CONSTRUCTION INDUSTRY COUNCIL
建造業議會

CIC Beginner's Guide on Construction Digitalisation – **Cybersecurity**

2024

Disclaimer

Whilst reasonable efforts have been made to ensure the accuracy of the information contained in this publication of Reference Materials, the CIC nevertheless encourages readers to seek appropriate independent advice from their professional advisers where possible. Readers should not treat or rely on this publication of Reference Materials as a substitute for such professional advice.

Enquiries

Enquiries on the Reference Materials may be made to the CIC Secretariat:

CIC Headquarters
38/F, COS Centre, 56 Tsun Yip Street,
Kwun Tong, Kowloon

Tel: +852 2100 9000
Fax: +852 2100 9090
Email: enquiry@cic.hk
Website: www.cic.hk

Copyright Notice

This Guide will only become truly useful if as many companies adopt it as possible. To that extent, it may be freely distributed and used in any format necessary, provided credit is given to the CIC.

Document Revision Tracking

Issue Date	Notes
October 2024	First publication

Table of Contents

Preface

The Construction Industry Council (CIC) is committed to seeking continuous improvement in all aspects of the construction industry in Hong Kong. To achieve this aim, the CIC forms Committees, Task Forces and other forums to review specific areas of work with the intention of producing Alerts, Reference Materials, Guidelines and Codes of Conduct to assist participants in the industry to strive for excellence.

The CIC appreciates that some improvements and practices can be implemented immediately whilst others may take more time for implementation. It is for this reason that four separate categories of publication have been adopted, the purposes of which are given as follows:

Alerts	The Alerts are reminders in the form of brief leaflets produced quickly to draw the immediate attention of relevant stakeholders to the need to follow some good practices or to implement some preventive measures in relation to the construction industry.
Reference Materials	The Reference Materials provide standards or methodologies generally adopted and regarded by the industry as good practices. The CIC recommends the adoption of the standards or methodologies given in the Reference Materials by industry stakeholders where appropriate.
Guidelines	The Guidelines provide information and guidance on particular topics relevant to the construction industry. The CIC expects all industry stakeholders to adopt the recommendations set out in the Guidelines where applicable.
Codes of Conduct	The Codes of Conduct set out the principles that all relevant industry participants should follow. Under the Construction Industry Council (Cap 587), the CIC is tasked to formulate codes of conduct and enforce such codes. The CIC may take necessary actions to ensure compliance with the codes.

To allow us to further enhance this publication for the benefit of the construction industry, we encourage you to share your feedback with us, after you have read this publication. Please take a moment to fill out the Feedback Form attached to this publication and send it back to us. With our joint efforts, we believe our construction industry will develop further and will continue to prosper in the years to come.

Executive Summary

The Beginner's Guide on Construction Digitalisation - Cybersecurity delves into the aspects of cybersecurity within the construction industry's digital evolution. This guide serves as a resource for construction practitioners, offering valuable insights and practical recommendations to security measures, safeguard sensitive data, and ensure uninterrupted operations in digital construction processes. By aligning with industry standards and best practices, practitioners can proactively address cybersecurity challenges at each phase of project development.

The guide underscores the significance of integrating cybersecurity measures into construction digitalisation projects, aligning with the Security Information Requirements (SIR) outlined in the CIC BIM Standards General. Through a structured triage process and the implementation of recommended actions like initiating a security-minded approach, developing security strategies, and collaborating with appointed parties to enforce security measures, practitioners can effectively mitigate risks and bolster the overall security resilience of digital projects.

Key topics covered include the definition of cybersecurity in construction digitalisation, emphasising the protection of digital building data and securing the Building Information Modelling (BIM) process. References to industry standards such as ISO 27001 and ISO 19650-5 highlight the importance of data protection, risk management, and security-minded information management in digital construction workflows.

The guide aims to equip practitioners with the necessary knowledge and strategies to enhance cybersecurity practices and ensure the secure digital transformation of construction processes.

1.Introduction

This guide is developed based on the content outlined in the CIC BIM Standards General, specifically referencing Section 2.4 on Security Information Requirements (SIR). While the CIC BIM Standards General provide foundational guidelines for information management using Building Information Modelling (BIM), this guide serves as a supplementary resource focusing on cybersecurity measures in the context of construction digitalisation.

Building upon the principles and workflow of information management using BIM as detailed in the CIC BIM Standards General, this guide delves deeper into cybersecurity considerations essential for safeguarding digital building data and information. In particular, it addresses key aspects of security strategy, management plans, breach incident response, and collaboration with stakeholders to enhance cybersecurity practices in construction projects.

