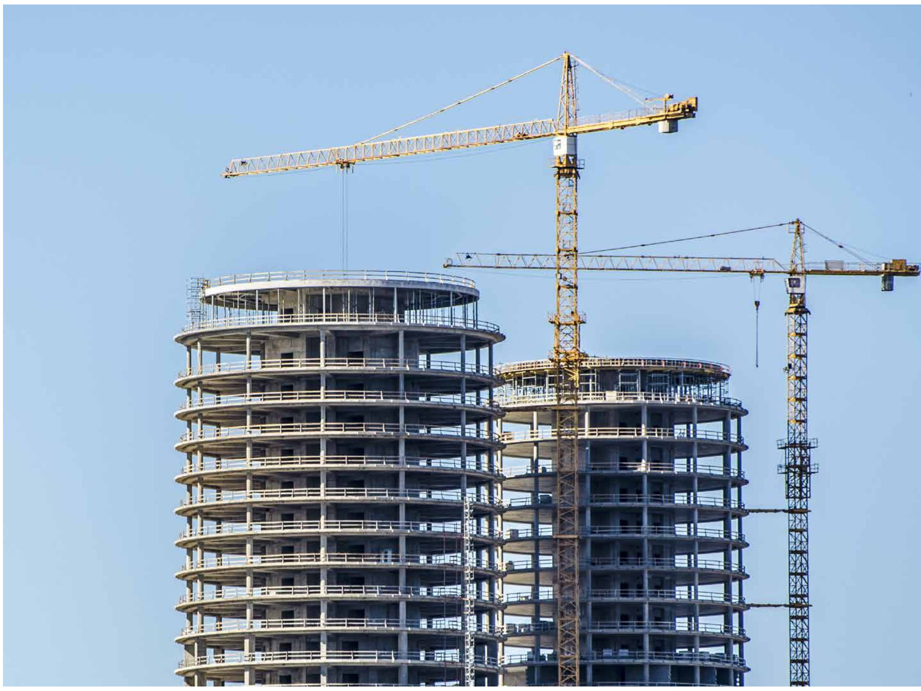
The Institution of Engineering and Technology

National Cyber Security Centre
a part of GCHQ

Code of Practice

Cyber Security in the Built Environment

2nd Edition



The Institution of
Engineering and Technology

Code of Practice

Cyber Security in the Built Environment

2nd Edition

Publication information

Published by The 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).

First published 2014 (ISBN 978-1-84919-891-2)
Second edition 2021 (ISBN 978-1-83953-346-4)

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

Copies of this publication may be obtained from:
The Institution of Engineering and Technology
PO Box 96, Stevenage, SG1 2SD, UK
Tel: +44 (0)1438 767328
Email: sales@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 organizations 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 Codes and Guidance Team, sales@theiet.org, The IET, Six Hills Way, Stevenage SG1 2AY, UK.

ISBN 978-1-83953-346-4 (paperback)
ISBN 978-1-83953-347-1 (electronic)

Typeset by S4Carlisle
Printed in the UK by Elanders Ltd, Merlin Way, New York Park, Newcastle Upon Tyne, TW NE 27 0QG

Contents

Contents

Contents

Acknowledgements

The IET would like to acknowledge the following individuals and organizations for their input into this Code of Practice:

Author

Hugh Boyes CEng FIET (Bodvoc Ltd)

The author wishes to acknowledge his appreciation for the support received from Rhys C (CPNI) who was a member of the Technical Committee for both the initial version and the updated version of this Code of Practice. Sadly, Rhys C passed away shortly before the final draft of this version was complete.

Technical Committee

Mike St. John-Green	Mike StJohn-Green Consulting Limited/Technical Committee chair
Sandra Connery	Atkins
David Fisk	Imperial College London
Derwen Hinds	Imperial College London
Roy Isbel	Information Assurance Strategies Ltd & University of Warwick
Martin Lee	Symantec
Sally Leivesley	Newrisk Ltd
Mani Manivannan	Arup
Stuart Mccormick	UK Defence and Security Exports
Richard Piggin	Rapiscan Systems
Matt Simpson	BAE Systems
Martyn Thomas	Martyn Thomas Associates Ltd

Members of NCSC technical community

National Cyber Security Centre (NCSC)

The NCSC was launched in 2016 to provide a single point of contact on cyber security matters for small and medium-sized enterprises (SMEs), larger organizations, government agencies and departments and the general public. It also works collaboratively with law enforcement agencies, defence agencies, the UK's intelligence and security agencies and international partners. The NCSC has supported the development of this Code of Practice.

Further details on the operations of the NCSC can be found at https://www.ncsc.gov.uk. The NCSC has produced guidance on cyber security which is available at: https://www.ncsc.gov.uk/section/advice-guidance/all-topics.

It is the intention of the IET and NCSC to review this Code of Practice regularly with a view to keeping it up to date, relevant and valuable.

Foreword

Cyber security of built assets and their systems is still an emerging field, but it now has much greater significance. The strategy for managing a built asset's security is relevant at every phase in its lifecycle, regardless of whether it is a new build, you are considering changes to, acquiring or operating an existing built asset. This document explains why it is essential that cyber security is considered throughout the lifecycle and the potential financial, reputational and safety consequences that may arise if cyber security threats are ignored. If the security strategy for a built asset does not address cyber security, or you do not have a security strategy for the built asset, you should address this issue now by asking yourself the following questions:

(a) Do you own, operate or occupy a building/built asset that has an electronic or computer-based operational system, for example, an automatic access control system (AACS), building management system (BMS), building automation and control system (BACS), closed circuit television (CCTV) system, heating ventilation and air conditioning (HVAC) system, supervisory control and data acquisition (SCADA) system, lighting control system, etc?
(b) If the operational systems were to fail, malfunction or were misused, could this result in economic, operational, physical or reputational loss or damage?
(c) Do you own an information asset that includes information about the design strategy, construction of your building/built asset and the operation of its systems?
(d) If this information asset was compromised, could this result in economic, operational, physical or reputational loss or damage?
(e) Are there supply chain risks that would affect your asset and its operations?
(f) Are there sensitivities with people that depend on these assets?
(g) Are there dependencies on other systems within the building/built asset, or on external systems (for example, cloud-hosted applications), that could affect your asset?
(h) Do you know of any events that could cause a failure in the internal critical systems or in systems connecting to your asset?
(i) Do you share information systems with business partners and/or suppliers?

If the answer to any of the above questions is yes, you should carry on reading this Code of Practice and decide what action needs to be taken.

