fines, loss of reputation, as well as loss of contract. In total, 83.6% of respondents to the study mentioned promotes good information quality as a DRM advantage that enables the smooth execution of construction projects by keeping data free of manipulation and alterations and this is

supported by the literature (Khatri and Brown, 2010; Yaqoob *et al.*, 2021). To avoid involuntary information twisting which has negative effects on the project, professionals should, therefore, put DRM into practice to provide good information quality.

Like the findings of this study, Zhang and Yuan (2016) and Bhushan *et al.* (2021) agree that management risks promote confidentiality. Confidentiality involves having total control over who has access to the information system (Bhushan *et al.*, 2021). Therefore, construction project parties need to adopt DRM strategies to protect the information system from unauthorised access. Beslin and Reddin (2004) and Yaqoob *et al.* (2021), claims correspond with those of this study that trust in project data is achieved through DRM. By putting in place DRM, there will be no open door for unconscious alteration to project information which will raise data trust issues in organisations. For this reason, DRM is highly needed to build trust in project data and fight mistrust among stakeholders. White and Murray (2016), Adekunle *et al.* (2022b) and Hendriyati *et al.* (2022) posited that DM promotes competitive advantage. DRM are a good weapon to fight data losses, theft of data, data exposition and data modification which will enable rival companies to imitate the formula and ways of providing services. Hence, professionals in the construction sector have the responsibility of protecting their private data and success secrets to promote their competitive advantage and keep their cutting-edge position in the market.

4.3.2 Component two: project data protection. The two first loaded in component two were “eradicates time wastage by quickly handling cyber-attacks” (91.7%), and “promotes data privacy and protection with different security methods” (89.6%). The “promotes hardware and software protection” (47.5%) was the last item. The overall percentage of the variance of the seven items loaded in component two was 6.037%.

Tanga *et al.* (2022b) posited that DRM helps to eradicate time wastage by quickly handling cyber-attacks. When construction professionals and staff are aware of the various attacks and measures it will be easy to protect the system and know what technique to use against different cyber-attack. This will save time and help the company form a shield of protection measures against external attacks.

Promotes data privacy and protection with different security methods was viewed as the positive result of good DRM by 89.6% of respondents to the questionnaire and this agrees with the literature (Bamigboye *et al.*, 2017; Tanga *et al.*, 2022a). DRM (cybersecurity) offers organisations and companies using electronic devices for communication purposes, good techniques and methods that will help to fight and prevent an intruder’s activities. Professionals should familiarise themselves with the different DRM techniques to safeguard their private information. According to Adekunle *et al.* (2022b), DRM improves communication by building relationships among project members, as well as preventing data modifications or deletion. Communication is the key to success in any organisation. This is done through the usage of ICT tools is advantageous to many organisations although they also the organisation’s sensitive information at risk and increase the need for DRM to promote the company’s success (Adekunle *et al.*, 2022a). DRM is needed to enable both good communication among stakeholders and private data protection. Like the participants in the study, Jakobsson and Myers (2006) and Deep *et al.* (2021) posited that the adoption of DRM minimises dispute risk (reduces disputes among stakeholders due to continuous data modification) as it prevents intruders from manipulating the data which can lead to disputes. The modifications frequent specification alteration due to frequent changes in plans and concepts, or the structure’s aesthetics (Deep *et al.*, 2021). Whether the excessive modifications come from an unprofessional client, an architect, the project manager or hackers it will result in disputes. To avoid disputes during the project lifecycle among construction project parties due to cyberattacks, professionals and other workers

involved in the exchange of data via ICT tools need to fully apply the different DRM measures. With 63.4%, enables a safe and productive construction environment was noted as a significant benefit of DRM in alignment with [Arora et al. \(2006\)](#) and [The Chartered Institute of Building \(2018\)](#). This is due to protection measures and that DRM offers measures to ensure that construction project data and staff's private information are not compromised by hackers. As a result, this can also have a positive psychological impact on stakeholders as they know that their sensitive information is protected. Therefore, DRM risk enhances good work productivity and performance in the construction sector.

