The Institution of Engineering and Technology

Building Information Modelling (BIM): Addressing the Cyber Security Issues

Building Information Modelling (BIM) is going to transform the way that the architecture, construction, engineering and facilities management (FM) industries work together.

This new collaborative approach is based on shared information models, which will be developed and maintained across the lifecycle of the building or infrastructure. A number of new risks are inherent in the adoption of BIM, in particular the need to address cyber security in the implementation of the collaborative processes and systems.

Built Environment

www.**theiet**.org/built-environment

Contents

1. Overview

On 31 May 2011 the Cabinet Office published the UK Government's Construction Strategy, announcing the Government's intention to require collaborative BIM on its projects by 2016. By collaborative BIM the Government means that all project and asset information, documentation and data will be handled electronically.

With industry, the UK Government has effectively embarked on a programme that will modernise the architecture, construction, engineering and facilities management (FM) industries. This is not without risk as the greater reliance on information technology has associated cyber security risks.

Whilst this document primarily addresses a number of the cyber security issues inherent in Level 2 BIM in the UK, it also seeks to highlight issues that will emerge as the work to define Level 3 BIM progresses. It is intended that this document will be updated in light of developments in the UK BIM Level 3 programme.

2. Introduction

Building Information Modelling (BIM) is the process of designing a building or structure collaboratively using a single coherent system of computer models. It is intended to offer savings in cost and time, greater accuracy in estimation, and reduction or avoidance of error, alterations and rework due to information loss. BIM should also deliver legacy value by providing an 'as built' information model for use by asset and facilities managers through the operational life of the building or infrastructure.

Adopting BIM is not just about the choice of software. To realise the benefits everyone in the architecture, engineering, construction and FM industries must work in fundamentally new ways. Both the use of technology and collaborative work processes is essential. BIM symbolises a movement in the UK construction industry involving a significant cultural shift to a new co-operative and positive work paradigm.

At the heart of BIM is a shared digital representation of the physical and functional characteristics of a building or structure. This use of a shared knowledge resource provides a reliable basis for decisions across the lifecycle of a building or structure, from conception to demolition. The knowledge resource is represented by the information management elements in Figure 1.

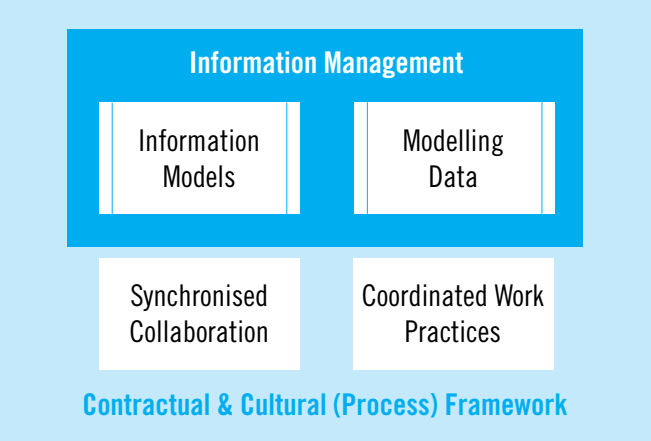


Figure 1: Elements of Building Information Modelling (BIM)

The mechanisms for managing the collaborative working are represented by the process framework elements in Figure 1. The process framework includes the business processes relating to review, acceptance and maintenance of information models, and the operational processes related to managing the IT environment. Cyber security affects both the technology and process elements of BIM.

BIM is not limited to the planning, design and construction phases of a building or structure. It is intended that information models will be used throughout the asset's lifecycle for asset management, performance monitoring and change management. It is expected that the information will be updated with changes over the asset's lifecycle and that performance and utilisation data will be added to the models. To facilitate collaborative working, BIM envisages the use of a Common Data Environment (CDE).

The CDE provides a single repository for information for any given project, which is used to collect, manage and disseminate all relevant approved project documents for multi-disciplinary teams as part of a managed process. The sophistication and scale of the CDE may vary considerably from a project server, extranet, or file-based retrieval system for a smaller project, to a complex cloud-based content delivery network for major projects undertaken by large international teams.

