CYBER ATTACK RISKS TO CONSTRUCTION DATA MANAGEMENT IN THE FOURTH INDUSTRIAL REVOLUTION ERA: A CASE OF GAUTENG PROVINCE, SOUTH AFRICA

SUBMITTED: July 2021
REVISED: June 2022
PUBLISHED: October 2022
EDITOR: Esther Obonyo
DOI: 10.36680/j.itcon.2022.041

Ornella Tanga, Ms,
cidb Centre for Excellence, Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa;
tambweorny@gmail.com

Opeoluwa Akinradewo, Mr,
cidb Centre for Excellence, Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa;
opeakinradewo@gmail.com

Clinton Aigbavboa, Prof,
cidb Centre for Excellence, Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa;
caigbavboa@uj.ac.za

Didibhuku Thwala, Prof,
University of South Africa (UNISA), College of Engineering, Science and Technology, Department of Civil Engineering
Email: Thwaladw@unisa.ac.za

SUMMARY: *The 4IR or the digital revolution refers to a collective term for a value chain organizational concepts and technologies that together build the Internet of Things, Internet of people, Cyber-Physical Systems (CPS), Internet of Services and the Internet of Energy. While this digital revolution has helped the construction industry to prevent cost and time overruns and enable efficiency and good work's quality, it also has disadvantages and risks such as cyberattacks and loss of jobs. This study set out to determine the risks associated with data management (cyberattacks) on construction projects in the fourth industrial revolution era. The research study will address the questions of "what are the cyberattacks risk attributed to construction data management in the fourth revolution era?" and "What are the differences in the opinion of respondents concerning the identified cyberattacks?". This research work used a quantitative method and gathered information from different construction professionals in the South African construction industry precisely in Gauteng province via a well-structured questionnaire through online platforms. These professionals involve quantity surveyors, architects, civil, mechanical, and electrical engineers practising under a firm, company, organisation, or institution within the Gauteng province, South Africa. Findings revealed that viruses, hacking, and password cracking are the most frequent risk to data management encountered in the construction industry. It was also indicated that construction project stakeholders need a strong knowledge of how attackers operate to address, avoid, and stop the different risks rising when executing a project. The study contributes to the body of knowledge by highlighting the various risks encountered in managing data in the construction industry which will assist professionals in the industry to pay attention to means of mitigating the identified risks. This will keep stakeholders abreast of how simple negligence from their side can deeply affect the project data thereby affecting project delivery. It was concluded based on findings that construction professionals need to avoid the occurrence of these risks to enhance satisfactory project delivery and protect their project information. The study recommended that all construction project parties require full training sessions on risks to data to prevent any types of intrusion into the company's information system.*

KEYWORDS: *construction industry, data risks, data management, fourth industrial revolution*

REFERENCE: *Ornella Tanga, Opeoluwa Akinradewo, Clinton Aigbavboa, Didibhuku Thwala (2022). 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, pg. 845-863, DOI: 10.36680/j.itcon.2022.041*

1. INTRODUCTION

The society has entered a period of tremendous transformation in the first quarter of the twenty-first century, which is very often referred to as industry 4.0 (4IR). It is defined by the emergence of more complex technologies that connect the digital, biological and physical worlds together. For instance, 3D printing, robotics as well as the internet of things (IOT) are the examples of the 4.0 technologies. Additionally, the abilities of Industry 4.0 are having an influence on all areas of the economy and are putting established social systems to the challenge (Rotatori et al., 2021). As a result of the 4IR, there is a growing global push to integrate innovative technologies into procedures and activities across organizations, which is starting to have an influence on how projects are designed, built, and executed in the building sector (World Economic Forum., 2018). Ayodele and Kajimo-Shakantu (2021) explained that the 4IR has led to an increase in data. These data are difficult to control in the construction industry because of their difference source of provenance. Data usually come from different stakeholders involved in a construction project. In building sector, data is represented by specifications, drawings, bills of quantities, construction program, quality assessment, performance reports, data location, comparative cost data, spatial data, user’s behaviour, and also market information are generated during construction various project phases. Leppikorpi (2018) stressed that data in many industries including construction companies are using data as a business competitive device because most organisations view the accessibility to data as a way to gain competitive advantage in the market; yet this perception inhibits data exchange among industry professionals. As a result, stakeholders' interest in data sharing is hampered by concerns about disclosing classified information to competitors. To address this, data management need to be incorporated to ensure that data reach to the intended people and not competitors.

According to Ayodele and Kajimo-Shakantu (2021), 4IR features or technologies enable good management of the different types of data that enhance construction projects delivery by reducing cost and help various construction companies to win more projects and stay in business during tight competition. Alaloul et al. (2020) pointed that Industry 4.0 enable product quality, decreases construction project delivery time, improves collaboration among stakeholders and client relationship, reduces construction rework through accurate information transmission among project members, and also decreases uncertainties. Bendovschi (2015) stressed that digitalisation or industry 4.0 exposes construction projects data to intruders because it is the type of industries that attract them but the internet usage and online activities. Moreover, Alaloul et al. (2020) explained that information and data exchange in the construction sector would be vulnerable to threats and put in harmful situations, resulting in a slew of IT security worries about data privacy. Thus, weather construction industries or not, all companies using and enjoying the adoption of the 4IR should be aware that attacks (risks) might happen anytime especially if the company does not have data management risks system in place to protect their information. Tao et al. (2022) explained that with the new innovation, many construction companies opt for building information modelling (BIM) tools to improve all the design cooperation among all parties involved in the project. The same tool is also utilised in various industries such as architecture and engineering because of the data management benefits it offers.

According to Xu et al. (2018), the digital revolution is more of transformative power, speed, complexity, and scale in comparison with previous eras. Sony (2020) stated that just as every previous industrial revolution, the fourth industrial revolution implementation also has its advantages and disadvantages. The fourth industrial revolution has benefited many industries by enabling cost and time overruns prevention, satisfactory project results, good quality of work, better cooperation, and data exchange among stakeholders, promote better reputation among others (Oesterreich and Teuteberg, 2016). Drucker (2014) explained that the disadvantages of industry 4.0 involve cyber-attacks due to the high connectivity level and job losses because of the automation adoption in industries. The benefits involve overall long-term data or information management that enhances good decision making for better business advancement and easy communication as teamwork is impossible without communication. Construction firms do not only use BIM but cloud storage also to handle data (Tanga et al., 2021a). Although, these tools are promoting good data management, they also present a threat because intruders use them to target data in the construction sector (Tao et al., 2022). Thus, data management risk is essential to the development of construction projects. The construction industry is forced to deal with various data and information coming from different stakeholders and teams involved in the projects. These data are growing at a fast pace and need proper management to ensure the success of a project. The fourth industrial revolution (4IR) has helped the sector to manage data all along the lifecycle through ICT tools (software). Unfortunately, 4IR is a double-edged sword because although it aids in the management of data, it requires the use of internet which makes construction project data vulnerable to cyberattacks. The negligence of this security risk can result in irreparable consequences (bombardment of cyberattacks) that will impact negatively the project execution.

The risk that are usually associated with the procedures of data management includes data corruption (Kanimozhi et al., 2019), storage device failure (Yaqoob et al., 2021), non-protection of physical hard drive storages and improper recording (Zhu et al., 2019). For the purpose of this study, the risk to be considered is cyber-attacks. With increasing reported cases of breach in organisation's firewall, it becomes vital to examine the risk associated with cyberattacks. With the fast development of technology, the construction industry has experienced a paradigm shift from keeping data on a paper base to an electronic base or digitalisation. This shift has led the construction organisation to gather and keep crucial and private information about labourers, projects, organisation, and other information in the cloud which expose it to various cyberattacks and protect and secure sensitive information (Maritz and Hattingh, 2015; Tanga et al., 2021a). According to Zhang and Yuang (2016), data security and privacy simply mean keeping the data confidentiality, integrity, and availability (called the CIA triad) whenever needed by the organisation. Confidentiality refers to the restriction and limitation rules to accessing private data. Integrity is the preservation of data against unlawful access and the availability of data is all about the accessibility of data any time needed by stakeholders (Terzi et al., 2015; Bhushan et al., 2021). Bhushan et al. (2021) mentioned that besides the CIA triad, there are also other properties related to data access to reinforce security such as non-repudiation, authenticity, and authorisation. Most construction companies including the South African industry opt for the implementation of the 4IR for the management of their data through the project lifecycle because of the benefits it provides forgetting the risks they run through its adoption. To this end, the main aim of this study is to determine the risks related to data management on construction projects due to the adoption of the 4IR as well as propose a means of protecting data in the era of digitalisation. The research questions in the same vein are stated as "what are the cyberattacks risks attributed to construction data management in the fourth revolution era?" and "What are the differences in the opinion of respondents concerning the identified cyberattacks?". There is a large number of studies on information communication tools (ICT) to address data or information management in the construction sector due to the large increase of data generated during the construction phase (Amusan et al., 2018, Amusan et al., 2021 and Tanga et al., 2021a) and its adoption, barriers and the requirements to eradicate the challenges of electronic data management system (EDMS) usage (Vasista & Abone, 2018 and Ozumba, 2018).