Furthermore, this guide aims to provide additional insights and practical recommendations to complement the Security Information Requirements (SIR) specified in the CIC BIM Standards General. By incorporating cybersecurity best practices and aligning with industry standards, practitioners in the construction industry can strengthen their security posture, protect sensitive data, and ensure operational continuity in the digitalisation of construction processes.

The triage process outlined in the CIC BIM Standards General serves as a critical step in assessing and addressing cybersecurity requirements within construction digitalisation projects. Based on the results of the triage process, the actions shown at the right should be considered to enhance cybersecurity measures:

1. Initiate the Security-Minded Approach
2. Develop a Security Strategy
3. Develop a Security Management Plan
4. Develop a Security Breach/Incident Management Plan
5. Work with Appointed Parties to Implement Security Measures

By following the triage process and implementing the recommended actions, construction practitioners can proactively address cybersecurity challenges, mitigate risks, and enhance the overall security resilience of construction digitalisation projects. This approach aligns with the principles of the CIC BIM Standards General and reinforces the importance of integrating cybersecurity considerations into every stage of the project lifecycle.

1.1 Definition of Cybersecurity in Construction Digitalisation

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks aim to access, alter, or destroy sensitive information, extort money, or disrupt business operations.

In the context of construction digitalisation, cybersecurity focuses on safeguarding digital building data. It involves securing the BIM process, which is a tool utilised throughout the project lifecycle. The guide makes reference to both ISO 27001 and ISO 19650-5. ISO 27001 provides a framework for managing and protecting sensitive information using a risk management approach. It is highly relevant to the cybersecurity measures discussed in the following sections, particularly in relation to data protection and encryption in digital construction workflows. ISO 19650-5 specifies the principles and requirements for security-minded information management in BIM-enabled organisations. It offers guidance on planning for and mitigating risks associated with the digitalisation of information. By adopting the security-minded approach described in ISO 19650-5, organisations can better protect themselves against cyber threats and ensure the confidentiality, integrity, and availability of their information in the context of the construction industry.

1.2 Importance of Cybersecurity in Construction Digitalisation

This guide focuses on cybersecurity in construction digitalisation. With the construction industry embracing digital technologies like BIM and Common Data Environment (CDE) or Common Data Collaboration Platform for BIM (BIM CDCP), it encounters distinct cyber threats. Safeguarding sensitive construction data, ensuring operational continuity, and fostering stakeholder trust are vital. By adhering to ISO 27001 standards for information security management, this guide offers tailored advice and best practices to help practitioners mitigate the risks and vulnerabilities linked to digitalisation in construction.

The importance of cybersecurity in construction digitalisation cannot be overstated. Incorporating cyber risk management into the BIM process is essential to safeguard sensitive information and maintain the integrity of building projects. The integrated nature of BIM also contributes to cybersecurity threats.

Cybersecurity includes all technology that stores manipulates, or moves data, such as computers, data networks, and all devices connected to or included in networks, such as routers and switches, portable devices (e.g., laptops, tablets, smartphones), IoT devices. All information technology devices and facilities need to be secured against intrusion, unauthorised use, and vandalism. Additionally, the users of information technology should be protected from theft of assets, extortion, identity theft, loss of privacy and confidentiality of personal information, malicious mischief, damage to equipment, business process compromise, and the general activity of cybercriminals.

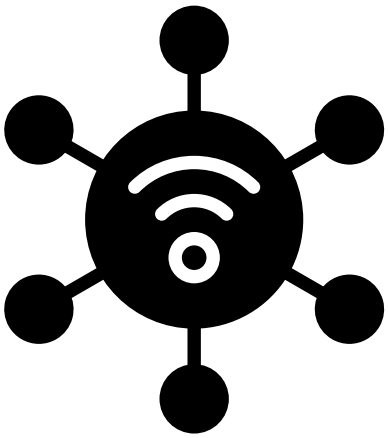
2. Cybersecurity Challenges in Construction Digitalisation

In this section, we will discuss the cybersecurity challenges in Construction Digitalisation. The advent of construction digitalisation has brought about a radical transformation in the industry, leveraging cutting-edge technologies to streamline processes and enhance productivity. However, the rapid integration of digital systems and networks also exposes the construction sector to cybersecurity challenges. Lets explore some of the prominent challenges that practitioners encounter in ensuring cybersecurity within the realm of construction digitalisation.