The concept of the CDE is important as it represents a system to manage the process of information generation and exchange between all project stakeholders. It is intended that information should be audited, monitored and tracked as it moves through the CDE. It is important to recognise that the contents of the CDE will develop across the lifecycle of the building or structure. This has information management implications, including the need for appropriate governance and a curator role to maintain data quality and integrity on behalf of the asset owner and users.

3. What is cyber security?

Cyber security is about more than technology; it encompasses people, process and governance issues, and their inter-relationships. These non-technical elements are management issues and are as important in cyber security as the deployment of appropriate technical solutions. As BIM involves a complex interaction between governance, people, process and technology, it is important that all personnel involved in a BIM project understand the cyber security implications.

An internationally agreed definition of cyber security is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets". This definition refers to:

- the "cyber environment" which effectively comprises the interconnected networks of electronic, computer-based and wireless systems; and
- the "organisation and users' assets" which include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted, processed and/or stored data and information in the cyber environment.

The cyber environment therefore encompasses the Internet, telecommunication networks, computer systems, embedded processors and controllers, and a wide range of sensors, storage and control devices. Although the definition above of cyber environment only makes reference to systems, it also includes the information, services, collaborative and business functions that exist only in cyberspace. Experience shows that even standalone systems and isolated networks are at risk, from both attacks by malicious users and from the introduction of malicious software via removable media or information storage devices.

Widespread use of the Internet and email has already revolutionised the way that organisations work. In implementing BIM, the construction industry will make greater use of these technologies to support collaboration and information exchange. It therefore needs to understand how to protect its information and operations in cyberspace. This protection of key information models, including plans, business cases, designs, tender specifications, financial models and contracts, is essential to maintain a sustainable and competitive business.

By applying appropriate cyber security measures, organisations seek to ensure they attain and maintain the security objectives of their own organisation and their stakeholders against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Confidentiality, including control and authorisation of access to information or data;
- Integrity, which includes trustworthy operation of electronic and computer-based systems, their software, any associated business processes, the assurance and authenticity of data or information, and the validity and retention of transactions including their authentication and non-repudiation;
- Availability of data, information, systems and processes required for the safe, secure and reliable design, delivery and operation of the building or facility. This encompasses both reliability and resilience, i.e. the need to handle and recover from a range of failures.

Implementing BIM inevitably creates a complex collaborative environment, with a diverse range of organisations sharing information and models

electronically. From a cyber security perspective, the situation will be complicated by the fact that organisations have differing levels of security awareness and discipline.

Control and protection of information will become more complex as the length of the supply chains grows during development of the design, construction, and then through outsourcing of operational services or support once in use. In addition to the changing user access across the lifecycle, there will also be changes to the sources of data, and during the operations phase the need to accommodate feeds of asset use, maintenance and energy consumption data.

4. What are the cyber security threats?

The cyber security threats affect the CDE and all systems that connect to it. They will potentially emanate from three groups:

- External threat agents;
- Internal threat agents;
- Systems and business failures.

External threat agents are malicious outsiders who are unconnected with the building or structure and the professions involved in its design, delivery or operation. They will range from terrorists and criminals, who are seeking access to the BIM data for reconnaissance purposes, e.g. when planning a terrorist incident or a crime, to competitors, hackers and hacktivists who are trying to steal intellectual property, gain unauthorised access to systems, and leak or publicise sensitive confidential information.

Damage caused by malware may be regarded as an external or internal threat agent depending on how it infects any BIM-related systems.

Internal threat agents are insiders, i.e. individuals connected with the building or structure and the professionals involved in its design, delivery or operation. A malicious insider may abuse their privileged or authorised access to the BIM data, e.g. to steal or leak sensitive commercial data, to corrupt the BIM data or to disrupt operations.

A non-malicious insider may through error, omission, ignorance or negligence cause a cyber security incident, e.g. operator or user errors may lead to corruption or loss of BIM data and impact the progress during design and build phases, or undermine performance monitoring during the operations phase.