Attacks on the operational systems used to manage buildings and their environment are no longer hypothetical or simply the fictional narrative portrayed in films. While attacks on these systems generally attract less publicity than those affecting online businesses, governments and financial institutions, their impact on those affected can be significant. For example, in November 2016 the residents of two apartment buildings in Lappeenranta, Finland, were left in the cold when the environmental control systems in their buildings stopped working as a consequence of a distributed denial of service (DDoS) attack. Additionally, in January 2017, guests were locked out of their rooms at the Romantik Seehotel Jaegerwirt hotel in Austria following a ransomware attack on the electronic key system.

Cyber security is not just about preventing hackers gaining access to systems and information. It also addresses maintaining control over and the integrity and availability of information and systems, ensuring business continuity and the continuing utility of information assets. To achieve this, consideration needs to be given to protecting systems from physical attack or *force majeure* events and designing resilient systems and supporting processes. From a resilience perspective, the systems should, as far as is reasonably practicable, maintain continuity of operational use and, in the event of failure, permit the timely and orderly recovery of operational use. Personnel security aspects are also important, as the insider threat from staff or contractors who decide to behave in a malicious way cannot be ignored.

Failure to be aware of and address cyber security risks could lead to serious injury or fatality, disruption or damage to systems, loss of use of the built asset, impact on business operations, financial penalties or litigation. Increased training and health and safety awareness have led to fewer serious accidents causing death, serious injury and damage to property. Built asset owners, operators and occupiers need to understand cyber security and promote awareness of the subject to a built asset's stakeholders. This includes appropriate briefing of the design, construction and facilities management teams.

The increased complexity of our built assets and their dependence on the extensive use of information and communications technologies at all phases of a built asset's lifecycle creates new vulnerabilities. The control systems and industrial Internet of Things (IIoT) solutions that are being deployed in built assets present an attractive target to a number of threat actors and their protection should be taken as seriously as the conventional IT systems we use in our daily business and leisure activities. Information can be exfiltrated and built asset or building control systems exploited by sophisticated actors. Awareness of these actions against the built environment is an essential part of the toolkit to manage cyber security.

Advanced technology using artificial intelligence (AI) is being deployed to monitor and detect changes in information technology (IT) and operational technology (OT) networks that are indicators of, or consistent with, cyber attacks. While this automation of threat detection will contribute to all security operations, the recent SolarWinds breach[1,2] demonstrates how trusted tools can be exploited to attack the systems they are deployed to protect. This breach illustrates the importance of understanding how a security incident in the built asset's supply chain could affect the asset and/or the organization's operations.

This Code of Practice provides clear practical guidance so that multidisciplinary teams can understand how the management of various aspects of cyber security apply to their job roles and their personal responsibilities in maintaining the security of a built asset. It explains how to consider the cyber security threats to the built asset, how to develop an appropriate security strategy and highlights some of the practical issues relating to its implementation.

This Code of Practice uses principles rather than national legislation or specific standards to promote good practice, and details how these principles can be applied to managing cyber security in the built environment. The need for specific cyber security measures will depend on the profile of the built asset, its use and the persons who occupy or use it. The Code of Practice focuses on built asset/building-related systems and, where they occur, all connections to the wider cyber environment. It adopts a straightforward approach, centred on risk management, which supports detailed thinking on the activities and controls required to manage the cyber security of an organization's built asset or building-related systems. It is important that the owners and operators of the built asset or building-related systems cooperate and collaborate with other users of information and communications technologies within the built asset. Other users include those who operate the organization's desktop and central IT functions, and where the built asset contains controls systems, such as industrial automation and control systems (IACS), with the relevant operations and engineering departments.

This Code of Practice is intended to be used as an integral part of an organization's overall risk management strategy and subsequent business planning, to ensure that the cyber security of the built asset/building-related systems is managed cost-effectively as a core part of the organization's business.

A companion NCSC sponsored Code of Practice regarding cyber security and safety is available on the IET website https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/.

[1] FireEye *Blog on SolarWinds attack* https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

[2] Microsoft *Blog on SolarWinds attack* https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

Section 1

Introduction

In this Code of Practice the term 'built asset' is used to encompass a broad range of constructed assets, ranging from individual buildings, to linear structures (for example, tunnels, pipelines and transport infrastructure) and collections of assets, such as campuses.

1.1 Aim and objectives

The aim of this Code of Practice is to provide guidance to a range of readers so that:

(a) a systematic approach is taken to the application of cyber security in the built environment that reduces the risks to their built asset, those occupying or using it, as well as those risks to the wider built environment that may be caused by their built asset or arise from cyber attacks against either their built asset or the wider environment;
(b) responsibilities and lines of accountability are clear, and the right person does the right thing at the right time in the lifecycle of the built asset(s);
(c) cost-effective security of information and control systems can be achieved and the systems are Secure by Design;
(d) protective security measures are included in the engineering design of individual built assets from the outset to deliver a secure and resilient built environment, and so that costly reworks are avoided;
(e) automated electronic security surveillance and monitoring systems (for example, CCTV with analytics and automated alert capability), whether internal or through an external interface, will be managed as a security risk with responsibilities for monitoring and incident response added to lines of accountability (for example, through communication between accountable parties for physical security and cyber security);
(f) a holistic design for the physical and cyber security of the built asset is developed based on a risk assessment that includes the wider interface of the built asset with any other systems that have the potential to affect the operational resilience of the built environment and the information assets of the business;
(g) a holistic design of physical and cyber security systems/infrastructure takes into account big data opportunities within the wider built environment that enhance security, for example, through integration of physical security infrastructure management and the monitoring of BMS and data network operations; and
(h) a prioritized lifecycle objective is for all security measures to be measured against a catastrophic failure event to ensure ongoing operations or degraded operations are secured.

To achieve this aim, the Code of Practice has the following objectives:

(a) to enable built asset owners and relevant stakeholders to create and implement an effective cyber security management system for their built assets within the built environment, taking into account the assets' context so as to address threats to their safety, security and resilience;
(b) to provide clear practical guidance so that multidisciplinary teams can understand and share how the management of various aspects of information and cyber security apply to their job roles and their personal responsibilities in maintaining the security of the built asset(s) and the surrounding built environment;
(c) to provide guidance that is easily understood and usable by a wide range of individuals from both technical and non-technical backgrounds; and
(d) to encourage integrated management of security risks to the built asset, including those from the supply chain, through an approach that can be monitored by the facility management.

To achieve these aims, this Code of Practice identifies questions to ask and describes the issues to be considered. It is not intended to be a checklist of efficient cyber security for the built environment. Unlike cyber security guidance published about generic IT or control systems, this Code of Practice addresses the complexity of both a built asset and the stakeholders' lifecycles, as the built asset progresses from concept through design, construction, operation, modification and potentially eventual demolition.