4.3.3 Component three: unplanned programme reduction. The two items loaded in component three were “reduces physiological impacts” (66%) and “efficient financial management (reducing unplanned expenses due to cyber-attacks)” (49.8%), with a total percentage of the variance of 4.870%.

Like the participants in this study, several authors posited that managing data risk challenges reduces physiological impacts ([Minei and Matusitz, 2011](#); [Gandhi et al., 2011](#); [Modic and Anderson, 2015](#); [Tanga et al., 2022a](#)). Because financial fraud victims suffer from serious emotional effects ([Minei and Matusitz, 2011](#); [Rosi et al., 2019](#)) people and businesses pay more attention to cyberattacks effects on their lives and business rather than the attack itself ([Gandhi et al., 2011](#)). Furthermore, [Deep et al. \(2021\)](#) [Zhao \(2023\)](#) and [Rehman et al. \(2022\)](#) added that managing finances is an important aspect to prevent overruns. These overruns either in terms of cost or time are the reason for present and future projects (business). Therefore, DRM plays a key role in the reduction of physiological impacts as it helps to keep the minds of stakeholders in perfect peace by knowing that measures have been taken to protect sensitive data in the working environment.

[Warren et al. \(2016\)](#) and [Tanga et al. \(2022b\)](#) supported this finding by stating that DRM enhances efficient financial management by reducing unplanned expenses due to cyber-attacks. Many organisations lose money because of the negligence of cyber-attacks as most of the cybercrimes go unrecorded and undetected. To detect the various cyber-attacks attempts, professionals need to apply security measures to avoid unplanned expenses that will impact negatively the company's finance. In addition, cyber-attacks will also affect the execution of the project since the firm will lack enough money to carry out the project.

5. Conclusion and recommendation

This study was set out to assess the benefits of DRM to the CI. To achieve this objective, the study adopted a quantitative research method. Questionnaire survey was distributed to professionals in the South African CI and their responses were analysed. Findings from the study revealed that managing risks associated with DM helps to minimise dispute risk, eradicate time wastage, promote data privacy and protection, improve communication, provide an appropriate risk approach to various attacks, guarantee the safety of project data and reduce hardware and software damage. Hence, to reap the full benefits of DRM, construction professionals need to carefully apply the measures that DRM provide while undertaking their various projects. DRM represent a good option for continuous 4IR adoption. By using it daily, risk prevention will be much easier. By highlighting the numerous benefits of DRM in the CI, the study adds to the body of knowledge and will help and motivate project stakeholders to continuously have an interest in how data is being managed, as well as pay attention to ways to mitigate data risks before, during and after the project delivery. Furthermore, this research study will keep professionals informed of how the project is prompt to fail if their DM carelessness continues in the construction environment.

It is recommended that construction project stakeholders must always apply DRM to secure their information systems from malicious activities that might cripple the project

execution, as well as benefit from Industry 4.0 features that ease the management of project data. The study recommended that professionals should continue to adopt DRM to prevent work delay and stoppage, undergo thorough training on data security measures proposed in this study and constantly reduce data risks. Furthermore, project members need to associate themselves with information technology professionals to keep abreast of the new data risks and their countermeasures. The limitation or drawback of this study is that this research was only carried out in the province of Gauteng as there was lockdown (travel restrictions) because of COVID-19. As a result, the findings of this study cannot be generalised to a larger population. Another limitation was the slow response rate of the chosen participants due to the physiological impacts of COVID-19 on them leading to time constraints. In future research studies, a larger sample size should be used to help the construction sector to shape more knowledge on DRM. And also, because much research on risk management emphasised on risk acceptance, thus further research on the notion of data risk refusal needs to be introduced.