Subsequent sections of this study focused on the theoretical background on data management and data management risks. Afterwards, the study discussed the different types of cyberattacks and their approach to disruption of data management systems. Subsequently, the study discussed the research methodology and delved into the findings and discussion of the findings. The study presented a conclusion and recommendation section before the referencing lists.

2. THEORETICAL BACKGROUND

DATA MANAGEMENT AND DATA MANAGEMENT RISKS

According to Halttula et al. (2020) both data and its management are strong drivers of efficiency improvement in buildings, roads and power supplies (infrastructures). For this improvement to take place, enterprises should avoid the fragmentation and sub-optimisation of data and the integrated project model is still the entity that needs to be optimised. Thus, because data occupy an important place in companies, it must be accessible at any time, correct, and contained in a single, centralised storage that is available to all project members. In this study, data is defined as all construction project all documents (including pictures and video) in electronic form which can be stored, controlled, secured, retrieved, exchanged as well as edited. KPMG (2021) the process by which an entity collects, organises, preserves, uses, and distributes data to conduct its core business across the project asset lifecycle operations is known as information management (IM). The use of this IM is very important especially at the project level because it can give the fuel for more widespread use of IM at the top management through the gathering and reusing of information (e.g. financial data or workforce data) 'upwards' to managerial tasks or objectives that are not based in the capital and delivery of assets. Tanga et al. (2021a) stated that the construction sector generates multiple files and document (data) throughout the project lifecycle and the way this data is managed represent an aspect to take seriously in the built environment because it a project success indicator. Furthermore, the authors emphasised that data management will prevent data unavailability, data incompleteness, data loss and theft as well as project interruption. This shows that data management is the power of any construction industry in the era of highly computerised world. Halttula et al. (2020) stated that everything in our modern economy is infused with automation, digitalisation as well as data management. To deal with three mentioned aspects of the economy above, there are an infinite number of gadgets and services available to help people and businesses (construction sector) increase the efficiency of their processes and activities. Dheyab (2018) stressed that data is managed through information communication software to achieve the three pillars of every construction projects which are quality, cost and time. This is because this software has the ability to reduce the time required to edit or complete the various project documents whether in the planning, designing or computing, reduce expenses incurred as a result of manual labor and drawing errors and also promote good quality control through the development of project integrated models that ensure adjustments are made before the real implementation. There are various activities included in information and data management such as data creation and specification, data acquisition, data storage, data assurance, data transmission, data quality checking, data rules, data improvement strategies, data maintenance, data value improvement, data archival, as well as data security management (AICPA, 2013, KPMG, 2021) from this, it is seen that information or data management does not cyber security (cyberattacks measures). Moreover, data management risks cover many factors such as non-protection of physical hard drive storages, mistakes from employees which can lead to unintended data alteration, wrong data storage, bad data exchange among employees, and data entry errors, misinterpretation of data (Green, 2015 and Talha, 2019). The authors further explained that technical issues as a result of mechanical, motion, physiological and electrical conditions, explosions, pressure extremes, fires, human factors, control systems, vibration and operating modes can also lead to data risks in sense where the computer containing data can be damaged or employees can make heavy mistakes that affect directly data. These type of data risks are completely different from cyberattacks but still part of data management risks. Based on the discussion above, data management risks are far more than cyberattacks and cybersecurity because once one of the activities listed above are not respected there is a risk. Furthermore, data management risks can also be achieved through various ICT software (Tanga et al., 2021b). such as BIM, Blockchain and other security features (Perera et al., 2020).

CYBERATTACKS

The adoption of industry 4.0 has required construction project members to change their data management systems. Data is now shared, accessed, and stored via the internet and automated processes using information technology systems. Due to the new data management systems, sensitive and personal data are constantly at risk. The risks are multiple because attackers are developing new techniques to steal private information or have unauthorized access to data, networks as well as programmes (Bendovschi, 2015). In a world increasingly powered by social media, online purchases and big data have changed the way of managing data in all sectors including the building sector. Because of this, confidentiality and security are constantly at risk in the construction industry (CI) (Bendovschi, 2015). These risks involve extortion, pharming, spamming, phishing, spoofing, spyware, viruses and Trojans, stolen hardware (mobile devices or laptop), password sniffing, website defacement, and breach of access (Bendovschi, 2015; Amal and Venkadesh, 2022). Moreover, Bendovschi (2015) stated that for businesses of all sizes as well as individuals, cyber-attacks are becoming more and more an everyday reality, and little is widely understood about cybercrime or cyberattacks. Cyberattacks, also called computer network attacks (CNA) refer to the systematic manipulation of computer systems, organisations, and networks, dependent on technology. Additionally, cyberattacks use malware to alter data, logic, or computer codes, resulting in disruptive effects that can endanger data and result in cybercrimes such as theft of identity and data (Techopedia, 2019). The risks will be focused on in the following sections.

2.1 Phishing

Phishing is a type of social engineering technique or cyber security problem in which an intruder tries to fraudulently steal the sensitive credentials of legitimate users by imitating electronic communications in an automated fashion from a trusted or public organisation. These techniques also include fraudsters attempting to get the user to divulge their private information through the exploitation of human flaw rather than software flaws (Jakobsson and Myers, 2006; Alswailem and Aladullah, 2019). Alswailem and Aladullah (2019) and Alabdan (2020) stated that besides using email, phishing has expanded to include voice over internet protocol (VOIP), text messages, SMS, and social networking sites. The above-stated ways through which phishing operate are used in the construction industry for communication purposes, thus the building sector is also exposed to phishing. Syiemlieh et al. (2015) listed some of the various existing phishing which are deceptive phishing, domain name-based phishing, man-in-the-middle phishing, content-injection phishing, key loggers, and screen loggers. Phishing involves encouraging many people to visit fake websites or sending emails that request sensitive information (Palmer, 2020). Vayansky and Kumar (2018) reminded us that phishing is a criminal activity that illegally obtains companies' private data like passwords and usernames by trying to deceive common websites users by emailing them fake website's versions to supply their credentials with the aid of different social engineering techniques.

2.2 Spyware

Spyware is a kind of malware used for spying on computer-user behaviour. This malware can gather the user's habits and information such as browsed websites especially through advertisements, installed applications, and downloaded programmes. All these operations can also be conducted by a trusted employee to harm the company for various reasons (Rountree, 2011 and Mahesh et al.,2020). It is installed without the permission or authorisation of the owner on a device. After installation, it infiltrates the computer, studies the user's behaviour and violates their privacy by exposing their private information to outsiders (Stafford and Urbaczewsk, 2004; Rouse et al., 2020). Mahesh et al. (2020) further explained that spyware captures data that often includes validation credentials that could be used to gain access to infested computer information systems in the future. Users typically use the same username and PIN across multiple computer systems; as a result, the stolen identifications could be used to log in to other nearby computers that are still not infected. Once access is acquired, more data theft or malware installation may occur, just as it did for other computers. The construction industry is vulnerable to spyware because workers also use the company's website and other internet services.

2.3 Malware

Malware is described as any malicious program code that has been inserted, altered, or removed from a software system to frequently and deliberately cause harm to the system's intended function (Namanya et al., 2018 and Diaz, 2020). Malware attackers are also interested in the construction sector's need software to store their data as well maintain their computers, therefore is it easy to harm the entire company through the various software. Sharp (2017) defined malware as a common term used to describe all forms of malicious software used by the attacker to violate data security, availability, confidentiality, and integrity. In addition, Sharp (2017) also suggested that in the broadest context, the term software should be understood properly because the malicious effect might make use of macros, executable code, scripts, interpreted code, among others. Namanya et al. (2018) highlighted that malware can trigger knowledge, money, and life loss and poses a major challenge to advances in technology, so it is vital to deal with it as soon as possible. The different types of malware are viruses, ransomware, worm, bad rabbit, trojan horse, backdoor, and logic bomb (Bendovschi, 2015). Viruses, ransomware, worm, and bad rabbit are briefly discussed below.