2.1 Data Protection and Privacy

Construction projects involve the handling of substantial volumes of sensitive data. Safeguarding this data from unauthorised access, breaches, and theft is of paramount importance. Construction practitioners face the challenge of establishing data protection measures, implementing encryption protocols, and ensuring secure storage systems. It is imperative to maintain the integrity and privacy of critical data throughout the construction digitalisation process. Regular audits, encryption of sensitive data, and user authentication protocols within BIM and CDE environments are essential for maintaining the integrity and privacy of critical project information. Training programs on secure data handling practices within BIM and CDE platforms can enhance cybersecurity awareness among project teams and mitigate the risks associated with unauthorised data access or manipulation.

2.2 Vulnerabilities in Internet of Things (IoT) and Connected Devices



The integration of the Internet of Things (IoT) has revolutionised the construction industry, enabling real-time monitoring, predictive analytics, and remote operations. However, this increased connectivity also introduces new avenues for cyber threats. Weaknesses in IoT infrastructure, such as inadequate security protocols, outdated firmware, and unsecured communication channels, pose significant risks. Construction practitioners must address these vulnerabilities by implementing rigorous security measures to safeguard construction digitalisation systems against potential breaches.

2.3 Supply Chain Risks

In the context of construction digitalisation, the intricate supply chains play a crucial role in project execution, involving various vendors, subcontractors, and partners. Each entity within the supply chain presents a potential cybersecurity risk that can impact the digitalisation ecosystem of construction projects. Cybercriminals may exploit vulnerabilities in these interconnected networks to gain unauthorised access or introduce malicious code, posing significant threats to the integrity of digital construction processes. To address these risks effectively, construction practitioners need to implement robust security measures tailored to the digital environment. This includes conducting thorough vendor risk assessments, establishing secure communication channels, and conducting regular audits to ensure the resilience of the construction digitalisation ecosystem against cyber threats.

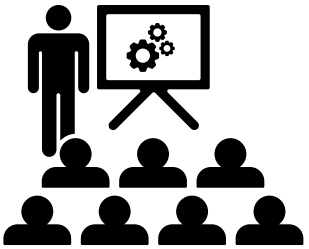
2.4 Insider Threats

In the realm of construction digitalisation, the focus on external cyber threats is prevalent; however, the significance of insider threats, whether intentional or unintentional, should not be underestimated. Employees, contractors, or individuals with privileged access to critical systems in digital construction processes can potentially compromise cybersecurity through intentional actions or inadvertent errors. One notable risk involves information leakage or data breaches from insiders during critical phases like the tender process, potentially leading to unfair competition and compromising the integrity of projects. Such breaches can result in financial losses and reputational damage, highlighting the importance of implementing stringent access controls, encryption protocols, and comprehensive employee training to mitigate insider threats effectively. By addressing these specific cyber risks with tailored countermeasures, construction practitioners can enhance cybersecurity resilience and safeguard sensitive project data throughout the digitalisation process.

2.5 Lack of Cybersecurity Awareness and Training

In many cases, construction practitioners may lack sufficient knowledge and awareness of cybersecurity best practices, unaware of the risks such as the use of common accounts and sharing of passwords. This knowledge gap significantly increases the risk of falling victim to social engineering attacks, phishing attempts, or other cyber threats. Construction practitioners should invest in comprehensive cybersecurity training programs, raise awareness about the latest threats and mitigation strategies, and cultivate a cybersecurity-conscious culture within their organisations.

A common misconception is that relying solely on networks can address cybersecurity concerns, especially in implementing the 4S principles (Safety, Security, Sustainability, and Smartness). While mobile networks offer connectivity benefits, they may not provide sufficient security measures. Organisations must understand that effective cybersecurity requires a multi-layered approach beyond network solutions, encompassing encryption, access controls, and employee training to combat evolving cyber threats and safeguard critical digital assets in construction projects.

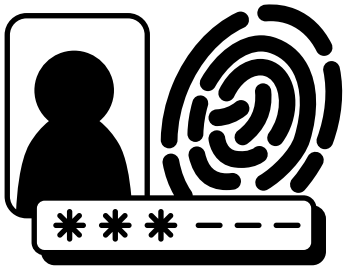


3.Cybersecurity Measures for Construction Digitalisation

In the realm of construction digitalisation, ensuring cybersecurity is important to protect sensitive data, maintain operational continuity, and build trust among stakeholders. This section provides an discussion of key cybersecurity measures that should be implemented to safeguard construction digitalisation processes and systems.