Systems and business failures may result from a range of causes, including:

- Nature, e.g. disruption due to solar, weather, animal or insect causes, which results in the failure or significant impairment of the systems used to store, process or manage BIM data;
- Systems failures, e.g. failure of storage devices resulting in corrupt or irrecoverable files, or non-availability of critical systems used to store, process or manage BIM data through poor maintenance or a lack of resilience in supporting IT infrastructure;
- Bankruptcies and business failures affecting the availability or access to BIM data or the systems used to store, process or manage BIM data.

5. So what does cyber security involve?

Cyber security has evolved from the discipline of Information Security, and as mentioned above, the three key elements are management of confidentiality, integrity and availability. Good cyber security involves putting in place appropriate mechanisms, e.g. security awareness, security policies, supporting business processes and technical solutions.The level of cyber security protection required will depend on the threats and risks involved, which in turn will be determined by a number of factors, including:

- Location of the building or facility;
- Physical environment;
- Profile and attractiveness as a target;
- Planned use/function, including particular safety or physical security requirements;
- Nature of occupiers/users;
- Any legal or regulatory requirements;
- The organisations that need access to the BIM data
- Complexity and criticality of building systems;
- Degree/level of systems integration and convergence
- Degree of connectivity of building systems to systems outside of the building

Threat assessments will need to be developed and updated across the building lifecycle, taking into account changes in relevant factors. The threat assessment will guide the need for specific cyber security policies, processes and technical solutions.

5.1 Confidentiality

From a confidentiality perspective poor cyber security may have a number of impacts including:

- Compromising the commercial confidentiality of a competitive tendering exercise. This may disadvantage an organisation or group of organisations bidding for a major project. The risk of such compromises will increase as more organisations contribute to, or have access to, a collaborative model during the bidding stage of a project.
- Exposure of information about building layout and use during the town planning and statutory approvals process. This may arise if access is provided to detailed models or plans carrying information about space allocation and use.
- Compromise of building security once it is occupied, through unauthorised individuals gaining access to the BIM information. For example, the individual may be able to conduct a hostile reconnaissance without needing to visit the site or gain entry to the facility by examining the information models and supporting data on security features and alarm systems.
- Loss or theft of valuable intellectual property (IP). This IP may be part of the detailed design or contained in the electronic documents and information stored within the information models. For example, there may be information in these documents on novel construction techniques, detailed calculations requiring specialist knowledge or the design of proprietary systems.

To protect sensitive or confidential data, you need to be able to identify this data within the BIM models and supporting information. There is also a need to address the effect of data aggregation. One or two isolated information sources in the CDE may not be particularly sensitive, but certain combinations of information sources when taken together may significantly increase sensitivity. For example, in a building that is required to resist forcible entry or attack, those parts of the CDE dealing with the facade and interior may not be too sensitive from a security perspective, but knowledge of any reinforcement in the perimeter walls and the specification of glazing, doors, etc. may compromise the overall security.

If sensitive information can be identified, then consideration can be given to implementing role-based access control. Allowing control and monitoring of access to BIM models and calculations can therefore be used to limit access both during design and construction, and during the overall lifecycle of the facility.

5.2 Integrity

From an integrity perspective, a key issue is maintaining the integrity of the models and any associated objects and data. On a large construction project there may be thousands of individuals who need access to the BIM information.

This can pose a significant threat from a configuration management and change control perspective, requiring complex processes to manage changes and variations. Without these controls it may be impossible to determine the consequential impact on the CDE information content. There is also a need to consider how to recover from failure or error conditions, whether caused by users or the system.

In addition to the configuration control mechanisms, the information manager must also address potential interoperability issues between different models held within the CDE. These may for example arise from differences in software packages used by project participants, from errors in cross referencing between models, from communications errors or from failures to check assumptions.

It is important that routine regular backup mechanisms are in operation and that recovery of models or information from the backups is practiced. It is too late to discover problems with the backup or recovery processes once there has been corruption of the latest set of files.

From an integrity perspective it is also important to consider the potential impact of malicious code. Two instances of malware targeting a BIM software platform have been identified. At present, the malware appears to facilitate theft of IPR or provide Trojan functionality, i.e. allowing remote unauthorised access to a computer or network. If the malware were to include ransom-ware functionality then the ability to maintain the integrity of BIM data would become a business critical issue.