2.3.1 Viruses

A computer virus is one of the most popular programme or executable file that can propagate through laptops and networks by creating duplicates of itself, usually without the user's knowledge (Aycock, 2006, Diaz, 2020). Aminuddin and Abdullah (2019) and Diaz (2020) stated that the virus infects other services, and spreads all over the network, and does whatever action the user would, including removing files, modifying file data, deleting all data on a hard disk and transmitting sensitive information over a network. The actions of the virus depend on the harm purpose for which it was designed. On top of that, this computer virus malware attempts to infect other files located in the computer system where it is housed and change its default behaviour when executed. Al Daoud et al. (2008) and Chakraborty (2017) listed the various strategies used by viruses to deceive virus fighters such as overwriting virus, prepending virus, encrypted virus, malicious mobile code, among others. All users of personal computers including those from the construction sector need to have robust frameworks for virus security to face increasing computer virus threats due to the high rise in computer use. The use of computer is seen through the use of excel XLS documents, word documents as well as MP3 documents (Chakraborty, 2017). If a computer user opens an infected document, the virus can install itself and infect any subsequent documents too (Konakalla and Veerank, 2013 and Diaz, 2020). Virus attacks on a machine are dangerous, resulting in more machine damage through the use emails programs (Aminuddin and Abdullah, 2019).

2.3.2 Ransomware

According to Aminuddin and Abdullah, (2019) and Diaz (2020), ransomware is a type of harmful software that in some way disables a computer's functionality while operating and shows a message which requires payment or wages to restore the system functionality. The word 'ransomware' is reflecting the way the malware works: this implies that it is a malware that demands payment for stolen personal information, features, or information restricted to user access (Kharraz et al., 2015). Deo and Farik (2016) described ransomware as a form of malware that propagates like a worm that restricts users' access to their own devices and users from the construction industry are not exempted. This is done either by locking the device's screen or encrypting and locking the user's files until a certain amount of money is paid. Shah and Farik (2017) categorized ransomware into two which are encrypting (Cryptolocker, Locky, Cryptowall) and locker ransomware (Winlocker).

2.3.3 Worm

A computer worm refers to software that propagates security or policy vulnerabilities through a network of commonly used services with the main objective of denying services to the user (Venkatraman et al., 2019 and Diaz, 2020). Chakraborty (2017) noted that the difference between worms and viruses is that worms do not need to connect themselves to a current application or infected files to propagate, thereby requiring user intervention to facilitate their propagation. Worms are computer programs that affect a computer or network's storage devices, install themselves on the system and then replicate information without the user's knowledge (Aycock, 2006; Diaz, 2020). This specific virus applies to the construction industry as well by the simple fact that the internet and computers are used to facilitate the execution of projects.

2.3.4 Bad Rabbit Ransomware

Bad Rabbit is a form of malware that uses a certain resource class on a computer system, such as message buffers, file space, or process control blocks (Sharp, 2017). According to Celiktas (2018), Bad Rabbit corrupted computers worldwide in September 2017 by confirming itself to be an Adobe Flash Player update patch. Its expansion is done on infected websites through drive-by downloads. Very often Bad Rabbit infections fool visitors by sending false alerts saying that there is a need to urgently update their Adobe Flash player that will lead them into clicking on the malware, which is, in fact, the real virus (Comodo Antivirus, 2019). The construction industry cannot be exempted from such attacks.

2.3.5 Trojan horse

Trojan Horse is a type of virus that needs the initial user's permission by accident or willingly based on the tricks that intruders put in place to run on the computer or a smartphone. This harmful program gets loaded user's device (phone or laptop) then communicates with the harmful application writers via a command and control (C&C) server to collect attackers' commands. The command could be to expose user personal information, subscribe to premium services, and distribute malware to other android applications (Aminuddin and Abdullah, 2019). Trojans were named after the Greek historical Trojan Horse strategy, where something mysterious and unpredictable comes in a harmless and helpful package that a user would usually accept; generally, a free download of software (Konakalla and Veeranki, 2013 and Aminuddin and Abdullah, 2019). Roy et al. (2013) and Diaz (2020) defined Trojan horses as E-mail viruses capable of stealing information destroying the computer network, or remote controlling and access of the user system or backdoor. As a result, users in this case construction stakeholders should be careful while exchanging information; because these viruses tend to be user-friendly programmes but may likely have some impure motives and usually carry some payload, such as methods and viruses for remote access. Gudipati et al. (2015) stated that Trojan horses are analogous to any computer programme running on our machines. Trojan horse claims to make the user perform an acceptable action; however, it performs actions that the hacker determines, to manipulate the program. This is also applicable to the construction sector because of the high usage of computers in the project's execution.

2.4 Hacking

Hacking refers to illegal access to a computer network and the hacking act kills the entire data, as well as shut computer programmes entirely based on their needs (Roy et al., 2013 and Odlyzko, 2019). Konakalla and Veeranki (2013) and Lohani et al. (2019) noted that hackers may be career-criminal men who are qualified and experienced at using computers and also specialised in human manipulation to extract important information from them. This is the reason why the construction industry should invest heavily in cybersecurity because they use both technological tools and human beings during the project execution. The authors added that if a leak point (vulnerability) is analysed and found in the target network, they can find ways to reach the device and apply their harmful activities. They are unpredictable because they may use diverse types of attacks or create their strategies of attacking the computer system and human tricks.

2.5 Distributed denial of service

As discussed previously in this study, there are various types of malwares. This harmful software uses social engineering to manipulate human and deceive them by leading to click on malicious links send in messages or emails to install itself in the computer system. In most cases, this result in a denial of service (DoS) until ransom is paid to the cyber attackers (Diaz, 2020). According to Panimalar and Khan (2018) and Madeti and Singh (2017), this attack starts with a computer program that is designed to manipulate a large number of computers at once and create botnets which are robotic networks between computers. Attackers utilise these botnets to launch DoS attacks effectively. After the attack is launched, the controlled networks overwhelm the victim's private computer (PC system) with multiple requests and messages causing crucial functions to be brutally stopped. Basically, a distributed denial service (DDoS) takes place when a large number of vulnerable and geographically distributed hosts as well as other networked computers are utilised to perform more DoS activities by attacking information provider’s services (Bhatia et al., 2018). The different types of DoS and DDoS incorporate teardrop attacks, TCP SYN flood attacks, and ping-of-death attacks (Amal and Venkadesh, 2022). Based on the discussion above, the construction sector must be aware of the distributed denial of service they are exposed to because of the internet services they use on daily basis on and off the construction site.

2.6 Man-in-the-middle attack

The definition of a man-in-the-middle attack (MIM or MITM) in PC security and cryptography refers to an intrusion in which the hacker transfers furtively and feasibly, a change in the communication between two targets. This is especially if the targets believe that they are communicating straightforwardly without the involvement of a stranger (Mallik et al., 2019). Because communication among stakeholders is a key requirement for project success in the building sector, therefore, intruders are easily attracted by the construction industry. Cryptography is a mathematical method or technique that attempts to keep the details stored in the data secret so that the unauthorised parties cannot know the details or science of secret writing (Rahim and Ikhwam, 2016). Furthermore, Rahim and Ikhwam (2016) suggested that the attacker requires access to a Wi-Fi switch that is unsecured or ineffectively anchored in the conventional man-in- the-middle attack. of the man-in-the-browser (MITB) malware.

2.7 Drive-by download attack

A drive-by download attack refers to a very stealthy and popular form of attack that hackers undertake to spread viruses and gain unauthorized access to an information system. This form of assault occurs when a computer is infected with malicious software simply by visiting a website (Ama and Venkadesh, 2022). The key objective of these attacks is to exploit the vulnerabilities in the user’s browser of or in the browser’s plugins to make the victims join bonnets (set of internet devices that are already infected by a common malware type) through the download of malware in their computers (Cova et al., 2012). This concern also the construction sector as attackers can trick construction workers into downloading some harmful application without knowing.

2.8 Password attack (Cracking)

Passwords are the most widely used method of user authentication, and obtaining them is a successful attack approach. A credential hack is when a user's credentials are illegally taken or decrypted. The user's password can be discovered by looking around the user's workstation, assuming, acquiring a login database, observing and tracking the network connection to recover the plaintext password (Ama and Venkadesh, 2022). Martin and Tokutomi (2012) stated that there are several various ways of authenticating a system's users such as the presentation of a physical object like a key card, proof of identity (fingerprint, face recognition), or to use something that the only user knows, like a pin or password.