3.1 Access Control and Authentication/Authorisation Measures

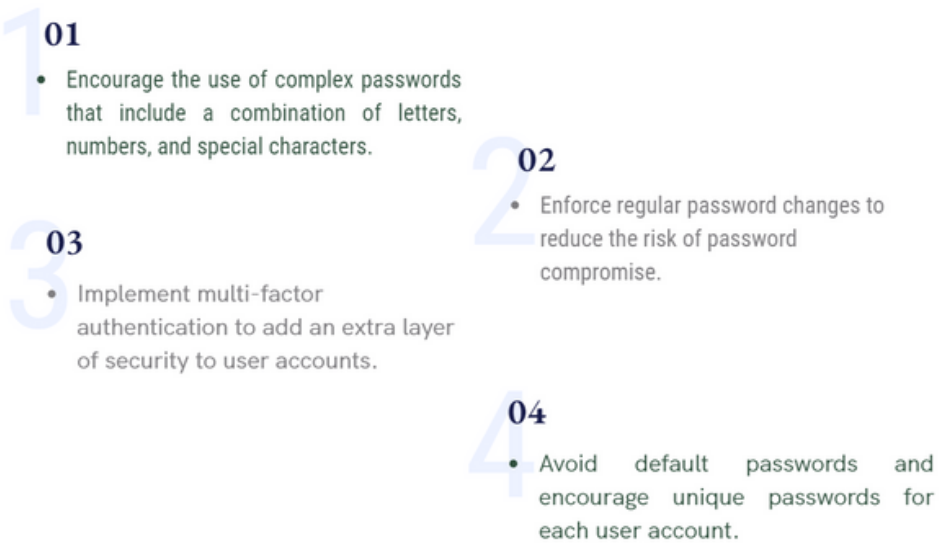
In construction digitalisation, ensuring a secure network infrastructure and implementing robust authentication and authorisation mechanisms are paramount for cybersecurity. Organisations should adopt a "Risk-based" assessment approach and define their risk appetite to determine the appropriate level of cybersecurity measures. Centralised Account Management and enforcement of "identity"-based access, along with Role-based Access Control, are essential components to strengthen security measures. Besides two-factor authentication, it is crucial to ensure the use of strong passwords and avoid default passwords. By aligning with ISO 27001 standards for information security management, a strong network infrastructure is established, incorporating measures such as firewalls, intrusion detection and prevention systems, and secure remote access mechanisms to combat unauthorised access and potential breaches. Implementing access control mechanisms, including role-based access and two-factor authentication, ensures that only authorised personnel can access critical systems and data, playing a pivotal role in safeguarding construction digitalisation processes and systems, thereby protecting sensitive data and maintaining operational continuity.



3.2 Data Protection and Encryption in Digital Construction Workflows

Protecting sensitive data is of paramount importance in construction digitalisation. Construction practitioners should implement data protection measures to safeguard data at rest, in transit, and in use. Encryption plays a critical role in ensuring the security of sensitive data by making it unintelligible to unauthorised individuals, whether it is stored on servers, in databases, or transmitted over networks.

In addition to encryption, a strong password settings strategy is essential for enhancing cybersecurity in construction digitalisation. Consider the following recommendations for password management:



Furthermore, data loss prevention (DLP) solutions can be implemented to monitor and prevent the unauthorised transfer of sensitive information. ISO 27001 provides a framework for implementing an information security management system (ISMS) that can help organisations manage and protect sensitive information using a risk management approach.

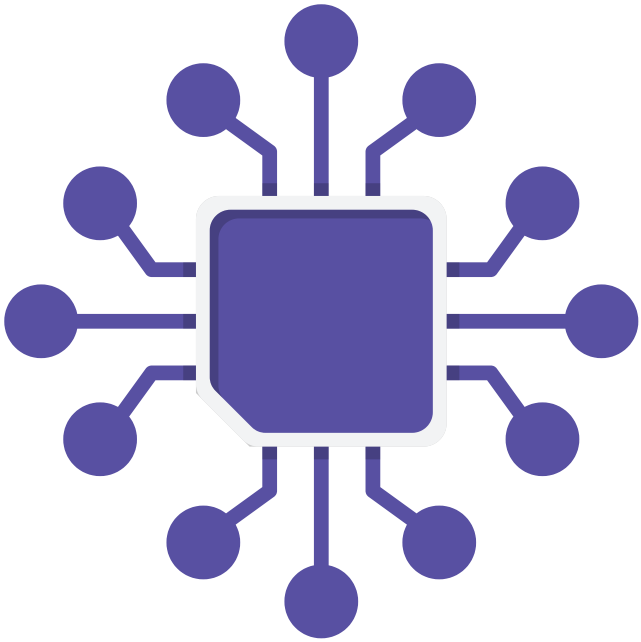
By integrating encryption practices with a comprehensive password settings strategy, construction practitioners can strengthen the overall security posture of their digital systems and mitigate the risks associated with unauthorised access and data breaches.