6. Practical implications

In practice, the findings of this study can be used to improve the management of data in construction projects by adopting effective DRM strategies. Construction professionals can use the findings to ensure that their work performance is enhanced by preventing data loss, reducing hardware and software damage, promoting good information quality and enhancing integrity. They can also use the findings to protect project data by eradicating time wastage by quickly handling cyber-attacks, promoting data privacy and protection and promoting hardware and software protection. Additionally, the findings can be used to ensure that construction projects comply with legal and regulatory requirements related to data protection and privacy. The study's findings can also be used in teaching to raise awareness among students and professionals about the importance of data risk management in construction projects. The study can be used as a basis for developing training programmes to teach students and professionals how to implement effective DRM

DRM	Data risks management
BIM	Building information modelling
DM	Data management
CI	Construction industry
MIS	Mean item score
SPSS	Statistical package for the social sciences
SD	Standard deviation
EFA	Exploratory factor analysis
KMO	KaiserMeyer-Olkin
FEPC	Ethics and Plagiarism Committee
FA	Factor analysis
IET	Institute of Engineering Technology
COVID-19	Coronavirus
KPIs	Key performance indicators
DG	Data governance
CCTV	Closed-circuit television
ICT	Information communication technology
Asymp. Sig. value	Asymptotic significance value

Source: Authors' own creation

Table 4.
Abbreviations and
definitions

strategies. In terms of public policy, the study's findings can be used to advise, inform and update policymakers about the importance of DRM in construction projects. Policymakers can use the findings to develop regulations and guidelines that require construction professionals to adopt effective DRM strategies to protect project data. Finally, the study's findings add to the body of knowledge on DRM in construction projects by identifying three factors related to the effective management of data. The study's findings can be used as a basis for further research to explore the effectiveness of different DRM strategies in construction projects [Table 4](#).

References

- Adekunle, P., Aigbavboa, C., Akinradewo, O., Oke, A. and Aghimien, D. (2022b), "Construction information management: benefits to the construction industry", *Sustainability*, Vol. 14 No. 18, p. 11366.
- Adekunle, P., Aigbavboa, C., Thwala, D., Oke, A. and Akinradewo, O. (2022a), "Construction information management: the role of fourth industrial revolution tools", *Hum. Factors Archit. Sustain. Urban Plan. Infrastructure*, Vol. 58, pp. 254-261.
- Al-Ajmi, H.F. and Makinde, E. (2018), "Risk management in construction projects", *Journal of Advanced Management Science*, Vol. 6 No. 2, pp. 113-116.
- Aljumaili, M. (2016), "Data quality assessment: applied in maintenance", Doctoral dissertation, Luleå tekniska universitet.
- Arcuri, M.C., Brogi, M. and Gandolfi, G. (2017), "How does cybercrime affect firms? The effect of information security breaches on stock returns", *Proceedings of the First Italian Conference on Cybersecurity. (ITASEC17)*, Venice, Italy, pp. 175-193.
- Arora, A., Nandkumar, A. and Telang, R. (2006), "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis", *Information Systems Frontiers*, Vol. 8 No. 5, pp. 350-362.
- Attia, M., Nasr, M. and Kassem, A. (2016), "E-mail systems in cloud computing environment privacy, trust and security challenges", *International Journal of Engineering Research and Application, IJERA*, Vol. 6, pp. 63-68.
- Bada, M. and Nurse, J.R. (2020), "The social and psychological impact of cyberattacks", in Benson, V. and McAlaney, J. (Eds), *Emerging Cyber Threats and Cognitive Vulnerabilities*, Academic Press, Cambridge, MA, pp. 73-92.
- Bamigboye, O.O., Olawuyi, O.F. and Tomori, R.A. (2017), "Analysis of cyber-security benefits on cyberspace in Nigerian insurance companies", *Journal of Communication*, Vol. 8 No. 2, pp. 136-140.
- Bendovschi, A. (2015), "Cyber-attacks—trends, patterns and security countermeasures", *Procedia Economics and Finance*, Vol. 28, pp. 24-31.
- Beslin, R. and Reddin, C. (2004), "How leaders can communicate to build trust", *Ivey Business Journal*, Vol. 69 No. 2, pp. 1-6.
- Bhushan, B., Sinha, P., Sagayam, K.M. and Andrew, J. (2021), "Untangling blockchain technology: a survey on state of the art, security threats, privacy services, applications and future research directions", *Computers and Electrical Engineering*, Vol. 90, p. 106897.
- Bishop, M. (2003), *Computer Security: Art and Science*, Addison-Wesley Professional, Boston, US.
- Buch, R., Ganda, D., Kalola, P. and Borad, N. (2017), "World of cyber security and cybercrime", *Recent Trends in Programming Languages*, Vol. 4 No. 2, pp. 18-23.
- Cains, M.G., Flora, L., Taber, D., King, Z. and Henshel, D.S. (2021), "Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation", *Risk Analysis*, Vol. 42 No. 8, doi: [10.1111/risa.13687](https://doi.org/10.1111/risa.13687), available at: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/risa.13687> (accessed on 14 April 2022).