2.9 Structured query language (SQL) injection attack

Ama and Venkadesh, (2022) explained that attacker who wants to do SQL injection can change a standard SQL query to take advantage of unproven database flaws. On top of this attackers can also exploit misfiltered characters to modify SQL statements. An SQL injection is a type of web application where the attacker provides SQL code to a web form user input-box to gain unauthorised and unrestricted access (Kindy and Pathan, 2012). Mavromoustakos et al. (2016) explained that if a user uses the SQL command and queries without validation and encoding, an SQL injection attack can happen. This occurrence will also enable the attackers’ tricks which allow the application to change information or execute unintended commands in various computers of different construction companies across the world.

2.10 Eavesdropping attack or snooping attack

According to Ama and Venkadesh, (2022), hackers compromise data transmitted by electronic devices in eavesdropping attacks. This happens when attackers use an unprotected network to communicate and evaluate data delivered and received. During this form of attack, an attacker may use a sniffer to eavesdrop on a computer or server in order to steal data while it is being transported. Moreover, it is difficult to detect it because there is no abnormal behavior during network transmission (Amal and Venkadesh, 2022). Modern eavesdropping can be achieved using current technologies such as concealed microphones and recorders, this is the simple act of listening to other people talking without them knowing it (Techopedia, 2019). Kröger and Raschke (2019) reported that apart from numerous other mobile device privacy issues, several people suspect that their smartphones are eavesdropping secretly on them. A snooping attack is a form of cyber-attack that steal information and it is transmitted via smartphones, laptops, and other linked devices over a network that access victim's sent or received data through network communication (Frankenfield, 2020).

Other security challenges

Cyber-crimes are becoming more sophisticated by employing new methods. Cybercriminals continuously change current malware fingerprints in order to exploit new technology holes. In other circumstances, they hunt for new technology's distinctive qualities to find holes in viral infiltration and they are attempting to take advantage of rapidly evolving IT and the large number of active users in order to acquire quick and easy access to a huge number of people (Amal and Venkadesh, 2022). Diaz (2020) opined that the use of firewalls to promote the establishment of logical perimeter safeguards is a great step to data management risks. Namanya et al. (2018) explained that that integrity checking is seen as critical in detecting any system alterations. It is, nevertheless, more of a strategy for event recovery than for malware (virus, Trojan, ransomware, worm) infection prevention. In this method, the digest of the program or file is calculated using a hashing function such as md5 sum, Sha1or Sha256, and saved in the data repository. Afterwards, the program/file digests are computed once more and compared to the previously calculated hash to verify whether the file has been altered or not (Namanya et al., 2018). The installation of anti- virus and anti- malware, malware scanners can help in the protection of data. This is because these techniques cannot spot or recognise malware but also remove them or disinfect infected files (Amal and Venkadesh, 2022). Diaz (2020) suggested that training of all the staff members, implement backup systems to always have a copy of lost information at any time. These methods will prepare all the stakeholders to know hackers operate, notify them of any detected malware and provide a plan B solution if even attackers succeed their mission especially in case of ransomware. According to Alswailem and Alabdullah (2019), machine learning (ML) has strong predictive power that can contribute to the security of data. It analyses and learns the phishing website's or malware characteristics and then forecasts new phishing and malware traits. Numerous strategies are available, including nave Bayes (NB), support vector machines (SVM), artificial neural network (ANN), decision tree (DT), RF, as well as Bayesian net (BN). The accuracy of attack detection varies depending on the algorithm as explained Alswailem and Alabdullah (2019). Transferring cybersecurity to a third party to use their expertise to protect the project information system. Additionally, cybersecurity systems should be continuously challenged with ethical hacking tests to identify unauthorized changes and previously undiscovered exposures, as well as rectify deviations before being replicated (Diaz, 2020). A regular password changing for access control purposes, use of data authentication methods, intrusion detection system to detect every potential treat and inline DDoS mitigation to intensify security by prevent the DDoS from processing in the network (Lal et al., 2016; Tiwari et al., 2017 and Allot, 2018). Nowadays, honeypots which are gadget used to prevent intrusion attacks by distracting and collecting information to have enough knowledge on how hackers operate (attack patterns) in order to formulate strong countermeasures or solutions against potential cybersecurity risks (Amal and Venkadesk, 2022). The construction sector can highly benefit from these cybersecurity measures if all stakeholders adopt them and make use of them at all the time. If these are neglected, attackers find their way into the information system, prevent the good function of the system as well as delay project execution activities.

3. RESEARCH METHODOLOGY

The study adopted a systematic literature review approach to give a detailed theoretical background overview for the study which involves extraction of published articles on the data management risks from renowned academic databases such as SCOPUS, Web of Science and Google Scholar. The targeted population for this research work was professional quantity surveyors, architects, civil, mechanical, and electrical engineers practicing under a firm, company, organisation, or institution within the Gauteng province, South Africa. This choice was based on their level of knowledge and experience in contributing to answering to this work' research objectives and they were selected from their respective professional bodies. A random sampling technique was used in carrying out this research because this sampling technique ensures that each part and set of individuals has an equivalent possibility of being incorporated into the sample. A sample size of 115 professionals was used to conduct this research study but 81 professionals responded. The data collection tool applicable to this research work was a well-structured questionnaire that provided the respondents with variables to rank based on their knowledge and opinions. In addition, a closed-ended-questions were used on the questionnaire used in this study. A five-point Likert scale was used for this study to assess the experience of respondents regarding the cyberattacks risks associated with data management. The five-point Likert scale was transformed into a mean item score (MIS) for each question under the assessment of data risk management on construction projects in the industry 4.0. To analyse the retrieved data obtained, the statistical package for the social sciences (SPSS) was used. The research objective was analysed using Mean Item Score (MIS), Standard Deviation (SD) and Non- parametric test. The MIS was used to rank variables based on the participants' opinions while the descriptive statistics was adopted to analyse the demographic information of the respondents. The non-parametric test Kruskal-Wallis H was assessed to determine whether there was a discrepancy in participants' opinions from different groups (Akinradewo et al., 2022). For validity test purposes, an expert statistician reviewed all the completed questionnaires to validate the items' quality to make sure that the measure is of high quality. Survey reliability refers to the consistency or dependability or stability level of a research tool (questionnaire). Cronbach's alpha was used to test the study instrument's reliability, and the outcome indicated an alpha value of 0.902, indicating that the data obtained from the well-structured questionnaire survey can be trusted.