This revised version combines the discussion on encryption, data protection, and the password settings strategy in a coherent and structured manner within the context of cybersecurity in construction digitalisation.

3.3 Regular Software Updates and Patch Management

Software vulnerabilities can be exploited by cybercriminals to gain unauthorised access to construction digitalisation systems. Construction practitioners must establish a comprehensive software update and patch management process to ensure that all software and firmware are up to date with the latest security patches. This includes operating systems, applications, and network devices. Regular vulnerability assessments and penetration testing should be conducted to identify and address any potential vulnerabilities before they can be exploited.

Implementing robust cybersecurity measures is critical to ensuring the success of construction digitalisation projects. By implementing strong network infrastructure, access controls, authentication and authorisation mechanisms, and conducting regular risk assessments, construction practitioners can protect sensitive data, maintain operational continuity, and build trust among stakeholders.

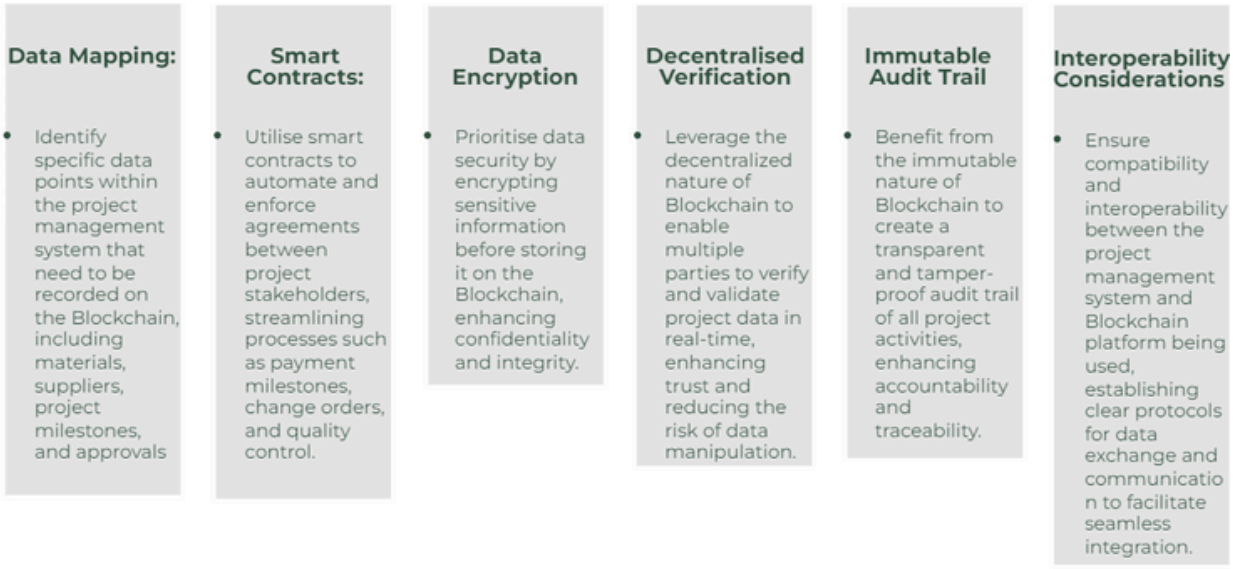


3.4 Integrating with Blockchain

Integrating blockchain technology can revolutionise project management in the construction industry by enhancing security, transparency, and efficiency. By leveraging the immutable and decentralized features of Blockchain, companies can streamline processes, reduce disputes, and ensure the integrity of project data.

One of the examples of integrating blockchain technology with BIM is the establishment of a secure and transparent supply chain record. Through Blockchain's distributed ledger technology, companies can track the movement of materials and products in real-time, ensuring the use of high-quality materials and verifying the authenticity of suppliers. This integration enhances data integrity within BIM/CDE and fosters trust among project stakeholders, leading to improved project outcomes and reduced risks.

The integration process involves several key steps to ensure the seamless interaction between these technologies:



By following these steps and harnessing the synergies between Blockchain and project management systems like BIM, construction companies can unlock significant advancements in data security, collaboration, and overall project efficiency.