5.3 Availability

From an availability perspective there are a number of critical points that need to be addressed in managing the CDE. During the design and construction stages, where time is of the essence, consideration needs to be given to the reliability and resilience of the storage location for the CDE. Some suppliers refer to the BIM data as being stored in 'the cloud'.

Organisations need to understand what cloud storage means with regards to availability and the security of their data. The IET has prepared a number of free factfiles on cloud computing [www.theiet.org/factfiles/it].

Another availability challenge will be software compatibility issues that may arise in respect of the BIM information over a building's lifecycle. The software industry is constantly creating new software versions of operating systems, data storage and retrieval applications, and the BIM modelling applications used by designers. Consideration must be given to how BIM information will be stored and modified across the lifecycle. Many of the legacy software problems that affect the financial sector will in time affect BIM, for example when access is required to data or a model that is held in an obsolete file format.

Compatibility of the software packages used by the project team may also create availability issues. For example, whilst it is possible to open a file saved in Microsoft Word format in a variety of packages, formatting of text and the fonts used may vary considerably. In a text document, changes in the fonts used may affect the pagination, whilst incompatibilities may hide embedded comments or tracked changes. The consequences could be more serious if changes affect diagrams or calculations, thus contributing to a loss of integrity or fidelity.

The use of an escrow arrangement whereby a copy of the BIM data is held and maintained by a trusted third party may be appropriate in some circumstances. For example, if there are concerns about the long term stability or viability of the organisation responsible for managing the BIM data. This is likely to become a significant issue where model data is to be retained throughout a facility's lifecycle, of say 50 or more years.

6. Legal Issues

In addition to the traditional information security triad (confidentiality – integrity – availability), there are some security-related legal issues that should be considered:

- Protection of intellectual property and intellectual property rights;
- Information Management responsibilities, including handling of cyber security incidents;
- Resolving BIM technology disputes.

6.1 Protecting Intellectual Property

Whilst the BIM Protocol [A] makes some provision in Clause 6, in particular Clause 6.2 regarding copyright and proprietary information, once information has been incorporated into an electronic model, it may become increasingly difficult to protect this data across the project lifecycle. Theft of intellectual property is a widespread problem in many industries where the product is digital, e.g. software, publications and multi-media. Consideration needs to be given to:

(a) whether sensitive data should be identified in the CDE;
(b) if it is to be identified, the mechanisms used to identify it;
(c) whether access controls need to be applied to sensitive data;
(d) who is responsible for managing the access controls?

6.2 Information Management responsibilities

The BIM Protocol [A] requires the Employer to appoint an Information Manager. An indicative scope of services [B] has been developed for this role and further information is provided in PAS 1192-2 [E]. The Information Manager has no design related duties, but is responsible for managing the CDE, managing project information, and supporting collaborative working, information exchange and the project team.

A proposed duty the Information Manager has in respect of the CDE is to "maintain the Information Model to meet integrity and security standards in accordance with the Employer's Information Requirements". The provision of services to host the CDE is treated as an additional (optional) service for the Information Manager role.

In the guidance on the Employer's Information Requirements [C], section 1.2 (Management) includes provision for incorporating standards and security requirements. The purpose of the sub-section covering security is to "communicate client specific security measures required in order to secure the data". This sub-section suggests that security is defined in terms of the UK Government's business impact levels, e.g. IL1 to IL4.

From a professional indemnity perspective, the Best Practice guide [D] suggests that where the BIM Protocol [A] is used, it is unlikely that any cyber security liabilities will be attached to plain users of BIM systems. However, it notes that some professional indemnity insurance policies seek to "exclude all liability associated with loss, damage or alternative of electronic documents however this occurs". Given the increasing threat from cyber security incidents, insurers may seek to apply such exclusions to BIM projects and to seek assurances that all participants are taking appropriate steps to protect their work and the CDE.