1.2 Who should use this Code of Practice?

This Code of Practice is especially applicable to the organization's board or other senior management functions that are required to take strategic decisions within an organization that owns, operates, occupies or otherwise uses a built asset. It is relevant to a wide range of job functions connected to the design, management, operation and security of any built asset-related systems, including those job functions responsible for:

(a) financial and operational management of the built asset(s);
(b) management of information relating to the built asset, security and systems;
(c) personnel and contractor security;
(d) ensuring that appropriate cyber security policy and associated procedures exist;
(e) ensuring that appropriate procedures are implemented;
(f) specification and design of systems, associated software and technologies;
(g) sale and systems integration of built asset-related systems;
(h) management of specific security tasks;
(i) safe and secure operation of all equipment, plant and machinery; and
(j) tertiary educators in systems engineering, security, architecture, construction disciplines and business administration.

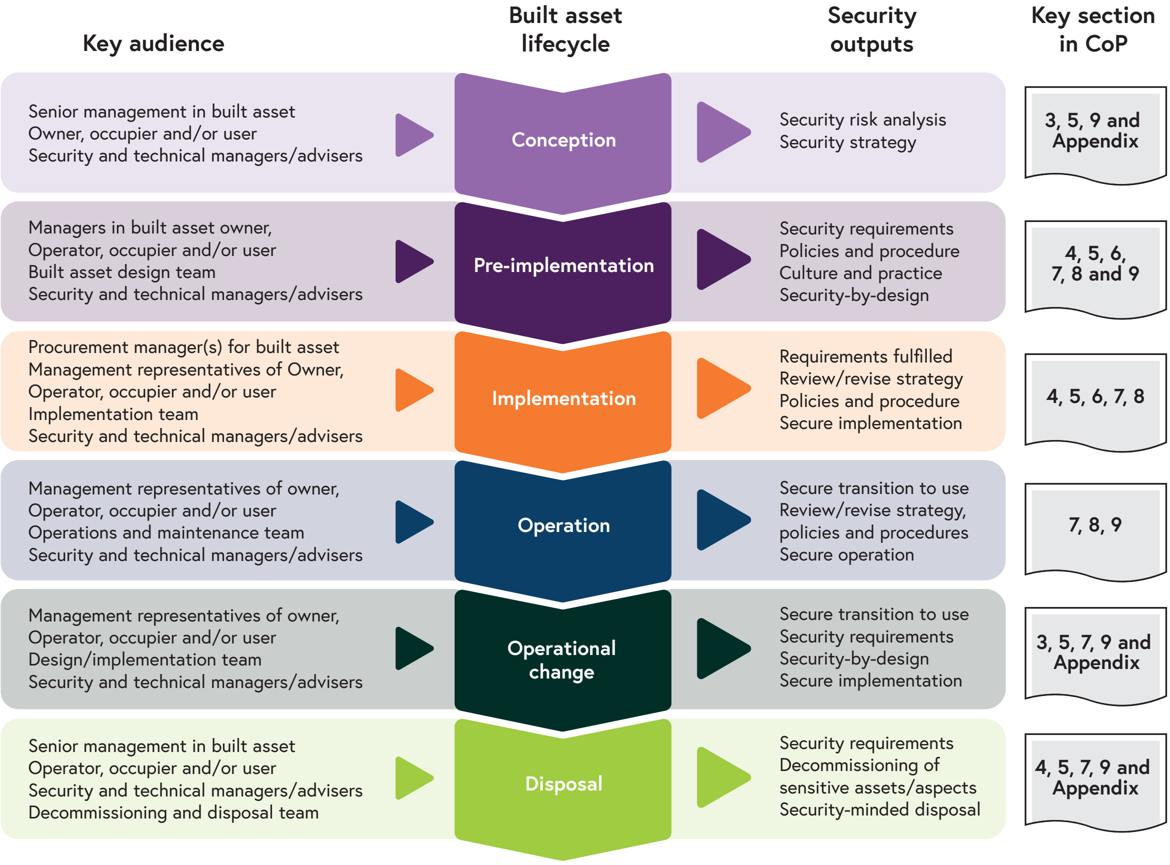
As illustrated in Figure 1.1, the Code of Practice follows a generic building lifecycle. Following the introduction in this Section, the body of this document contains the following Sections:

(a) Section 2 provides an overview of the use of digital technologies in the built environment, the implications for information management and cyber security, and the identification and management of security risks.
(b) Section 3 provides an overview of key security principles for built assets, their ownership, occupation and use.
(c) Section 4 examines security over the built asset lifecycle.
(d) Section 5 addresses the application of cyber security through the lifecycle of a built asset.
(e) Section 6 explores the management of technical aspect of built asset systems.
(f) Section 7 describes the management of process aspects relating to the security of asset information and the cyber security of built asset systems.
(g) Section 8 discusses the management of the people aspects.
(h) Section 9 outlines the application of the Code of Practice.
(i) Annex A discusses risk management in the context of built assets and their systems.

The Code of Practice will also benefit individuals who wish to improve their knowledge of cyber security and who may not be from a traditional security-trained background or experienced in managing built asset-related systems. It is unlikely that these individuals will have the specific knowledge associated with cyber security as part of their core competency.

When a built asset is owner-occupied, this Code of Practice may be used to influence the design and improve the security of the built asset during design, construction and subsequent operation. From a built asset occupier's or user's perspective, this Code of Practice may help to understand the cyber security

Figure 1.1 Structure of this Code of Practice



Key audience	Built asset lifecycle	Security outputs	Key section in CoP
Senior management in built asset Owner, occupier and/or user Security and technical managers/advisers	Conception	Security risk analysis Security strategy	3, 5, 9 and Appendix
Managers in built asset owner, Operator, occupier and/or user Built asset design team Security and technical managers/advisers	Pre-implementation	Security requirements Policies and procedure Culture and practice Security-by-design	4, 5, 6, 7, 8 and 9
Procurement manager(s) for built asset Management representatives of Owner, Operator, occupier and/or user Implementation team Security and technical managers/advisers	Implementation	Requirements fulfilled Review/revise strategy Policies and procedure Secure implementation	4, 5, 6, 7, 8
Management representatives of owner, Operator, occupier and/or user Operations and maintenance team Security and technical managers/advisers	Operation	Secure transition to use Review/revise strategy, policies and procedures Secure operation	7, 8, 9
Management representatives of owner, Operator, occupier and/or user Design/implementation team Security and technical managers/advisers	Operational change	Secure transition to use Security requirements Security-by-design Secure implementation	3, 5, 7, 9 and Appendix
Senior management in built asset Operator, occupier and/or user Security and technical managers/advisers Decommissioning and disposal team	Disposal	Security requirements Decommissioning of sensitive assets/aspects Security-minded disposal	4, 5, 7, 9 and Appendix

risks, both in respect of physical security risk associated with use of the built asset and the potential use or misuse of data or information relating to its occupancy or use.