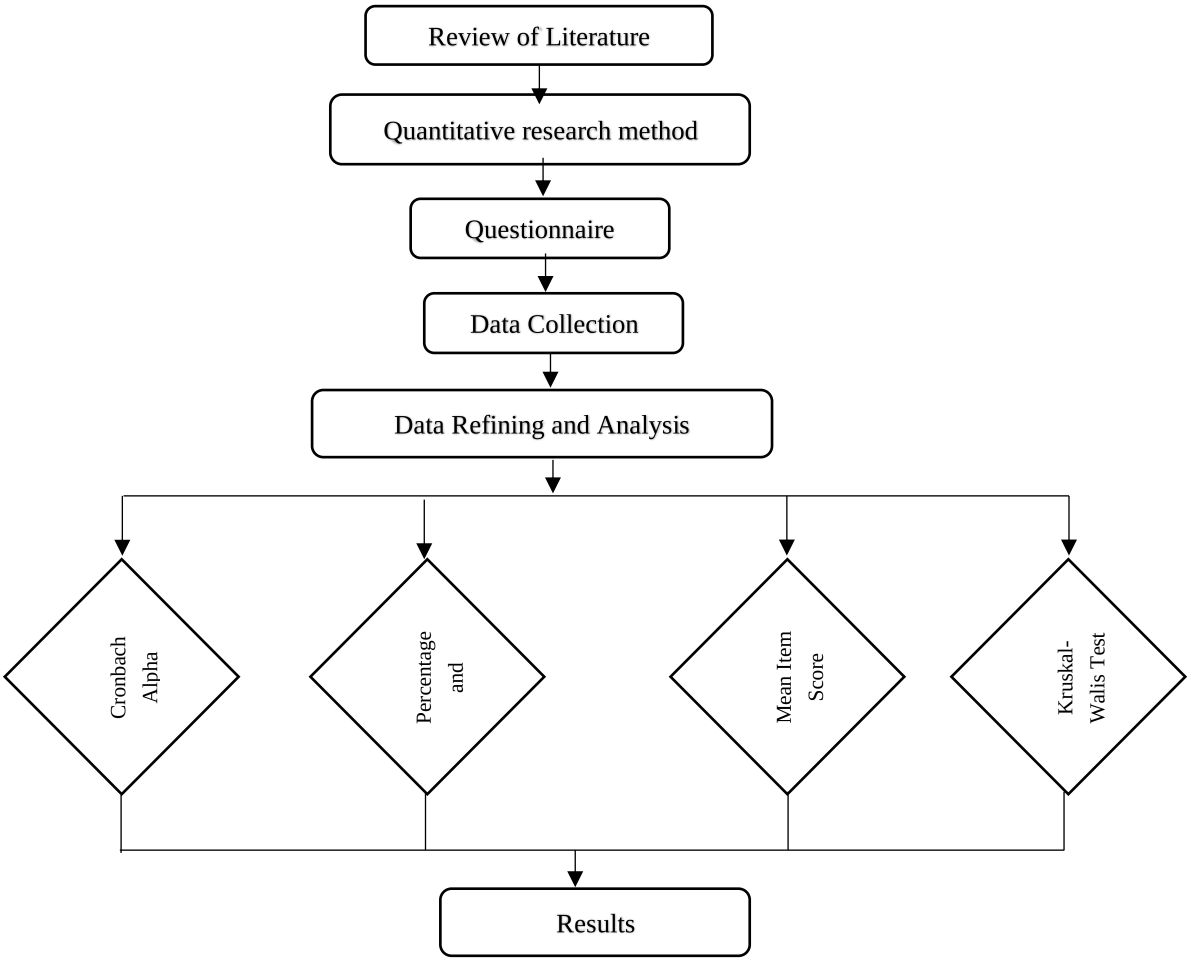

Fig. 1: Research Methodology

4. FINDINGS AND DISCUSSION

4.1 Biographical data results

The findings relating to respondents' professional affiliations revealed that all respondents were qualified to answer the specifically designed questionnaire for this study because they had the necessary qualifications as most of the respondents have bachelor's degree representing 32% followed by those with a master's degree representing 30%, honours' degree representing 17%, post-matric certificate or diploma 14% and a doctorate degree representing 7%. Also, 7% of the respondents were architects, 27 % were quantity surveyors and 12 % were civil engineers. The industrial, mechanical, and electrical engineers all numbered 1% each, while 20% of the participants were construction managers, and 14 % were construction project managers 14%. 16% indicate that they were representing other construction project members as shown on Table 1. The findings also showed that respondents had sufficient years of experience to provide suitable responses to achieve the objectives of research study since 86% of respondents had experience ranging between 1-5 years and 20 years of experience. Lastly, the findings on the respondents' level of awareness of data management revealed that of the 81 respondents, 74 respondents had a score of level of awareness ranging between 5/10 to 10/10.

TABLE 1: Background information of respondents

Educational Qualification	**Frequency**	**Percent**
Doctorate	6	7.0
Masters	24	30.0
Honours	14	17.0
Bachelor	26	32.0
Post-matric certificate	11	14.0
Total	81	100
Professional Affiliation	**Frequency**	**Percent**
Construction project manager	11	14.0
Construction manager	16	20.0
Engineers	13	15.0
Quantity Surveyor	22	27.0
Architect	6	7.0
IT Professionals	13	16.0
Total	81	100
Experience of respondent	**Frequency**	**Percent**
Less than 12 months	11	14.0
1 to 5 years	30	37.0
6 to 10years	23	28.0
11 to 15 years	11	14.0
16 to 20 years	6	7.0
More than 20 years	0	0.0
Total	81	100

4.2 Mean Item Score and Non-Parametric Test for Risks of Construction Data Management in The Fourth Industrial Revolution Era

The Kruskal-Wallis H test was conducted to analyse the respondents' responses concerning the risks of construction industry data management in the fourth industrial era. According to the respondents, 'viruses' with a mean score of 4.28, Kruskal-Wallis H of 21.018 and asymp. Sig. value of 0.007; 'hacking' with (M= 4.21; Kruskal-Wallis H= 8.463; asymp. Sig. value= 0.390); and 'password attack (cracking)' with (M= 4.11; Kruskal-Wallis H= 10.930; asymp. Sig. value= 0.206) were ranked as the first three data risks; while 'worm' with (M= 3.65; Kruskal-Wallis H= 14.441; asymp. Sig. value= 0.071); 'Bad Rabbit ransomware' with (M= 3.57; Kruskal-Wallis H= 13.675; asymp. Sig. value= 0.091); and finally, 'Structured Query Language (SQL) injection attack' with (M=

3.51; Kruskal-Wallis H= 20.445; asymp. Sig. value= 0.009) were ranked as the three last data risks as shown in table 2.

TABLE 2: Mean item score and non-parametric test for risks of construction data management in the fourth industrial revolution era

Risks of construction data management in the fourth industrial revolution era	Mean	Kruskal-Wallis H	Asymp. Sig.	R
Viruses	4.28	21.018	0.007	1
Hacking	4.21	8.463	0.390	2
Password attack (Cracking)	4.11	10.930	0.206	3
Man-in-the-middle attack (MIM or MITM)	3.90	11.120	0.195	4
Drive-by download attack	3.79	12.115	0.146	5
Malware	3.77	10.416	0.237	6
Distributed Denial of Service (DDoS)	3.75	12.394	0.134	7
Eavesdropping attack (snooping or sniffing attack)	3.74	16.773	0.033	8
Trojan horse	3.72	8.384	0.397	9
Ransomware	3.70	19.791	0.011	10
Spyware	3.70	8.802	0.359	10
Phishing	3.68	10.752	0.216	12
Worm	3.65	14.441	0.071	13
Bad Rabbit ransomware	3.57	13.675	0.091	14
Structured Query Language injection attack	3.51	20.445	0.009	15

The non-parametric test using the Kruskal-Wallis H test indicated that there is a statistically significant difference in the opinion of the respondents concerning the following factors: viruses and eavesdropping attack or snooping or sniffing attack. The differences in the opinion of the respondents (Architects, Quantity Surveyors, Civil engineers, Industrial, Mechanical, Electrical engineers, Construction Managers, and construction project managers, and IT professionals) can be due to their point of view concerning these variables. There are differs opinion due to the fact that each respondent as unique experiences in handling data management. For instance, viruses were ranked lower by mechanical engineers compared to the other eight engineers while eavesdropping attack or snooping or sniffing attack was ranked lower amongst the quantity surveyors as compared to the eight remaining groups.

The findings of this study indicated that viruses, hacking, password cracking, man-in-the-middle attack (MIM or MITM), and drive-by download attack were among the most frequent risks encountered in the construction industry. Aminuddin and Abdullah (2019) and Diaz (2020) posited that viruses are the most frequent data management risk. Viruses in the construction industry refer to malware that attempts to infect other files and change its default behaviour when executed (Amal and Venkadesh, 2022). Because of viruses, files are removed, modified, and even destroyed. This brings disputes and misunderstanding while undertaking a construction project as well as a need to rework, which is a waste of time and money. Hacking, which was also viewed by participants in this study as being the most frequent risk is described by Roy et al. (2013) and Odlyzko (2019), as taking place when an attacker accesses the company's computer to kill all the data and programmes found in it. This makes hacking dangerous as it results in the destruction of all the company's, project's and employee's data. This can lead to work stoppage, time wastage and cost overruns on the company's overheads. Amal and Venkadesh (2022) claims correspond with those of this study that password cracking is among the highest types of data management risks. Thus, construction professionals need to know how attackers operate when it comes to password cracking.

Password cracking happens when attackers guess all the numbers, symbols and letters used in a password and in this way gain access to the user's computer information and puts private information at risk (Ama and Venkadesh 2022). Due to password cracking the company's data can be easily stolen, modified, and even destroyed and complicate the project execution process.

Furthermore, this study indicated that man-in-the-middle attack (MIM or MITM) is another major factor of data risk management. The work of Rahim and Ikhwam (2016) Mallik et al. (2019) all agree that this form of attack is a major risk to data management. Man-in-the-middle attacks occur when the attacker transfers furtively and possibly change the communication between two targets who believe that they are communicating with each other directly (Mallik et al., 2019). All construction professionals need to be aware of this kind of attack because it puts sensitive project's data at risk, especially the company's finances, for example, money can be sent to the wrong person. This study indicated that participants identified drive-by download attack as another main risk to data management. This supports the work of Cova et al. (2012) and Ama and Venkadesh (2022) who suggested that drive-by download attack is a frequent risk to data management. A drive-by download attack happens when the victim is tricked onto a malicious webpage that contains code, written in the language of JavaScript (Provos et al, 2008). This is another risk to data management that construction professionals need to pay attention to as it can also lead to private data being permanently at risk as they could unconsciously download malware onto their computers.