3.5 Securing Public Cloud Services for CDE or CDCP

The utilisation of CDE or CDCP and the digitisation of construction processes often entail the adoption of public cloud services. However, the security of cloud environments can raise significant concerns. Therefore, it is essential to address key cybersecurity measures when selecting public cloud services.
When considering public cloud services for CDE or CDCP, construction professionals should prioritise the following cybersecurity measures:

Data Encryption

Ensure that data stored in the cloud is encrypted both in transit and at rest to protect it from unauthorised access.

Compliance with Standards

Verify that the public cloud service provider complies with industry standards and regulations related to data security and privacy, such as ISO 27001.

Access Control

Implement robust access controls to restrict permissions and ensure that only authorized personnel can view or modify sensitive project data.

Incident Response Plan

Develop a comprehensive incident response plan to effectively manage and mitigate security breaches or data leaks in the cloud environment.

Regular Security Audits

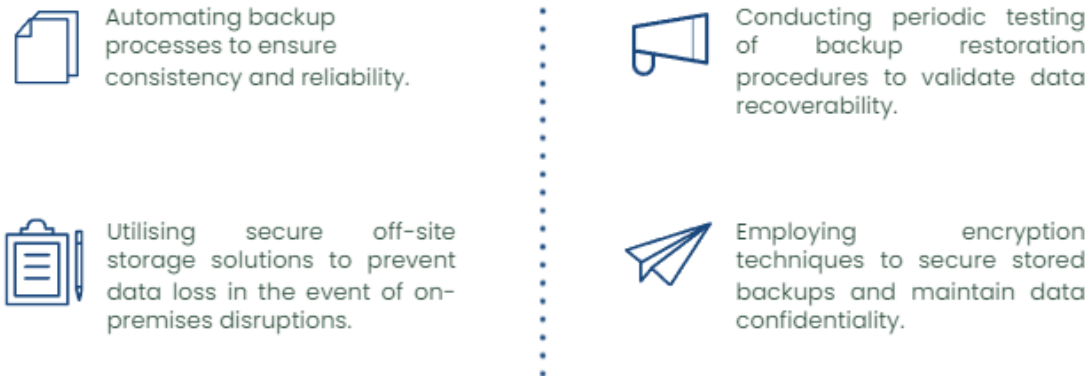
Conduct frequent security audits of the cloud infrastructure to identify and address vulnerabilities promptly.

3.6 Backup Mechanism in Construction Digitalisation

In the realm of construction digitalisation, where the CDE or BIM CDCP serves as a central hub for project information, the importance of a reliable backup mechanism cannot be overstated. Safeguarding critical project data stored within the CDE or BIM CDCP is essential for maintaining operational continuity and data integrity throughout the project lifecycle. It is important to note that the CDE may continue into the AM / FM stage, thus ensuring the cybersecurity of the CDE is crucial for the ongoing security and integrity of data during both project execution and subsequent operational phases.

A robust backup strategy tailored to the unique requirements of the CDE or BIM CDCP environment is crucial. Regular backups of BIM models, project documentation, and collaboration data within the CDE or BIM CDCP should be performed to protect against data loss due to various threats, including cyber incidents, system failures, or accidental deletions.

Key considerations for implementing an effective backup mechanism within the CDE or BIM CDCP include:



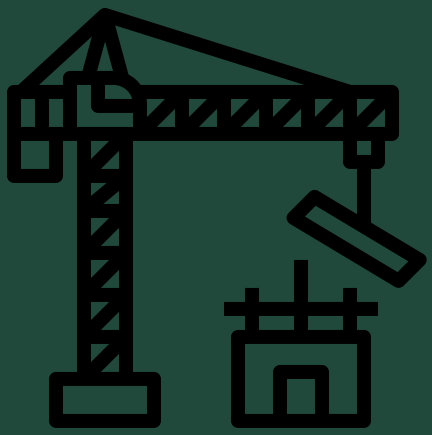
By integrating a dedicated section on backup mechanisms within the context of the CDE or CDCP, construction practitioners can strengthen their cybersecurity posture and proactively address data protection challenges specific to digital construction workflows. This emphasis underscores the critical role of data backup in ensuring the resilience and security of project information within the collaborative environment of the CDE or CDCP.

By incorporating these cybersecurity measures into the selection and utilization of public cloud services for BIM CDE, construction professionals can enhance the security posture of their digital projects and safeguard critical project information effectively.

4 .Emerging Trends and Future Considerations

This section aims to provide construction practitioners involved in construction digitalisation with insights into emerging trends and future considerations in cybersecurity. By understanding these trends, construction practitioners can proactively adapt their strategies to meet evolving cybersecurity challenges.