The Code of Practice includes an annex providing more detailed information about assessing and managing cyber security risks related to the built environment, and the factors to be considered in assessing the context of built asset systems. A glossary of technical terms and a bibliography of relevant standards and guidance material are also included as annexes.

The approach adopted in this Code of Practice is principles-based: it outlines the good practice principles that may be applied to achieve the aim and objectives set out in Section 1.1. By adopting this approach, the Code of Practice offers flexibility rather than prescribing technical solutions that may not address specific threats to a built asset. Owners, operators, occupiers and users should use these principles to identify and adopt appropriate and proportionate cyber security measures to protect their built assets based on a contextualized risk assessment.

1.3 Applicability

This Code of Practice is applicable to built assets associated with a wide range of organizations, irrespective of size, including the industrial, commercial and public sectors. The degree to which cyber security is a significant issue will depend on the context, which varies from one built asset to the next, and is determined by the nature of the built asset, its use and/or occupants and the impact that a cyber security incident could have on its use, and the benefits the built asset is designed to deliver.

In this document the terms 'built asset', 'built asset data', 'built asset systems', 'built asset systems owner' and 'information asset' are used. These terms are defined as follows:

(a) built asset: encompasses individual buildings (for example, offices, factories, data centres, airports, stations, hospitals, hotels, etc.), campuses, sites, structures (for example, tunnels, pipelines, roads, railways, etc.), including their immediate physical environment.
(b) built asset data: encompasses any data, information, models and processes that are associated with the ownership, design and operation of a built asset. This includes the collaborative databases that are referred to as Building Information Modelling[3] (BIM) as well as information relating to operation of the built asset, for example, computer-aided facilities management (CAFM) systems.
(c) built asset systems: the systems deployed will depend on a built asset's nature and use, but may include combinations of the following types of digitally-based system:
   i. lighting automation and control;
   ii. heating, ventilation and air conditioning (HVAC);
   iii. fire, smoke detection and alarms;
   iv. motion detectors, CCTV, security and access control;
   v. lifts and escalators;
   vi. industrial processes or equipment;
   vii. shading devices; and
   viii. energy management and metering;
(d) built asset systems owner: the organization that owns the systems and is ultimately accountable for the safe operation and maintenance of the systems.
(e) information asset: data that has a specific context, which may be in digital or print form, and has actual or potential value to an individual, an organization or a government.

This Code of Practice is intended to cover built asset systems, their control and integration.

In addition to the above cyber-physical systems, which are often generically referred to as building management systems (BMS), building automation and control systems (BACS) or industrial automation and control systems (IACS), supervisory control and data acquisition (SCADA) systems, this Code of Practice covers IT systems used in the design, construction, operation and maintenance of the built asset.

1.4 Relationship between the built environment, built asset lifecycles and asset information

Built assets rarely exist in isolation and form part of a built environment, with elements effectively integrating the asset and environment, for example, the means of pedestrian, goods and in some cases vehicular access to the built asset, and connections from the built asset to utility networks. Some built assets are essential for the operation of the built environment, such as providing transport, water, gas, electricity and communications infrastructure. The wider built environment is, therefore, an ecosystem where there may be dependencies upon the built asset and vice versa. These dependencies can be in terms of physical or digital relationships and/or the provision of services from or to the built asset.

[3] The term Building Information Modelling potentially covers a wide range of digital engineering activities, ranging from the electronic exchange and collaborative storage of design documentation, 3D graphical modelling of built assets, which may be purely representational (for example, a visualization of building design) or simulations (for example, presentation of pedestrian or traffic flows, CCTV fields of view, etc). The term digital twin is a currently being used, often indiscriminately, to encompass a variety of models ranging from design simulations to more complex built asset control systems.

Section 1 – Introduction

The development of and changes to built assets often require the sharing of asset information, such as obtaining planning consents and regulatory approval. This integration and information sharing could result in the disclosure of sensitive information if appropriate information management is not implemented by built asset owners and those managing information about the wider built environment.

This Code of Practice can be applied to a built asset at any point in its lifecycle, including:

(a) during the specification, design, construction and operation of a built asset;
(b) when changes are made to the design and operation of an existing built asset; and
(c) when there is a change in ownership of an existing built asset, a perceived risk or a change in use of the built asset.

The complexity of built asset and technology lifecycles and their interaction is examined in Section 4.

Management of built asset information is an important issue. The use of digital technologies across all stages of the asset lifecycle increases the risk that sensitive or potentially sensitive information about the built asset, its occupancy or use, may be disclosed, thus enabling its malicious exploitation by third parties. The relationship between information management and cyber security is examined in Section 2 and illustrated in Table 2.1. While both should address security in a holistic manner, by considering the relevant aspects of governance, personnel, physical and technical security domains, cyber security is often perceived as a practice that primarily focuses on the technology aspects rather than addressing the broader information management or governance issues.

This Code of Practice encourages built asset owners, operators and users to adopt a holistic approach to security by adopting an integrated approach to information management and cyber security. An appropriate security strategy can only be established once there is a clear understanding of the value of the built asset-related data/information and the built asset systems and supported business processes. Only then can appropriate investment be made in effective security measures to mitigate security risks, whether originating from the personnel, physical or technical security domains.

Section 2

Overview

This Section provides an overview of the application of digital technologies in the built environment.

It explains what cyber security is and identifies typical cyber security needs across the built asset lifecycle. It also examines the built asset-related stakeholder roles that are potentially involved in maintaining cyber security of a built asset.

2.1 Application of digital technologies in the built environment

2.1.1 Information technology (IT) and operational technology (OT)

The built environment employs a wide range of technologies across the lifecycle of a built asset.

The IT systems employed in the built environment include personal IT devices (such as tablets, laptops and desktop computers), communications and networking infrastructure, and the use of processing and storage systems that may be provided as local servers, which are hosted in data centres or cloud-based platforms. The OT is the cyber-physical system that forms part of the built asset and its environment to deliver services such as HVAC, lighting, access control, people and goods movement (lifts and escalators). This OT typically comprises elements that are recognized as IT (for example, an operator workstation with a Windows™ operating system, running built asset system applications) and more specialist elements (for example, programmable logic controllers (PLCs), sensors and actuators). The term OT is widely used in the context of process, production and engineering control systems, which – depending on the nature of the built asset(s) – may be a core part of an asset's business function. In this wider context, the OT elements may include SCADA, IACS and DCS.