The other types of risks recognised by the participants included malware, distributed denial of service (DDoS), eavesdropping attack or snooping or sniffing attack, Trojan horse, ransomware, spyware, phishing, worm, Bad Rabbit ransomware, and structured query language injection attack. Bendovschi (2015) and Sharp (2017) posited that malware is a type of risk to data management. Namayna et al. (2018) described malware as any hostile code that has been used to deliberately cause harm to the system's intended function. Risk management of data needs to address the dangers of malware as soon as possible to prevent intruders from harming the information system. In line with this research work, Bhatia (2018) posited that distributed denial of service (DDoS) is among the risks of data management. Amal and Venkadesh (2022) stated that Denial of Service (DoS) occurs in a computer network when a cyberattack uses up all of the system's resources, making it unable to respond to service requests. Bhatia (2018)stated that when DoS attack traffic includes multiple sources, it is called the Distributed Denial of Service (DDoS) attack. This is a harmful risk that construction professionals need to pay attention to avoid inaccessibility to communications and other services that a computer can provide to enhance project delivery excellence.

According to Kroger and Raschke (2019), eavesdropping attacks or snooping or sniffing attacks are among the risks of data management and the participants in this study also recognised this. An eavesdropping attack may inject software by direct entry or a virus or other malware into a compromised computer to practice fraudulent activities. In addition, the attacker does not require any permanent link to the device to operate an eavesdropping attack (York, 2010). All of those involved in a construction project needs to be more careful about snooping to avoid all forms of spy, fraud, and theft of private information which can easily compromise the execution of construction projects. Gudipati et al.'s (2015) and Aminuddin and Abdullah (2019) findings agree with those of this study that the Trojan horse is a significant risk to data management. Trojan horse is a user-friendly appearing virus stealing information, or destroying the computer network (Diaz, 2020). Furthermore, Trojan horse forces the user to perform acceptable actions determined by the hacker who manipulates the programme (Gudipati et al., 2015). Most of the information in the construction industry are exchanged through e-mails for rapid and remote communication. Attackers can easily access the company system and practice malicious activities through a Trojan horse attack. Thus, stakeholders must do their best to apply security measures for information protection.

Having the same view as participants in this study, Aminudiin and Abdullah (2019) and Diaz (2020) posited that ransomware is also a type of risk to data management. Ransomware is a form of malware that propagates like a worm and restricts users to access their device, either by locking the screen of the device or by encrypting and locking files of the users until a ransom is paid (Deo and Farik, 2016). Without knowledge or the measures needed to overcome these risks, companies can lose a lot of money as well as important project information. Mahesh et al. (2020) claims align with those of this study that spyware represents a data management risk. Mahesh (2020) insisted that this harmful action of collecting project or personnel data whenever installed on a device without permission can be conducted by an insider. Therefore, stakeholders should also be aware of stakeholders can harm stakeholders and the overall project. On top of that, because stakeholders trust each other, an insider can easily harm the all project and get away without any suspicion. Alswailem and Aladullah (2019) and Alabdan (2020) posited that phishing a risk to data management. According to Palmer (2020), attackers through email push and motivate users to reveal their private information through the use of emails. This can even extend to hackers sending malicious links to the target that will lead straight to counterfeit websites. Construction professionals cannot be exempted from this type of trick sometime by curiosity, thus, falling into the trap. Worm was also identified as a way that ackers find to attain project data. Venkatraman et al. (2019) support this by explaining that preventing the users from accessing information files is the goal every hacker. Diaz (2020) added that worms have the ability to not only execute itself but also spread at a great speed whenever vulnerabilities are detected in the any other system. Thus, construction companies need to protect their information system as well as avoid this risk as it can easily multiply itself and be difficult to control in a long run. Furthermore, Sharp (2017) posited that bad rabbit ransomware cannot be excluded from risks to data management. Comodo Antivirus (2019) further described that this risk shows a sense of emergency by pushing targets to update their adobe flash player while the intention is to lead targets to download malware that will lock computer resources. Most people would like to have their software to be up to date, thus, construction project parties can easily fall for this and compromise their private information. Lastly, SQL injection attack which is also considered by respondents to the study as a risk is supported by Ama and Venkadesk (2022) and Mavromoustakos (2016). This technique aim is to completely destroy the information container or repository (Ama and Venkadesk, 2022) through the injection of a SQL code via the means of web pages input (Kindy and Pathan, 2012) Most construction professionals do not pay attention to the validation of SQL command and queries which represent an open door to attackers (Mavromoustakos, 2016). This may be due to the fact that the construction sector already involves too many tasks to accomplish (design, construction execution). Adding the validation of SQL queries can be overwhelming and not part of their domain. Hence, it is better to associate IT workers for the SQL validate and keep the project data safe.

Implication of findings

The empirical findings are in tandem with facts established from the literature review and all the variables ranged between 4.28 and 3.51 of a five-point Likert scale. It is unmistakable that these different forms risks of data management are encountered during project lifecycle and can significantly impact the execution of a construction projects. This is owing to carelessness of stakeholders concerning the management of data. viruses most of the time that are fraudulently injected into construction project devices means of communication. Viruses are the most frequent data management risks that destroy project data, thus, bringing data confusion, dispute and rework of the executed structure. These days Hijacking and password cracking are the common risks in construction projects. Intruders trying by all means to attain company's private data, they are able to manipulate employees and guess passwords put in place to protect important data. This is very dangerous because once the attackers succeed the information system control will shift from stakeholders to cybercriminals. It is highly expected from project parties to know that intruders can play the man-in-the-middle attack card to twist their conversations including financial conversation. As a result, they risk to lose large amount of project money if their tricks are not well known. With the high use of digitalisation in the construction sector, cyber attackers can take the opportunity to proceed with the drive-by-download attack especially if projects members are tempted to visit every webpage that is presented on internet which lead unwanted virus installation. The seizing of important data will follow, and its exploitation will be the next step. Still based on the variables' ranking, malware, DDoS, and ransomware are data management risks. Everything starts with a harmful code used or the installation of hostile software to commit crime against project data. After the code is used most of important data is altered against the will of the device owner, the attackers find a way to block the stakeholders access to the resources required for day-to-day activities such as memory and software on a computer. If the above explained problem comes from many various sources, then a DDoS takes place. Furthermore, this always lead to ransomware because whenever the resources including the file systems are not accessible to the user especially the help of encryption methods, the criminals take the opportunity to request money in exchange of resources restoration.

Eavesdropping attack is excluded from the risks to data management. Through this specific method, the information system can be permanently at risk as to attack usually listen stakeholder's communications go undetected. This is a very dangerous attacks as secret data can be recorded and used to construction destroy companies. Furthermore, project's parties are fooled through Trojan horse attacks because the hackers present good appearing and helpful software that is free of charge while criminals are simply preparing their way to access the information system. Moreover, the project's information system is also exposed to spyware, phishing, worm, Bad Rabbit ransomware, as well as structured query language injection attack. Spyware can provide from both insiders and outsiders. The aim of spyware is to gather sensitive information and use it against people and organisations. Many stakeholders think that attackers only come from the outside. Every stakeholder should put in mind that people can work for the same project without having the same center of interest. Thus, the top management need to be more careful of the protection of data. Curiosity can easily lead stakeholders to visiting fake website or giving away their private information through the use of phishing. Especially nowadays where money and promotions (e.g. sale of construction product materials) are the best way to attract targets. As construction project stakeholders, worm need to be avoided as they spread easily and prevent normal access to project data, thereby, penalising the execution of the project. It is the responsibility of stakeholders to make sure data their information system is far from bad rabbit ransomware. The attackers in these attacks look for a way to get money from the computer users through the encryption of information files. With the 4IR, the construction industry generates all types of data including videos and audios. Adobe flash player being an application that helps to view sophisticated data. The update of this application is crucial has it allows the viewing of data. Therefore, it is better for stakeholders to update willing the application on a regular basis without waiting for hackers to send update alerts. A risk such as SQL injection need to be taken into consideration all the time in the construction industry because employee's data, intellectual properties and trade secrets can be stolen easily. However, attacks like this need to be dealt with the association of IT officials as SQL query validation is required very often to secure data.