- Chen, D. and Zhao, D. (2012), "Data security and privacy protection issues in cloud computing", *International Conference on Computer Science and Electronics Engineering*, pp. 647-651, doi: [10.1109/ICCSEE.2012.193](https://doi.org/10.1109/ICCSEE.2012.193).
- Dada, M.O. (2013), "Conflicts in construction projects procured under traditional and integrated methods: a correlation analysis", *International Journal of Construction Supply Chain Management*, Vol. 3 No. 1, pp. 1-15.
- Deep, S., Bhoola, V., Verma, S. and Ranasinghe, U. (2021), "Identifying the risk factors in real estate construction projects: an analytical study to propose a control structure for decision-making", *Journal of Financial Management of Property and Construction*, Vol. 27 No. 2.
- Dhillon, G. (2015), *What to Do before and after a Cybersecurity Breach. The Changing Faces of Cybersecurity Governance Series*, Kogod Cybersecurity Governance Center, Washington, DC.
- Eiselen, R., Uys, T. and Potgieter, T. (2007), "Analysing survey data using SPSS13", 3rd ed.
- Erfani, A., Ma, Z., Cui, Q. and Baecher, G.B. (2023), "Ex post project risk assessment: method and empirical study", *Journal of Construction Engineering and Management*, Vol. 149 No. 2, pp. 1-9.
- Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P. (2011), "Dimensions of cyber-attacks: cultural, social, economic, and political", *IEEE Technology and Society Magazine*, Vol. 30 No. 1, pp. 28-38.
- Hendriyati, P., Farida, A., Rahardja, U. and Ramadhan, T. (2022), "Management information systems on integrated student and lecturer data", *APTISI Transactions on Management (ATM)*, Vol. 6 No. 1, pp. 1-9.
- Jakobsson, M. and Myers, S. (Eds) (2006), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, John Wiley and Sons, New Jersey, NJ.
- Karlsen, J.T., Graee, K. and Massaoud, M.J. (2008), "The role of trust in project-stakeholder relationships: a study of a construction project", *International Journal of Project Organisation and Management*, Vol. 1 No. 1, pp. 105-118.
- Khalfan, M.M., McDermott, P. and Swan, W. (2007), "Building trust in construction projects", *Supply Chain Management: An International Journal*, Vol. 12 No. 6, pp. 385-391.
- Khatri, V. and Brown, C.V. (2010), "Designing data governance", *Communications of the ACM*, Vol. 53 No. 1, pp. 148-152.
- Minei, E. and Matusitz, J. (2011), "Cyberterrorist messages and their effects on targets: a qualitative analysis", *Journal of Human Behavior in the Social Environment*, Vol. 21 No. 8, pp. 995-1019.
- Modic, D. and Anderson, R. (2015), "It's all over but the crying: the emotional and financial impact of internet fraud", *IEEE Security and Privacy*, Vol. 13 No. 5, pp. 99-103, doi: [10.1109/MSP.2015.107](https://doi.org/10.1109/MSP.2015.107).
- Nourani, A., Ayatollahi, H. and Solaymani Dodaran, M. (2022), "Data management in diabetes clinical trials: a qualitative study", *Trials*, Vol. 23 No. 1, pp. 1-9.
- Nyamuchiwa, K., Lei, Z. and Aranas Jr, C. (2022), "Cybersecurity vulnerabilities in off-Site construction", *Applied Sciences*, Vol. 12 No. 10, pp. 1-25.
- Pallant, J. (2007), "SPSS survival manual: a step-by-step guide to data analysis using SPSS".
- Pham, H.T., Pham, T., Truong Quang, H. and Dang, C.N. (2022), "Supply chain risk management research in construction: a systematic review", *International Journal of Construction Management*, pp. 1-11.
- Preneel, B. and Takagi, T. (Eds), (2011), *Cryptographic Hardware and Embedded Systems—CHES*, Springer, Berlin.
- Rehman, S.U.M., Thaheem, M.J., Nasir, A.R. and Khan, K.I.A. (2022), "Project schedule risk management through building information modelling", *International Journal of Construction Management*, Vol. 22 No. 8, pp. 1489-1499.
- Rosi, A., Cavallini, E., Gamboz, N., Vecchi, T., Van Vugt, F.T. and Russo, R. (2019), "The impact of failures and successes on affect and self-esteem in young and older adults", *Frontiers in Psychology*, Vol. 10, p. 1795.