During the strategy, business case and design stages of the built asset lifecycle there will be extensive use of conventional IT, with office and design applications run both locally and on cloud platforms. The IT technologies employed are familiar to IT and cyber security professionals and the security threats to the technology are broadly understood.

The increasing use of Building Information Modelling (BIM) has seen a significant rise in the use of 3D models and collaborative file and data storage environments, known as common data environments (CDEs). The term 'digital twin' is currently being used to refer to a virtual representation of a built asset. It is important to understand the nature and limitations of digital twins, as well as the potentially related threats and vulnerabilities. At their simplest these models may be graphical and/or computational representations of the asset for a specific purpose, such as modelling energy use and efficiency. These models may be used during the design of the built asset and during its operation to compare projected and actual performance using static data. More sophisticated models may permit evaluation of changes, the 'what-if' analysis of modifications to the operation of the asset and its systems, which is again based on static collected data. It is proposed that some digital twins should have connectivity to systems in the built asset, with live exchange of data between the twins. In this scenario, the digital twin is a control system and should be treated as OT, with appropriate testing validation and security in place.

Site-based aspects of the design, such as surveying, are increasingly using an array of digitally enabled technologies such as light detection and ranging (LIDAR) scanning to obtain point clouds from which 3D models of surrounding assets may be developed. The topographical surveying of a site may involve use of GPS-enabled surveying tools and use of drone-borne cameras to provide aerial views of the site. The adoption and use of new technologies can create new risks, for example, those arising from the capture of sensitive information about existing and neighbouring built assets, or from the potential vulnerabilities of the devices themselves.

During the construction phase there can be a range of IT and OT assets in use. The IT will primarily be the same as outlined above, although there may be significantly more use of portable personal IT devices, for example tablet devices and mobile phones used to capture site information and update construction information. Recent developments have seen the use of some OT during asset construction, for example, the use of robotic and/or semi-autonomous equipment to support and enhance the performance of construction workers. For safety and security reasons there has also been an increase in the use of electronic security controls for site access and of IoT devices worn by the workforce to monitor their location, health and safety.

This increased use of digital technologies on construction sites creates new attack surfaces that may be exploited. For example, use of near real-time built asset site-wide reporting systems that integrate sensors and other reporting systems may expose interfaces to systems used to record the as-built data. Awareness of how these automated systems are deployed and used is important for all disciplines involved in the work, with appropriate functionality provided to allow interrogation of captured data and enable recognition of anomalous or erroneous data. Awareness of the vulnerabilities should inform the assurance and security of this dynamic data capture process, so that confidence in the provenance and quality of the data is maintained for the duration of a project.

During the later stages of construction, the OT systems that are required to operate the built asset will be installed, tested and commissioned ready for asset handover to the asset owner/user. During these works the OT systems will be accessible to a number of contractors and/or suppliers who will be testing and configuring the systems. This can create a range of potential vulnerabilities related to the authenticity of components (hardware and software), the entities that have on-site and/or remote access (whether authorized or not), and the transition from testing/commissioning to operational readiness. Increasingly, there is connectivity between the OT system and the internet (for example, for remote monitoring or support) and/or the enterprise IT network used by the built asset owner/operator/occupier. This connectivity can create further vulnerabilities because IT security managers rarely have visibility of the OT systems and their external connectivity.

Given the relatively short life of most digital technologies compared with the built assets, there will be a number of technology refreshes over the lifecycle of a built asset. Associated vulnerabilities include obsolescent and unsupportable systems/components, hybridization of systems through integration of old and new technologies, and exposure of previously standalone systems to internet-connected systems. To address emerging security vulnerabilities over a system's lifecycle it is important that the support arrangements include the provision, installation and testing of patches for software and firmware. An important part of managing assets that include software components is to know how long the supplier plans to support it with updates, how these will be obtained and deployed, and how software obsolescence will be addressed when the updates stop.

2.1.2 Connected and smart buildings

In the built environment ecosystem, the level of connectivity of buildings and degree to which they are 'smart' varies considerably. Typically, the intent is to provide a variety of monitoring (for example, energy, environmental and occupancy) to inform and optimize the use of systems to make the best economic use of the built asset while maintaining a comfortable and healthy environment for occupants. Often a key aim is to achieve energy efficiency by reducing energy consumption in areas that are unoccupied or lightly occupied, or through making maximum use of environmental factors to reduce the need for energy intensive heating or cooling, or demand management to improve electricity grid performance.

The smart element of a building may involve the use of data gathering and analytics or machine learning to optimize the performance of the built asset. However, the concept of demand-side management of electricity will see the built assets, and their appliances, offering flexibility by modulating levels of demand and/or local generation or discharge of stored electricity. Innovations like this are intended to create a more sustainable built environment, with the smart elements enabling a collaborative approach to the use of constrained resources. Cyber vulnerabilities may exist in a smart building implementation and need to be addressed at the design and construction stages.

Conceptually, a connected building may have networked and communications-enabled devices providing remote monitoring data feed to entities that support or manage plant and machinery that support the use of the built asset. For example, lift manufacturers collecting telemetry data from their installed lifts to monitor for early signs of failure and then to dispatch spares and maintenance personnel to fix the potential fault before service failure occurs. Connectivity may also be used to enable alternative business models for the plant and machinery, such as Heat as a Service models where a service provider retains ownership of the equipment in return for a performance-based heating contract.

In connected and smart buildings, the technology and flow of data to third parties can introduce a variety of vulnerabilities. For example, the potentially increased risk that one or more of the connections may be deliberately or inadvertently connected to the occupier's enterprise IT network, thereby providing a backdoor. There is also potential for collected systems data to be used to model the pattern of life of the building's occupants and/or pattern of use of rooms or zones within the built asset, which may be used for malicious purposes.

The recent compromise of SolarWinds' IT monitoring and management tools is an example of how an organization can be compromised by trusting an apparently trustworthy third party. While this example relates primarily to IT networks, rather than building automation and control systems, a similar compromise of a trusted third party occurred in the Target stores breach[4], which exposed the credit card and personal data of over 100 million consumers. In this case, credentials relating to an HVAC maintainer were used to gain access to the company's supplier portal and from there a sophisticated attack was mounted on the company systems.