5. CONCLUSION AND RECOMMENDATION

The risks associated with data management on construction projects have been identified as follows in this study viruses, hacking, password cracking, man-in-the-middle attack (MIM or MITM), drive-by download attack, malware, distributed denial of service, eavesdropping attack or snooping or sniffing attack, Trojan Horse, and ransomware. The above-cited risks represent a threat to the construction sector because of the regular use of the internet and electronic devices for different purposes such as drawing of construction plans, easy communication among stakeholders as well as information storage. Electronic devices and the internet enable good work performance for satisfactory project outcomes while risks prevent better work performance on construction sites due to their effects on computers and project information. Therefore, construction professionals need to avoid the occurrence of these risks to enhance satisfactory project delivery and protect their project information. This risk avoidance will take place through the usage of the various data management measures such as blockchain, anti-virus, malware scanners, machine learning, honeypots among others. It can be concluded that using all the measures to protect information will enhance data availability, project continuity, good data quality (free from manipulation) as well as project delivery in the prescribed time. The study contributes to the body of knowledge by highlighting the various risks encountered in managing data in the construction industry which will assist professionals in the industry to pay attention to means of mitigating the identified cyber risks. This will keep stakeholders abreast of how simple negligence from their side can deeply affect the project data thereby affecting project delivery.

It is recommended that construction professionals should collaborate with cybersecurity developers or IT officers to be updated about the new types of risks and data risk management measures. Project parties are urged to adopt blockchain to strengthen their data secure and promote data availability and immutability as well as data backup option which will allow data continuity even if attackers succeed to completely destroy the data located on a computer. All construction workers should avoid clicking on links sent over emails or SMS. Stakeholders should avoid free things such as the download of software that are free of charge because anyone can be attracted by free stuff. The construction industry should employ a third party to deal with data risks at an advanced level. Additionally, all construction project parties require full training sessions on risks to data to prevent any types of intrusion into the company's information system. The limitation of this study is that this research was conducted in Gauteng province as there were travel restrictions due to COVID-19. Therefore, the results of this study cannot be generalized to a greater population. In future research studies, improvements should be made in terms of achieving a large sample size. By doing so, the construction sector will benefit from more knowledge on the risks associated with data management on construction projects. Moreover, further studies should be done to determine the basic IT knowledge that construction professionals must have as a key component that can help to prevent data risk.

ACKNOWLEDGEMENT

The authors would like to acknowledge the financial support provided by National Research Foundation, South Africa to fund this research.

REFERENCES

AICPA., 2013. An overview of data management. [Online] Available at: https://www.aicpa.org/InterestAreas/InformationTechnology/Resources/DataAnalytics/DownloadableDocuments/Overview_Data_Mgmt.pdf [Accessed on September 2021]

Akinradewo, O.I., Aigbavboa, C.O., Edwards, D.J. and Oke, A.E., 2022. A principal component analysis of barriers to the implementation of blockchain technology in the South African built environment. *Journal of Engineering, Design and Technology*.

Al Daoud, E., Jebril, I.H. and Zaqaibeh, B., 2008. Computer virus strategies and detection methods. *International Journal of Open Problems in Computer Science and Mathematics*, *1*(2), pp.12-20.

Alabdan, R., 2020. Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(168), pp 1-39.

Alaloul, W.S., Liew, M.S., Zawawi, N.A.W.A. and Kennedy, I.B., 2020. Industrial Revolution 4.0 in the construction industry: Challenges and opportunities for stakeholders. *Ain shams engineering journal*, *11*(1), pp.225-230.

Allot, 2018. Inline DDoS Protection versus Scrubbing Center solutions. [Online]. Available at: https://www.allot.com/resources/SB-DDoS-Protection-inline-vs-scrubbing-1.pdf [Accessed 21 March 2022].

Alswailem, A., Alabdullah, B., Alrumayh, N. and Alsedrani, A., 2019, May. Detecting phishing websites using machine learning. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

Amal, M.R. and Venkadesh, P., 2022. Review of Cyber Attack Detection: Honeypot System. *Webology*, *19*(1) pp. 5497-5514.

Aminuddin. N.I., Abdullah. Z., 2019. Android Trojan Detection Based on Dynamic Analysis. *Advances in computing and intelligent system. 1*(1) pp. 1-7.

Amusan L., Adewumi D., Ajao A.M., Ogundipe K.E. (2021) Adoption, Implementation Information and Communication Technology Platform Application in the Built Environment Professional Practice. In: Ahram T.Z., Karwowski W., Kalra J. (eds) *Advances in Artificial Intelligence, Software and Systems Engineering*. Springer, Cham. Pp 446-455. Https://doi.org/10.1007/978-3-030-80624-8_56.

Amusan L.M, Oloniju L.I, Akomolafe. M, Makinde. A, Nkolika-Peter P, Farayola. H and Faith. O., 2018. Adopting Information and Communication Technology in Construction Industry, *International Journal of Mechanical Engineering and Technology 9*(1), pp. 739–746.

Aycock, J., 2006. *Computer viruses and malware*. Heidelberg, Berlin: Springer Science & Business Media.

Ayodele, T.O. and Kajimo-Shakantu, K., 2021, February. The fourth industrial revolution (4thIR) and the construction industry-the role of data sharing and assemblage. In *IOP Conference Series: Earth and Environmental Science* (Vol. 654, No. 1, p. 012013). IOP Publishing.

Bendovschi, A., 2015. Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, pp.24-31.

Bhatia, S., Behal, S. and Ahmed, I., 2018. Distributed denial of service attacks and defense mechanisms: current landscape and future directions. In *Versatile Cybersecurity* (pp. 55-97). Springer, Cham.

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 & Electrical Engineering*, *90*, p.106897.

Celiktas, B. 2018 *The ransomware detection and prevention tool design by using signature and anomaly based detection methods*. (Doctoral dissertation). Istanbul Technical University.

Chakraborty, S., 2017. Module functioning of computer worm, PC virus and anti virus programs. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *2*(1), pp.94-99.

Comodo Antirus, 2019. Bad rabbit. How to prevent bad rabbit ransomware attacks. . [Online] Available at: https://antivirus.comodo.com/blog/comodo-news/bad-rabbit-ransomware/ [Accessed 7 June 2020].

Cova, M., Kruegel, C. and Vigna, G., 2010, April. Detection and analysis of drive-by-download attacks and malicious JavaScript code. In *Proceedings of the 19th international conference on World wide web. 26-30 April 2010. North Carolina, USA.* pp. 281-290. ACM Press.

Creswell, J.W. (2014), Research Design_Qualitative, Quantitative, and Mixed Method Approaches, 4th ed., SAGE Publications, doi: 10.2307/3152153.

Deo, S. and Farik, M., 2016. Information security: Recent attacks in Fiji. *International Journal of Scientific & Technology Research*, *5*(12), pp.218-220.

Dheyab, S.N., 2018, November. Electronic Management In Construction Projects. In *2018 1st Annual International Conference on Information and Sciences (AICIS)* (pp. 275-285). IEEE.

Díaz, R.M., 2020. Cybersecurity in the time of COVID-19 and the transition to cyber immunity. [Online] Available at: https%3A%2F%2Frepositorio.cepal.org%2Fbitstream%2Fhandle%2F11362%2F46511%2F1%2FS2000678_en.pdf&clen=478364&chunk=true [Accessed on 14 Marc 2022].

Drucker, P., 2014. *Innovation and entrepreneurship*. New York: Routledge.

Frankenfield, J., 2020. Eavesdropping attack. What is an eavesdropping attack? [Online]. Available at: https://www.investopedia.com/terms/e/eavesdropping-attack.asp [Accessed 20 November 2021].

Green, P.E., 2015. Enterprise risk management: A common framework for the entire organization. Oxford: Butterworth-Heinemann.

Gudipati, V.K., Vetwal, A., Kumar, V., Adeniyi, A. and Abuzneid, A., 2015, May. Detection of Trojan Horses by the analysis of system behavior and data packets. In *2015 Long Island Systems, Applications and Technology*. 1- 1 May 2015. New York, USA. pp. 1-4. IEEE.

Halttula, H., Haapasalo, H. and Silvola, R., 2020. Managing data flows in infrastructure projects-The lifecycle process model. *Journal of Information Technology in Construction (ITcon)*, *25*(12), pp.193-211.

Jakobsson, M. and Myers, S.(eds.), 2006. Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. New Jersey: John Wiley & Sons.

Kanimozhi, E.A., Suguna, M. and Shalini, S.M., 2019, March. Immediate detection of data corruption by integrating blockchain in cloud computing. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-4). IEEE.

Igwenagu, C., 2016. *Fundamentals of research methodology and data collection.* Saarbrücken, Germany:LAP Lambert Academic Publishing.

Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. (2015) Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, vol 9148. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-20550-2_1 Kindy, D.A. and Pathan, A.S.K., 2012. A detailed survey on various aspects of sql injection in web applications: Vulnerabilities, innovative attacks, and remedies. *arXiv preprint arXiv:1203.3324*.

Konakalla, A. and Veeranki, B., 2013. Evolution of security attacks and security technology. *International Journal of Computer Science and Mobile Computing*, *2*(11), pp 270-276.