-
- Shi, J. and Saleem, S. (2012), "Computer security research reports: phishing", available at: www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/reports.pdf (accessed 2 January 2021).
- Staunton, C., Tschigg, K. and Sherman, G. (2021), "Data protection, data management, and data sharing: stakeholder perspectives on the protection of personal health information in South Africa", *Plos One*, Vol. 16 No. 12, p. e0260341.
- Sui Pheng, L., Shing Hou, L., Pheng, L.S. and Hou, L.S. (2019), "The economy and the construction industry", *Construction Quality and the Economy: A Study at the Firm Level*, pp. 21-54.
- Sultanate of Oman Information Technology Authority (2017), "IT risk management framework", available at: www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf (accessed on 14 April 2022).
- Talha, M., Abou El Kalam, A. and Elmarzouqi, N. (2019), "Big data: trade-off between data quality and data security", *Procedia Computer Science*, Vol. 151 No. 2019, pp. 916-922.
- Tanga, O.T., Aigbavboa, C.O., Akinradewo, O.I., Thwala, D.W. and Onyia, M. (2021a), "Construction digitalisation tools in South African construction industry: an added advantage", *IOP Conference Series: Materials Science and Engineering*, Vol. 1107 No. 1, p. 12230.
- Tanga, O., Akinradewo, O., Aigbavboa, C., Oke, A. and Adekunle, S. (2022a), "Data management risks: a bane of construction project performance", *Sustainability*, Vol. 14 No. 19, p. 12793.
- Tanga, O., Akinradewo, O., Aigbavboa, C. and Thwala, D. (2022b), "Cyber Attack risks to construction data management in the fourth industrial revolution era: a case of Gauteng province, South Africa", *Journal of Information Technology in Construction (ITcon)*, Vol. 27 No. 41, pp. 845-863.
- Tepeli, E., Taillandier, F. and Breyse, D. (2021), "Multidimensional modelling of complex and strategic construction projects for a more effective risk management", *International Journal of Construction Management*, Vol. 21 No. 12, pp. 1218-1239.
- The Chartered Institute of Building (2018), "The role of security in the construction industry", available at: www.ciob.org/sites/default/files/TheRoleofSecurityintheconstructionindustry.pdf (accessed 18 October 2020).
- The institute of engineering technology (2014), "Building information modelling (BIM): addressing the cyber security issues", available at: www.theiet.org/media/1222/bim-cyber.pdf (accessed 18 October 2020).
- Van Besouw, J. and Bond-Barnard, T. (2021), "Smart project management information systems (SPMIS) for engineering projects—project performance monitoring and reporting", *International Journal of Information Systems and Project Management*, Vol. 9 No. 1, pp. 78-97.
- Warren, T., Favole, J., Haber, S. and Hamilton, E. (2016), "Cybercrime costs more than you think", Hamilton Place Strategies Report.
- White, R. and Murray, R.M. (2016), "A cybersecurity risk in the construction industry", available at: www.dhglp.com/Portals/0/ResourceMedia/publications/construction-cybersecurity.pdf (accessed 10 October 2020).
- Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y. (2021), "Blockchain for healthcare data management: opportunities, challenges, and future recommendations", *Neural Computing and Applications*, Vol. 34 No. 14, pp. 1-16.
- Yebenes, J. and Zorrilla, M. (2019), "Towards a data governance framework for third generation platforms", *Procedia Computer Science*, Vol. 151, pp. 614-621.
- Zhang, N. and Yuan, Q. (2016), "An overview of data governance", Economics Paper, December.
- Zhao, X. (2023), "Construction risk management research: intellectual structure and emerging themes", *International Journal of Construction Management*, doi: [10.1080/15623599.2023.2167303](https://doi.org/10.1080/15623599.2023.2167303).