2.1.3 Digital engineering and built asset information

As mentioned in Section 2.1.1 the widespread use of digital engineering tools, such as 3D modelling and laser surveying, presents a number of risks to entities wishing to protect sensitive information relating to their built assets. The use of these digital technologies should be supported by appropriate information management and cyber security policies to reduce the risk that built asset information may be used to harm the security and/or safety of the asset and those occupying or using it. A particular concern regarding built assets with a high public profile, for example, those supporting defence or law enforcement, and those that form part of critical national infrastructure, is that unauthorized access to the 3D models and asset information may aid hostile reconnaissance. To address such concerns, the Centre for the Protection of National Infrastructure (CPNI) guidance on built asset security[5] and the recently published 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*

[4] Radichel T. *Case study: Critical Controls that Could Have Prevented Target Breach* Bethesda, MD: SANS Institute, 2014. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

[5] CPNI *Security-Minded approach to Digital Engineering* https://www.cpni.gov.uk/security-minded-approach-digital-engineering and CPNI *Security-Minded approach to Information Management* https://www.cpni.gov.uk/security-minded-approach-information-management

building information modelling. Part 5: Security-minded approach to information management[6] provide a security framework for use throughout the built asset lifecycle.

2.1.4 Security of endpoints

Given the nature of the architecture, construction and engineering industries there is a high level of subcontracting. This expands the attack surface through the connection of third-party devices, whether owned by an organization or by an employee or tradesperson – in terms of bring your own device (BYOD) – to built asset systems. The related cyber risk can arise from compromised devices (for example, laptops and tablet devices) and from end-point peripherals such as mice, keyboards, printers and barcode scanners. While the threat from rogue devices is generally understood and can be mitigated through good cyber hygiene, such as the adoption of the government-backed Cyber Essentials recommendations, the threat from malicious hardware or peripherals receives less attention. Depending on the peripheral, this risk can be mitigated using specialized solutions that detect compromised hardware and by purchasing peripherals from reputable sources.

2.2 Information management and cyber security

The protection of built assets and built asset information encompasses two related but separate disciplines: information management and cyber security. These disciplines are compared in Table 2.1 and key aspects are described further in Sections 2.2.1 and 2.2.2.

Table 2.1 Comparison of information management and cyber security

	Information management/security	Cyber security
Description	An organization's governance, strategies, policies, processes, controls and culture employed to optimize data and information use to meet its business needs while minimizing risks. This is achieved through inter-system and inter-organization data and information integration and exchange and, where applicable, in compliance with legal and industry regulations.	The application of technologies, processes and controls devised and implemented by an organization to protect data, software, systems, networks, and devices from unauthorized access and attack.
Covers	Covers the information lifecycle from its source through capture, maintenance, use, synthesis, publication, to archival or in many cases, to purging or destruction. This lifecycle should be supported by appropriate measures to assure and maintain the quality of the organization's data and information.	Covers the system lifecycle from planning through analysis, design, development, integration and testing, implementation, operations and maintenance and eventual decommissioning. While the system should maintain data and information integrity, i.e. prevent unauthorized changes, it does not assure the quality of the data and information.
Approach	Provides a foundation for assessing information risk and prioritizing security measures and investment by identifying the criticality and/or sensitivity of data and/or information used by an organization.	A risk-based approach that focuses on an organization's critical and/or sensitive assets, whether physical or digital, taking into account system vulnerabilities and the nature of the threat environment.
Focus	Focuses on the value of data and information to an organization and its stakeholders and potential harm that may arise from its misuse.	Focuses on the value of systems and supported business activities to the organization and its stakeholders.
Output	Develops an inventory of the data and information required by an organization, its relationships and use of data by the organization and its stakeholders.	Develops an understanding of the role and relationships of systems in the delivery of an organization's business functionality and operation.

[6] 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. Part 5: Security-minded approach to information management*

Table 2.1 Cont.

	Information management/security	Cyber security
Access	The sharing of data and information is often subject to both legal constraints and to sharing agreements established between the organizations involved.	External access to an organization's systems, whether by individuals, organizations or other systems typically involves technical access control measures and secured interfaces.
Aggregation	Should address the risks associated with aggregation, whether by volume or by association, or both.	Should address technical mitigations that may evolve as aggregation takes place and threat actor motivation changes accordingly[7].
Goals	In addition to the cyber security goals, also takes account of safety, utility (i.e. long-term usefulness of the data), authenticity (i.e. data provenance) and its possession (for example, data subjects' rights).	Traditionally focusses on three security goals: confidentiality, integrity and availability. Generally little recognition of the interaction between safety and security.

2.2.1 Information management

In the built environment information management is the approach used to maintain data quality over the built asset's lifecycle, where quality is related to the fitness for purpose of the decisions that are or will be made with the data. When considering built asset information, quality key attributes include relevance, clarity (the meaning of the data), consistency (data having the same meaning for different parts of an organization or different stakeholders), accessibility and security. Data and information have value, which is determined by properties such as accuracy, timeliness, completeness and provenance. However, there are costs and benefits associated with these properties, so if it is sufficiently accurate and timely, for the purpose for which it is or will be used, there is little benefit incurring additional costs to improve accuracy or make it available sooner.

From a security perspective it is essential to understand the value of the data and information to the built asset owner, its occupiers/users and to third parties (whether their intent is benign or hostile). Through this understanding, the appropriate and proportionate controls and protective measures can be deployed to protect the organization against actual and perceived threats, both now and in the future.

2.2.2 Cyber security

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 retain control and coherence, and enable trustworthy operation of the organization and users' assets in the cyber environment. Where:

(a) the 'cyber environment' (also referred to as 'cyberspace'), comprises the interconnected networks of electronic and computer-based systems, which therefore encompasses the internet (including an organization's intranet), telecommunication networks, computer systems, embedded processors and controllers, and a wide range of sensors, storage and control devices. Given the interconnected nature of many systems, it cannot be limited to only those elements that are controlled or owned by the organization;

(b) the 'organization and users' assets', which includes personnel, applications, services, social; and

(c) business functions that exist only in cyberspace, and the totality of transmitted, processed and/or stored data and information in the cyber environment.