KPMG., (2021). The value of information management in the construction and infrastructure sector. [Online] Available at: https://www.cdbb.cam.ac.uk/files/cdbb_econ_value_of_im_report.pdf [Accessed on 02 February 2022].

Kröger, J.L. and Raschke, P., 2019, July. Is my phone listening in? On the feasibility and detectability of mobile eavesdropping. In *IFIP Annual Conference on Data and Applications Security and Privacy.* 15-17 July 2019. Charleston, USA. pp. 102-120. Springer, Cham.

Lal, N.A., Prasad, S. and Farik, M., 2016. A review of authentication methods. International Journal of Scientific and Technology Research, 5(11), pp.246-249.

Leppikorpi, T., 2018. *Utilizing information systems in inter-organizational collaboration and information sharing* (University of tampere).

Lohani, S., 2019. Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research*, *4*(1) pp. 385-395.

Madeti, S.R. and Singh, S.N., 2017. A comprehensive study on different types of faults and detection techniques for solar photovoltaic system. *Solar Energy*, *158*, pp.161-185.

Mahesh, V. and KA, S.D., 2020, July. Detection and Prediction of Spyware for user Applications by interdisciplinary approach. In *2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE)* (pp. 1-6). IEEE.

Mallik, A., Ahsan, A., Shahadat, M. and Tsou, J., 2019. Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, *3*(2), pp.77-92.

Maritz, M.J. and Hattingh, V., 2015. Electronic communication in the construction industry. *Journal of Engineering, Design and Technology, 13*(1), pp 74-93.

Martin, S. and Tokutomi, M., 2012. Password cracking. University of Arizona: Computer Security Reports Csc566.

Mavromoustakos, S., Patel, A., Chaudhary, K., Chokshi, P. and Patel, S., 2016, December. Causes and prevention of sql injection attacks in web applications. In *Proceedings of the 4th International Conference on Information and Network Security. 31October-1 November 2016.* Johannesburg, South Africa. pp. 55-59. Association for Computing Machinery.

Odlyzko, A., 2019. Cybersecurity is not very important. *Ubiquity*, *2019*(June), pp.1-23.

Oesterreich, T.D. and Teuteberg, F., 2016. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. *Computers in Industry, 83,* pp.121-139.

Ozumba, A.O.U. and Shakantu, W., 2018. Exploring challenges to ICT utilisation in construction site management. *Construction Innovation. 18*(3), pp 1471-4175.

Palmer, D (2020) ZDnet, 2020. What is phishing? Everything you need to know to protect yourself from scam emails and more **[**Online]. Available at: https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/ [Accessed 20 April 2020].

Panimalar, A., Pai, G. and Khan, S., 2018. Artificial intelligence techniques for cyber security. *International Research Journal of Engineering and Technology*, *5*(3), pp.122-124.

Perera, S., Nanayakkara, S., Rodrigo, M.N.N., Senaratne, S. and Weinand, R., 2020. Blockchain technology: Is it hype or real in the construction industry? *Journal of Industrial Information Integration, 17*(2020), p.100125.

Provos, N., Mavrommatis, P., Rajab, M. and Monrose, F., 2008. All your iframes point to us. [Online] Available at: https://www.usenix.org/legacy/event/sec08/tech/full_papers/provos/provos.pdf [Accessed 05 July 2020].

Rahim, R. and Ikhwan, A., 2016. Cryptography technique with modular multiplication block cipher and playfair cipher. *International Journal of Scientific and Technology Research*, *2*(6), pp.71-78.

Rotatori, D., Lee, E.J. and Sleeva, S., 2021. The evolution of the workforce during the fourth industrial revolution. *Human Resource Development International*, *24*(1), pp.92-103.

Rountree, D., 2011. *Security for Microsoft Windows system administrators: introduction to key information security concepts*. San Francisco: Elsevier.

Rouse, M., Brush, K., Gillis A. and Teravainen T., 2020. Spyware. [Online]. Available at: https://searchsecurity.techtarget.com/definition/spyware [Accessed 4 April 2020]

Roy, S., Nag, S., Maitra, I.K. and Bandyopadhyay, S.K., 2013. International Journal of Advanced Research in Computer Science and Software Engineering. *International Journal*, *3*(6), pp. 1706-1746.

Shah, N. and Farik, M., 2017. Ransomware: Threats, vulnerabilities and recommendations. *International Journal of Scientific & Technology Research*, *6*(06), pp.307-309.

Sharp, R., 2017. An Introduction to Malware. [Online]Available at: https://core.ac.uk/download/pdf/24847956.pdf [Downloaded: 25 December 2020].

Sony, M., 2020. Pros and cons of implementing Industry 4.0 for the organizations: A review and synthesis of evidence. *Production & Manufacturing Research*, *8*(1), pp.244-272.

Stafford, T.F. and Urbaczewski, A., 2004. Spyware: The ghost in the machine. *The Communications of the Association for Information Systems*, *14*(1), pp. 291-306.

Sun, D.Z., Mu, Y. and Susilo, W., 2018. Man-in-the-middle attacks on secure simple pairing in Bluetooth standard V5. 0 and its countermeasure. *Personal and Ubiquitous Computing*, *22*(1), pp.55-67.

Syiemlieh, P., Khongsit, G.M., Sharma, U.M. and Sharma, B., 2015. Phishing-An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation. *Proceedings of National Conference on Advances in Engineering, Technology & Management (AETM'15). 4-4 April 2015.* Haryana, India. pp.1-8. IOSR-JSE.

Talha, M., Abou El Kalam, A. and Elmarzouqi, N., 2019. Big data: Trade-off between data quality and data security. *Procedia Computer Science*, *151*(2019), pp.916-922.

Tanga O., Akinradewo O., Aigbavboa C., 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. Pp. 465-471. Https://doi.org/10.1007/978-3-030-80624-8_58

Tanga, O.T., Aigbavboa, C.O., Akinradewo, O.I., Thwala, D.W. and Onyia, M., 2021b, April. Construction Digitalisation Tools In South African Construction Industry: An Added Advantage. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1107, No. 1, p. 012230). IOP Publishing.

Tao, X., Liu, Y., Wong, P.K.Y., Chen, K., Das, M. and Cheng, J.C., 2022. Confidentiality-minded framework for blockchain-based BIM design collaboration. *Automation in Construction*, *136*, (2022) pp.104172.

Techopedia, 2019. Eavesdropping. [Online] Available at: https://www.techopedia.com/definition/13612/eavesdropping [Accessed 02 May 2020].

Terzi, D.S., Terzi, R. and Sagiroglu, S., 2015. A survey on security and privacy issues in big data. In 2015 10th *International Conference for Internet Technology and Secured Transactions (ICITST)* 14-16 December 2015. London, UK. pp. 202-207. IEEE.

Tiwari, M., Kumar, R., Bharti, A. and Kishan, J., 2017. Intrusion detection system. *International Journal of Technical Research and Applications*, *5*(2), pp.38-44.

Vasista, T.G. and Abone, A., 2018. Benefits, barriers and applications of information communication technology in construction industry: A contemporary study. *Int. J. Engineering and Technology*, *7*(3.27), pp.492-499.

Vayansky, I. and Kumar, S., 2018. Phishing–challenges and solutions. *Computer Fraud Security*, *2018*(1), pp.15-20.

Venkatraman, S., Alazab, M. and Vinayakumar, R., 2019. A hybrid deep learning image-based analysis for effective malware detection. *Journal of Information Security and Applications*, *47*, pp.377-389.

World Economic Forum., 2018. Creating a Shared Future in a Fractured World. [Online] Available at: https://www.weforum.org [accessed on 10 March 2022]

Xuming, L., Lina, C., Peng, J., Xiao, G. and Shuo, C., 2019, November. Current status and future prospects of data leakage prevention technology: A brief review. In *Journal of Physics: Conference Series* (Vol. 1345, No. 2, p. 022010). IOP Publishing.

Xu, M., David, J.M. and Kim, S.H., 2018. The fourth industrial revolution: opportunities and challenges. *International Journal of Financial Research*, *9*(2), pp.90-95.

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*, pp.1-16.

Zhang, N. and Yuan, Q., 2016. An overview of data governance. Economics Paper. [Online] Available at: https://www.researchgate.net/profile/Zhang-Ning-25/publication/321899578_An_Overview_of_Data_Governance/links/5a3867a8aca272a6ec1e8864/An-Overview-of-Data-Governance.pdf [Accessed on 23 June 2022].

Zhu, L., Wu, Y., Gai, K. and Choo, K.K.R., 2019. Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, *91*, pp.527-535.