6.3 Resolving BIM technology disputes

Clause 5 of the BIM Protocol [A] addresses risks associated with the provision and exchange of electronic data, specifically:

- Clause 5.1 states that a Project Team Member gives no warranty as to the integrity of electronic data;
- Clause 5.2 excludes liability for any corruption or unintended amendment, etc. of the electronic data

which occurs after transmission of a Model by the Project Team Member, unless caused by a failure to comply with the Protocol.

Many technology disputes arise from systems failure and it is inevitable that in some BIM projects data loss or corruption will occur, resulting in a loss of integrity in the Model. From a cyber security perspective, Clause 5 does not appear to encourage Project Team Members to follow best security practice or take appropriate steps to assure the integrity and/or protection of BIM data. The net effect of Clause 5 is that the residual liability for the integrity of the electronic data lies with the Employer. This is not always the case with other protocols and the situation will change with the use of a single model in BIM Level 3.

7. Implementing cyber security on a BIM project

From a project perspective, implementing cyber security good practice will require attention to four key areas:

- Cyber security policies and procedures;
- Cyber security awareness and education;
- Protecting the project's technical infrastructure;
- Protecting the asset's systems and infrastructure.

These three areas represent a mixture of management, personnel and technical issues that need to be addressed across the project team and throughout the supply chain.

7.1 Cyber security policies and procedures

The design, construction and operation of a building or structure will involve a diverse range of organisations, ranging from large international corporations, to small companies, partnerships or individuals. The UK Government has produced a briefing document for executives [F], which explains the risks and need for good cyber security.

The security awareness and maturity of project participants will vary considerably. Some may hold national or internationally recognised accreditations, whilst others may have little or no knowledge of cyber security principles and practices. For those organisations which are security aware, their cyber security policies are likely to mainly focus on protecting their own information and as such may not be suitable for use as part of a collaborative project.

The security maturity of the employer organisations will also vary considerably, from knowledgeable organisations with specific security needs and their own professional security staff or advisers, to relative naïve organisations who do not understand the potential cyber security risks or threats.

Depending on the nature of the project, the employer and the potential cyber security risks, the Information Manager should consider whether an overall cyber security policy is required for the project. This policy should address the inevitable gaps that will exist between organisations and clearly establish cyber security responsibilities for the CDE, access to the CDE and the protection of BIM data.

As part of this project policy, responsibility for managing cyber security incidents should be established. The policy should be supported by an appropriate set of project cyber security procedures, e.g. a procedure relating to access control that identifies who determines access levels, how these are managed and implemented, and the process for joiners and leavers.

7.2 Cyber security awareness and education

Personnel are often the weak link in a cyber security situation, whether through careless behaviour, e.g. losing removable media (USB memory sticks, etc.), or ignorance, e.g. clicking on phishing emails or opening malware attachments. The risks of malware infections and loss of proprietary and confidential information can be reduced by raising user awareness and addressing

acceptable and secure use of project related systems. In collaborative situations, it is easy for all parties to assume that someone else is responsible for cyber security.

Awareness and education activities are important at an overall project level. Project team members need to work together to maintain cyber security of the BIM data. These activities must continue across the project lifecycle, ensuring that personnel and suppliers joining the project are aware of the policies and their responsibilities. There is also a need to address the release of organisations and individuals from their project roles, to reduce the risk of improper use or disclosure of sensitive data.

7.3 Protecting the project's technical infrastructure

In 2012, the UK Government produced a set of cyber security advice sheets [G], which explain ten steps that can be taken to improve an organisation's cyber security. These steps are applicable both to organisations involved in the project and to those involved in the CDE. They include secure configuration of IT and communications systems, managing user privileges, managing removable media, malware protection, network security, and monitoring systems for unusual activity. A combination of good cyber hygiene by users and use of appropriate technical security measures can significantly reduce the cyber security threats to a project.

7.4 Protecting the asset's systems and infrastructure

Some assets developed using BIM are already using the CDE to store data from sensor networks, which were deployed during the construction phase, and are connecting to building management systems to collect performance data. This integration of BIM information models and operational building systems presents a significant risk.