4.1 EXPLORE HOW CYBERSECURITY CAN ENHANCE CONSTRUCTION DIGITALISATION



Traditionally, cybersecurity has been viewed as a hindrance or constraint to digitalisation efforts. However, a paradigm shift is occurring, recognising cybersecurity as an enabler and enhancer of construction digitalisation. By implementing robust cybersecurity measures, construction practitioners can build trust among stakeholders, protect sensitive data, and ensure operational continuity. This shift involves integrating security practices and considerations into the design and implementation of digitalisation initiatives from the outset, rather than treating security as an afterthought.

4.2 INTEGRATION OF INTERNET OF THINGS (IOT) AND ARTIFICIAL INTELLIGENCE (AI)

The integration of IoT and AI technologies is rapidly transforming the construction industry, providing real-time monitoring, predictive analytics, and automation. However, these advancements also introduce new cybersecurity challenges. Construction practitioners must explore innovative approaches to secure IoT devices and networks, such as implementing blockchain technology for enhanced data integrity and adopting AI-driven threat detection and response systems. The convergence of IoT and AI in construction cybersecurity will be crucial to staying ahead of sophisticated cyber threats.

4.3 PRIVACY AND ETHICAL CONCERNS IN CONSTRUCTION DIGITALISATION

As construction digitalisation expands, privacy and ethical considerations come to the forefront. The collection and utilisation of vast amounts of personal and sensitive data raise concerns about data privacy, consent, and transparency. It is essential that construction practitioners in this domain navigate the intricacies of privacy regulations and implement privacy-by-design principles to ensure compliance and protect individuals' personal information. In this regard, it is crucial to observe the Personal Data (Privacy) Ordinance (Cap. 486) when handling personal data, particularly emphasizing the Six Data Protection Principles. The Six Data Protection Principles outline the fundamental guidelines for the fair and lawful use of personal data, ensuring that individuals' privacy rights are respected throughout the data lifecycle.

4.4 THE ROLE OF REGULATIONS AND STANDARDS IN CONSTRUCTION CYBERSECURITY

Regulations and industry standards play a vital role in shaping cybersecurity practices in construction digitalisation. Construction practitioners must stay abreast of evolving regulations and compliance requirements specific to the construction industry for example Guidelines for Security Provisions in Government Accommodations by the Secretary for Security. Adhering to these standards helps establish a baseline for cybersecurity practices and fosters a culture of continuous improvement within the industry.

Emerging trends and future considerations in cybersecurity for construction digitalisation offer construction practitioners valuable insights into the evolving landscape of cyber threats and mitigation strategies. By embracing cybersecurity as an enabler rather than a constraint, integrating IoT and AI technologies securely, addressing privacy and ethical concerns, and adhering to regulations and standards, construction practitioners can navigate the ever-changing cybersecurity landscape with confidence. As construction digitalisation continues to revolutionise the industry, proactive and adaptive cybersecurity measures will be crucial to safeguarding sensitive data, ensuring operational continuity, and building trust among stakeholders.

As organisations navigate the complexities of cybersecurity in construction digitalisation, it is essential to adopt robust frameworks to guide their security practices. Many organisations have embraced the NIST Cybersecurity Framework, now in version 2, which outlines six major functions: Governance, Identity, Protection, Detection, Response, and Recovery. This framework provides a structured approach to cybersecurity, helping organisations establish comprehensive security measures and effectively mitigate cyber risks. For detailed guidance on implementing cybersecurity best practices, readers are encouraged to refer to the NIST Cybersecurity Framework v2 at NIST Cybersecurity Framework v2.

5.Conclusion

In conclusion, cybersecurity is a critical consideration for construction practitioners involved in construction digitalisation. As the industry continues to adopt new technologies and processes, it is essential to maintain robust security measures to protect sensitive data, maintain operational continuity, and build trust among stakeholders. This guide has provided an overview of the cybersecurity challenges facing the construction industry, as well as practical measures that can be taken to mitigate these risks. By staying informed about emerging trends and future considerations in cybersecurity, construction practitioners can proactively adaptheir strategies to meet evolving threats.