Establishing digital trust is an exercise of symmetry, reciprocity and transparency with different stakeholders in the digital context based on the corporate/personal risk appetite(s) and the capacity to

[7] Government Security Classifications https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

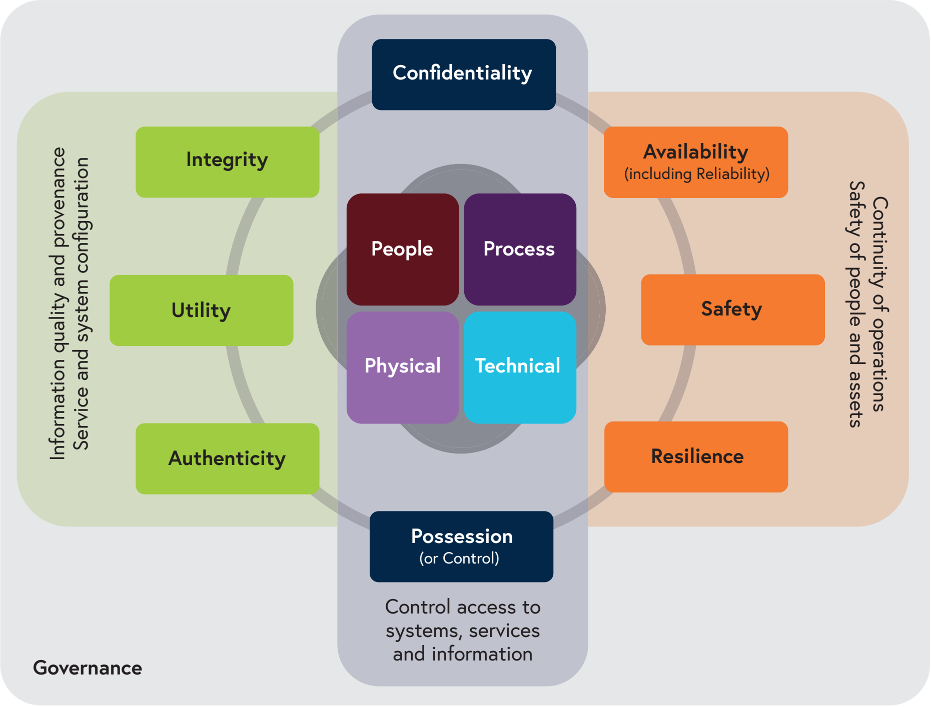
manage the risks. In the built environment, a key consideration is in what and whom are you as a business and/or individual placing your trust in, because the security responsibilities and governance in the cyber and built environments are generally not aligned.

It is important to recognize that the cyber environment includes its critical supporting infrastructure, for example, utilities, uninterruptible power supply (UPS), generators and main power switch boards. Experience shows that even systems thought to be standalone and isolated networks are at risk, from both attacks by malicious users and the introduction of malicious software via removable media. It should not be assumed that because a system is not apparently connected to the Internet or any other network it is therefore secure. In practice there may be built-in connectivity such as cellular phone technology, installed for ease of maintenance or remote system management. These capabilities, which system users are usually not aware of, may be used to allow the download and remote installation of patches and updates, or to provide automated diagnostic and fault reporting. Although currently the most common vector for cyber incidents affecting these systems is physical access via an intruder or insider, remote attacks are increasing in effectiveness as criminals look for unprotected routes to compromise critical systems.

2.2.3 Security goals

Given the differences in lengths of the lifecycle for the physical structure of built assets, their control systems, and typical organization IT systems and personal computing devices, this Code of Practice addresses cyber security management through a set of eight goals, as shown in Figure 2.1. By addressing these goals, appropriate solutions may be adopted and adapted over the built asset lifecycle in response to changes in the built asset and technology, the use of the built asset and technology, and the nature and severity of potential threats.

Figure 2.1 Eight security goals applicable across the four security domains (people, physical, process and technical)



Key cyber security goals as applied to cyber-physical systems are outlined below. When considering these goals, a risk management approach should be adopted, which will inform the degree to which any preventative or protective mitigation measures are implemented and the degree to which any residual risk is acceptable to and accepted by the built asset owner, operator or occupier (as appropriate). In assessing the residual risk, consideration should be given as to how resilient the organization and the built assets would be if the risk materializes.

(a) **Confidentiality**. The built asset system(s) and associated processes should be designed, implemented, operated and maintained to prevent unauthorized access, for example, to sensitive financial, medical or commercial data. All personal data shall be handled in accordance with the Data Protection Act 2018 and additional measures may be required to protect privacy due to aggregation of data, information or metadata, for example, where this could lead to occupants' patterns of life being identified.

(b) **Possession and/or control**. The built asset system(s) and associated processes should be designed, implemented, operated and maintained to prevent unauthorized control, manipulation or interference. An example would be the loss of access, for an authorized user, to a built asset system. There is no loss of confidentiality, system availability or integrity, but the system owner or user is no longer able to control the system.

(c) **Integrity**. The built asset system(s) and associated processes should be designed, implemented, operated and maintained to prevent unauthorized changes being made to assets, processes, system state or the configuration of the system itself and to automatically report such changes or attempted changes. A loss of system integrity could occur through physical changes to a system, such as the unauthorized connection of a Wi-Fi access point to a secure OT network, or through a fault, such as the corruption of a database or file due to the system being compromised through ransomware.

(d) **Authenticity**. It should be possible to verify the authenticity of inputs to and outputs from the built asset system(s), its state and any associated processes. It should also be possible to verify the authenticity of components, software and data within the system and any associated processes. Authenticity issues could relate to data, such as a forged security certificate, or they could be hardware related such as a cloned device or counterfeit system component.

(e) **Availability**. The built asset system(s) and associated processes should be consistently accessible in an appropriate and timely manner. If either a system or associated process suffers disruption or impairment, or an outage occurs, it should be possible to recover a normal operating state in a timely manner. A loss of availability could occur through the failure of a system component, such as a disk crash, or from a malicious act, such as a denial-of-service attack, preventing use of a system connected to the internet.

(f) **Utility**. The built asset system(s) and associated processes should be designed, implemented, operated and maintained so that the utility of the assets is maintained throughout their lifecycle. An example of loss of utility would be a situation where system sensors are replaced, and the replacements have different technical characteristics. Although the system continues to operate satisfactorily, changes in the quality of the collected data results and this compromise its use in long-term condition monitoring and trend analysis.

(g) **Resilience**. The built asset system(s) and associated processes should be designed, implemented, operated and maintained so that data, information, systems and any associated processes or services can transform, renew and recover in a timely way in response to adverse events. For example, if a building's HVAC system is dependent on cloud-based processing for energy efficiency functionality, the system should still be capable of operating and delivering a minimum acceptable HVAC capability in the event of a loss of connectivity with the cloud-based processing. Therefore, the building would remain habitable, but there could be some economic and environmental impact arising from the reduced energy efficiency.