For example, by accessing the BIM model it may be possible to control or override setting on heating, ventilation and air conditioning (HVAC) plant, switch off building power distribution systems, or control combined heat and power (CHP) systems. These interfaces need to be designed and implemented so as to maintain the security of both the BIM information models and the operational systems.

8. Cyber security of operational BIM data

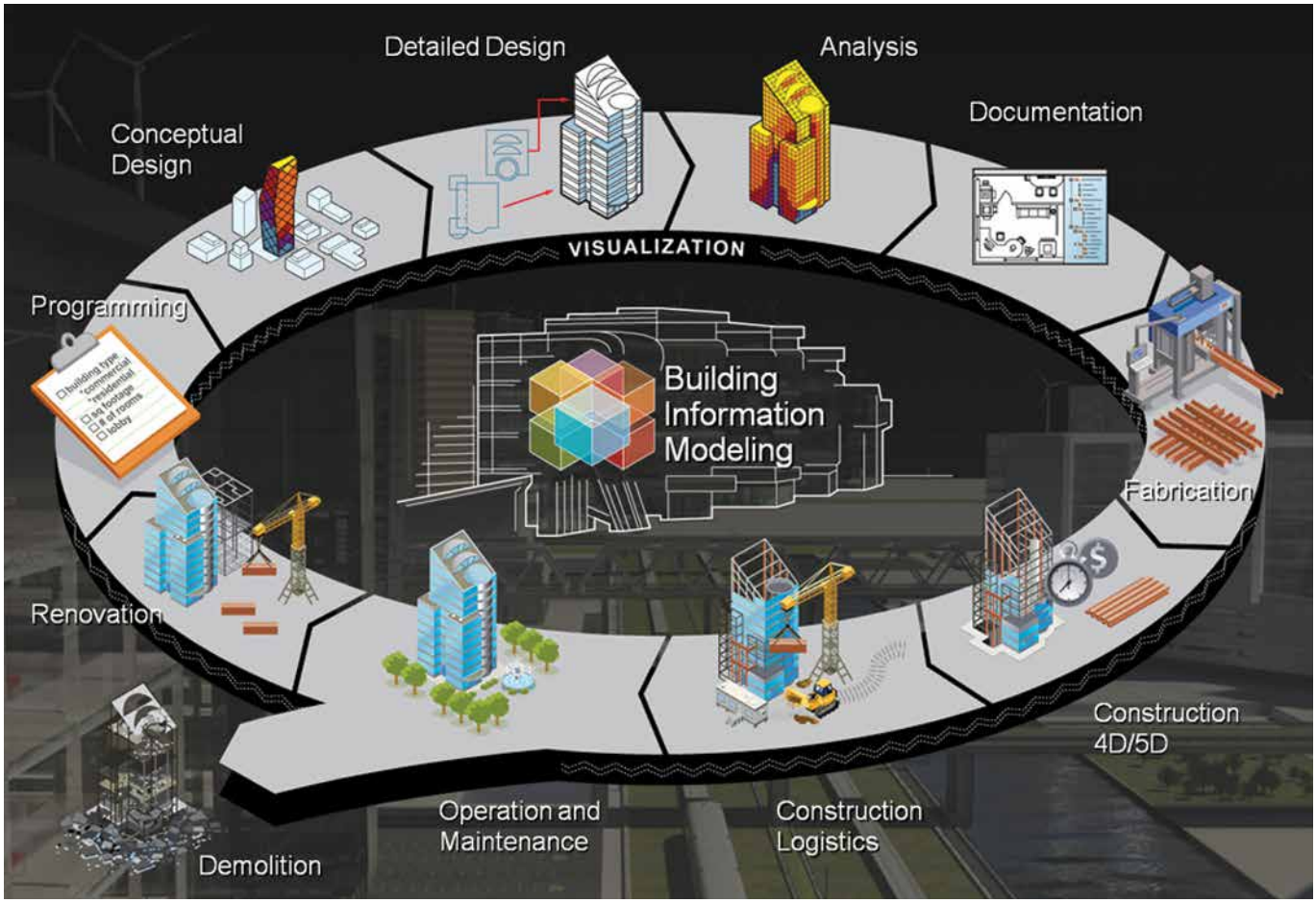
As a construction project moves from the design phase into delivery, there will be a need to update the information models to reflect the 'as built' building or facility. Changes may be required to reflect issues or problems encountered during construction or to reflect actual material or building products that were used.