6. Reference

- BS EN ISO 19650-1: Organization and digitization of information about buildings and civil engineering works, including building information modelling -- Information management using building information modelling: Concepts and principles.
- BS EN ISO 19650-2: Organization and digitization of information about buildings and civil engineering works, including building information modelling -- Information management using building information modelling: Delivery phase of the assets.
- BS EN ISO 19650-3:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling. Operational phase of the assets.
- BS EN ISO 19650-4:2022 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling - Information exchange
- BS EN ISO 19650-5:2020: Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM). Information management using building information modelling. Security-minded approach to information management.
- ISO/IEC 27001 – INFORMATION SECURITY MANAGEMENT
- CIC BIM Standards General
- CIC Production of BIM Object Guide – General Requirements
- CIC BIM Standards for Mechanical, Electrical and Plumbing
- Construction Digitalisation Roadmap for Hong Kong (2021)
- Common Data Environment (CDE) Data Standard, 2021, Building and Construction Authority
- DEVB(W) 430/80/01, Information Security of Project Data, Development Bureau
- OGCIO, Practice Guide for Cloud Computing Security Version 2.0 April 2024

7. Committee on Building Information Modelling

The Task Force on BIM Standards

Membership List

Chairperson	Representing Organisation / Remarks
Ar. Aaron CHAN Wing-kai	Existing Com-BIM Member/ The Hong Kong Institute of Architects
Member	**Representing Organisation / Remarks**
Prof. Jack CHENG Chin-pang	Chairperson of Committee on BIM
Ar. David FUNG	Hong Kong Alliance of Built Asset & Environment Information Management Associations Company Limited/ The Hong Kong Institute of Architects
Mr. Kwok Tak-wai	The Hong Kong Federation of Electrical and Mechanical Contractors Limited
Ir Ole WONG Ming-yan	Existing Com-BIM Member/ The Association of Consulting Engineers of Hong Kong
Cr Michael WONG Wai-lun	Existing Com-BIM Member/ Hong Kong Construction Association
Mr. Froky WONG Yuen-hung	The Hong Kong Institute of Building Information Modelling
Sr YIP Yin-yung	Existing Com-BIM Member/ The Real Estate Developers Association of Hong Kong
Mr. LEE Chi Hang, Alfred	Development Bureau
Mr. CHEUNG Ka Lai, Gally	Buildings Department
Ms. Chelsie CHAN Choi-yin	Lands Department

Convenor and Secretary

Mr. Alex Ho — Construction Industry Council

Mr. George Wong

Mr. Lok Fung

8. Acknowledgement

The CIC would like to acknowledge the assistance of the following organisations for providing valuable comments for the CIC Beginner's Guide on Construction Digitalisation - Cybersecurity:

- Architectural Services Department
- Buildings Department
- Civil Engineering and Development Department
- Development Bureau
- Drainage Services Department
- Electrical and Mechanical Services Department
- Highways Department
- Lands Department
- The Airport Authority Hong Kong
- The Association of Consulting Engineers of Hong Kong
- The Hong Kong Federation of Electrical & Mechanical Contractors Limited
- The Hong Kong Institute of Architects
- The Hong Kong Institute of Building Information Modelling
- The Real Estate Developers Association of Hong Kong
- Water Supplies Department

The CIC thanks all stakeholders who have offered opinions.

Feedback Form

CIC Beginner's Guide on Construction Digitalisation - Cybersecurity

To improve future editions of this publication, we would be grateful to have your comments.

(Please put a "✓" in the appropriate box.)

1. **As a whole, I feel that the publication is:**	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Informative	❑	❑	❑	❑	❑
Comprehensive	❑	❑	❑	❑	❑
Useful	❑	❑	❑	❑	❑
Practical	❑	❑	❑	❑	❑
2. **Does the publication enable you to understand more about the subject?**	Yes		No		No Comment
	❑		❑		❑
3. **Have you made reference to the publication in your work?**	Quite Often		Sometimes		Never
	❑		❑		❑
4. **To what extent the publication benefits you?**	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Supply chain Information/data integrity	❑	❑	❑	❑	❑
Work efficiency	❑	❑	❑	❑	❑
Project Collaborations	❑	❑	❑	❑	❑
5. **Overall, how would you rate our publication?**	Excellent	Very Good	Satisfactory	Fair	Poor
	❑	❑	❑	❑	❑
6. **Other comments and suggestions, please specify (use separate sheets if necessary).**					

Personal Particulars (optional):*
Name: Mr. / Mrs. / Ms. / Dr. / Prof. / Ar. / Ir / Sr ^
Company:
Tel:
Address:
E-mail:

* The personal data in this form will be used only for this survey. Your data will be kept confidential and dealt with only by the Construction Industry Council.

^ Circle as appropriate.

Please return the feedback form to:
CIC Secretariat – Construction Digitalisation
E-mail: bim@cic.hk;
Address: 38/F, COS Center, 56 Tsun Yip Street, Kwun Tong, Hong Kong
Fax No.: +852 2100 9090