Further reading

- Akinradewo, O., Aigbavboa, C., Aghimien, D., Oke, A. and Ogunbayo, B. (2021), "Modular method of construction in developing countries: the underlying challenges", *International Journal of Construction Management*, Vol. 23 No. 8, p. 1970300, doi: [10.1080/15623599.2021.1970300](https://doi.org/10.1080/15623599.2021.1970300).
- Böhme, R. and Schwartz, G. (2010), "Modeling cyber-insurance: towards a unifying framework", *Workshop on the Economics of Information Security (WEIS)*, Harvard University, Cambridge, pp. 7-8.
- Creswell, J.W. (1994), *Research Design: Qualitative and Quantitative Approaches*, Sage, Thousand Oaks, CA.
- Dave, K.T. (2013), "Brute-force attack; seeking but distressing", *International Journal of Innovations in Engineering and Technology (IJJET)*, Vol. 2 No. 3, pp. 75-78.
- Dimitrieska, S., Stankovska, A. and Efremova, T. (2018), "The fourth industrial revolution: advantages and disadvantages", *Economics and Management*, Vol. 14 No. 2, pp. 182-187.
- Farwell, J.P. and Rohozinski, R. (2011), "Stuxnet and the future of cyber war", *Survival*, Vol. 53 No. 1, pp. 23-40.
- Gross, M.L., Canetti, D. and Vashdi, D.R. (2016), "The psychological effects of cyber terrorism", *Bulletin of the Atomic Scientists*, Vol. 72 No. 5, pp. 284-291.
- Liu, X., Cao, J., Yang, Y. and Jiang, S. (2018), "CPS-based smart warehouse for Industry 4.0: a survey of the underlying technologies", *Computers*, Vol. 7 No. 1, pp. 1-13.
- Losonczy, P. (2018), "Importance of dealing with cybersecurity challenges and cybercrime in the senior population", *Security Dimensions*, Vol. 26 No. 26, pp. 173-186.
- Mohammad, S.M. (2020), "Risk management in information technology", *Internal Journal of Innovations in Engineering Research and Technology (IJERT)*, Vol. 7 No. 5, pp. 373-381.
- Ostertagova, E., Ostertag, O. and Kováč, J. (2014), "Methodology and application of the Kruskal-Wallis test", *Applied Mechanics and Materials*, Vol. 611, pp. 115-120.
- Pawlak, P. and Wendling, C. (2013), "Trends in cyberspace: Can governments keep up?", *Environment Systems and Decisions*, Vol. 33 No. 4, pp. 536-543.
- Retnowardhani, A. and Suroso, J.S. (2019), "Project management information systems (PMIS) for project management effectiveness: Comparison of case studies", *2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)*, 16th-17th October, Jember, Indonesia, pp. 160-164, *IEEE*.
- Symantec (2010), "Norton cybercrime report: the human impact", available at: www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf (accessed 02 September 2020).
- Tanga, O., Akinradewo, O., Aigbavboa, C. and Thwala, D. (2021b), "Usage of cloud storage for data management in the built environment", in Ahram, T.Z., Karwowski, W., Kalra, J. (Eds), *Advances in Artificial Intelligence, Software and Systems Engineering*, Springer, Cham, Vol. 271, pp. 465-471.
- Tehranipoor, M. and Wang, C. (Eds) (2011), *Introduction to Hardware Security and Trust*, Springer Science and Business Media, Berlin, Heidelberg.
- Vidhyalakshmi, P. (2012), "Data security risks in cloud computing", available at: www.researchgate.net/publication/216700324_Data_Security_Risks_in_Cloud_Computing (accessed on 19 October 2022).

Corresponding author

Ornella Tanga Tambwe can be contacted at: tambweorny@gmail.com

For instructions on how to order reprints of this article, please visit our website:

www.emeraldgrouppublishing.com/licensing/reprints.htm

Or contact us for further details: permissions@emeraldinsight.com