This updating of the information models is critical if the BIM data is to be used once the asset is operational. For legal liability reasons, it is important that this updating process is appropriately managed, with controls over who can update the models, and measures in place to protect their integrity and availability.

As the building or facility is being commissioned and brought into use, there may be a need to extend the CDE to include facilities management information or to interface it to other systems, e.g. to computer aided facilities management (CAFM) systems or space planning tools. As part of the handover of the building or facility, it may be necessary to transfer responsibility for the information models from a construction information manager to an operational information manager, the latter taking responsibility for the ongoing custody and maintenance of the 'as built' data information.

The operational information manager will need to address the ongoing cyber security of the BIM data, including maintaining:

- confidentiality and access controls as personnel and contractors change over the operational life of the asset;
- integrity by ensuring the information models are continuously updated to reflect changes to the asset, whether through maintenance or further projects;
- availability as the information and storage technologies change and evolve over the asset's lifetime.



The availability issues may be a significant task given the rate of change of operating systems and application software.

9. Looking ahead

The UK Government has commenced the planning of the BIM Level 3 programme. This will involve greater electronic integration of project teams and will increase the potential for serious impact on projects from cyber security incidents. This briefing document aims to raise awareness of some of the cyber security issues facing BIM projects. The IET intends to publish more detailed guidance on the implementation of cyber security in BIM projects during the implementation of the UK BIM Level 3 programme.

10. References

A. Construction Industry Council, Building Information Model (BIM) Protocol, CIC/BIM Pro, First edition, February 2013, London

B. Construction Industry Council, Outline Scope of Services for the Role of Information Management, CIC/INF MAN/S, February 2013, London

C. BIM Task Group, Employer's Information Requirements – Core Contents and Guidance Notes, Version 07, 28 February 2013, London

D. Construction Industry Council, Best Practice Guide for Professional Indemnity Insurance when using Building Information Models, CIC/BIM INS, February 2013, London

E. British Standards Institution Ltd, PAS 1192-2:2013, Specification for information management for the capital/delivery phase of construction projects using building information modelling, 978 0 580 82666 5, 28 March 2013, London

F. HM Government, 10 Steps to Cyber Security: Executive Companion, BIS/12/1120, September 2012, London

G. HM Government, 10 Steps to Cyber Security: Advice Sheets, BIS/12/1121, September 2012, London

The Institution of Engineering and Technology

Author: Hugh Boyes CEng FIET CISSP

Published by: Institution of Engineering and Technology, London, United Kingdom

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no 211014) and Scotland (no SC038698).

© The Institution of Engineering and Technology
First published 2014

This publication is copyright under the Berne Convention and the Universal Copyright Convention. All rights reserved. Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may be reproduced, stored or transmitted, in any form or by any means, only with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at this address:

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way, Stevenage
Herts, SG1 2AY, United Kingdom
www.theiet.org

While the publisher, author and contributors believe that the information and guidance given in this work is correct, all parties must rely upon their own skill and judgement when making use of it. Neither the publisher, nor the author, nor any contributors assume any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause. Any and all such liability is disclaimed. The moral rights of the author to be identified as author of this work have been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

A list of organisations represented on this committee can be obtained on request to IET standards. This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with the contents of this document cannot confer immunity from legal obligations.

It is the constant aim of the IET to improve the quality of our products and services. We should be grateful if anyone finding an inaccuracy or ambiguity while using this document would inform the IET standards development team, (IETStandardsStaff@theiet.org), The IET, Six Hills Way, Stevenage SG1 2AY, UK.

www.**theiet**.org/built-environment

The Institution of Engineering and Technology (IET) is working to engineer a better world. We inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society. The Institution of Engineering and Technology is registered as a Charity in England and Wales (No. 211014) and Scotland (No. SC038698).