(h) **Safety**. The design, implementation, operation and maintenance of a built asset system and its associated processes should be designed taking the above goals into account to avoid jeopardizing the health and safety of individuals, the environment or any associated assets. The disciplines of safety and security have historically been managed independently, but with digital technology the interdependencies must now be actively managed. A safety issue could arise through malware causing a failure to display or communicate a system's alarm state, such as a smoke detector, which then resulted in damage to property or loss of life. Safety and security may be defined as separate sets of initiating events (malicious or accidental, respectively) that can lead to a common set of adverse outcomes. However, the measures to assure safety can be undermined by malicious actors and the measures to assure security can be undermined by accidental user actions or component failures. Consequently, the interaction between safety and security measures should be understood so that safety-related decisions, whether related to design or operation, actively support and do not undermine security requirements and vice versa. Where conflict occurs between safety and security requirements or proposed implementations, maintaining systems security – specifically preventing loss of control – should take precedence since safety measures are generally predicated on the system being in control. The rationale for the implemented approach should be clearly understood, documented and appropriately approved. Where specific functional safety required to achieve an acceptably low risk of harm then IEC 61508 series *Functional safety essential to overall safety* should be considered.

Section 3

Security principles

This Section identifies five top-level principles that should be applied to the application of digital technologies in the built environment:

1. senior management accountability (Section 3.1);
2. holistic approach to security (Section 3.2);
3. security goals for cyber-physical systems (Section 3.3);
4. balanced approach to safety and security (Section 3.4); and
5. managing change (Section 3.5).

The principles are examined in further detail in later Sections in this Code of Practice. It is important that senior managers avoid inadvertent or unintentional simplification or trivialization of the application of the principles.

3.1 Senior management accountability

Senior (board-level) managers, should have an awareness of and responsibility for cyber security and put in place appropriate governance to mitigate threats and prevent harm to the built assets and their environment.

Commentary

The development of new/next generation systems and functionality is leading the evolution of traditional, largely standalone, built asset systems into ecosystems. These may include a combination of:

(a) federated systems or software as a service (SaaS) solutions, such as cloud-based platforms that may service multiple organizations;
(b) IoT architectures, such as the use of sensing data to provide insights and intelligence about asset condition, performance and use; and
(c) embedded machine learning (ML)/AI, such as algorithms processing sensors and other data to optimize the use of the built assets, and reduce resource consumption and greenhouse gas emissions.

As a consequence of these and other technology developments, asset owners/users will need to adopt governance arrangements that accommodate data and information sharing coupled with appropriate security and privacy measures, with allocation of responsibility addressing the capacity and capability to manage risks. In these ecosystems, suppliers will typically have lengthy terms and conditions that seek to limit responsibility for any failure or inaction on their part that affects security.

Levels of uncertainty or residual risks that escalate from this complexity of connectedness in next generation systems will need a thorough understanding of the threats, opportunities and vulnerabilities with clear levels of explanation and frequent updating of mitigation measures to meet new risks and to comply with corporate governance requirements on risk reporting.

3.2 Holistic approach to security

A holistic approach to cyber and cyber-physical security should be adopted, addressing risks and control measures in the four security domains: physical, people, process and technical.

Commentary

In developing an appropriate governance and security regime for built assets, the relationships between security domains is critical. Although well designed and technically secure, the operation of a system can be compromised through:

(a) poor personnel security (for example, addressing the insider threat through employment screening, particularly of sensitive roles, and use of role-based access to systems, or failure to establish an appropriate security culture supported by security awareness training);

(b) loss of system-physical integrity that may arise from poor access control to, or protection of, components and infrastructure as a result of theft, vandalism, tampering or unauthorized modification;
(c) a lack of ineffective implementation of processes and procedures to secure, maintain and operate the systems (for example, a joiner and leavers process that fails to remove user accounts when personnel, such as staff and contractors, cease to have authorized access to a system or that fails to change system privileges as personnel change roles and responsibilities); and
(d) catastrophic loss of resilience whether brought about through natural hazards, accidents or attacks (that may be cyber, cyber-physical or physical in nature), which may deny access to the built asset and/or its systems, or reduce the availability of key operational personnel.

The security domains may be managed by different people and departments within an organization, but it is the responsibility of senior managers to ensure that there is effective co-ordination and co-operation between the domains.

3.3 Security goals for cyber-physical systems

In developing and implementing security measures, the following security goals should be derived from the business requirements for the built asset, its systems and associated processes or services. These goals should maintain:

(a) possession – they are designed, implemented, operated and maintained to prevent unauthorized control, manipulation or interference with their function or use;
(b) confidentiality – to manage access to and prevention of unauthorized access to data and information, both in isolation and in aggregate;
(c) availability (including reliability) – they should be consistently discoverable, accessible, usable and, where appropriate, can be disclosed in an appropriate and timely fashion;
(d) safety – they should be designed, implemented, operated and maintained to prevent the creation of harmful states, which might lead to injury or loss of life, or unintentional environmental damage, or damage to assets;
(e) resilience – an ability to transform, renew and recover in a timely way in response to adverse events;
(f) integrity – maintaining the completeness, accuracy, consistency, coherence and configuration;
(g) utility – data and/or information should remain usable and useful across the lifecycle of the data and information, and of any associated asset, individual, organization; and
(h) authenticity – the provenance should be verifiable in respect of:
 i. data and/or information input to, and output from systems;
 ii. the systems and their state; and
 iii. any data and/or information relating to the built asset and/or its environment.

Commentary

The above goals are applicable at varying levels across business systems and functions and cannot be treated in isolation. For example, in a cloud-based built asset system:

(a) who actually has possession of the data? Who is the controlling party providing the storage media on which the data resides? In which jurisdiction is the storage media located? and what are the business's rights to recover the data in the event of supplier failure or dispute? There may be a number of sub-contracts between the business, application provider and the party actually hosting the data.
(b) who has access to the data, the application provider, their support personnel, the hosting provider and its support personnel? If the application provider is part of a larger organization, does the parent organization have access to the data?
(c) how is availability of the cloud-based system measured and what is the consequence of a loss or poor performance of the connectivity between the built asset and the application? What happens if there are internet issues with your own service provider, the hosting provider's internet service or, more generally, as a result of events affecting the global internet infrastructure? If the built asset loses connectivity to the application, are the systems within the asset adequately resilient to enable its continuing use?
(d) how can you establish that the data stored and processed in respect of the built asset is authentic and that its integrity is being maintained – and that, if you change to another application supplier, the historic data will be accessible and meaningful in the new application?

Answering these types of questions is not a one-off exercise to be completed during the procurement of an asset or service, they will need to be periodically revisited to ensure that changes in business need, the application/product/service and the supporting supply chain are monitored and the risks managed. Where these questions cannot be answered, or provision cannot be made for agreements on cloud transparency and security monitoring, there should be an allowance for uncertainty of security and a weighting given to this on the achievement of security goals. This should be part of the reporting procedure for corporate governance management in the organization.

Where the business owner is a tenant or has acquired, or wants to acquire, shared accommodation as-a-service, then additional due diligence checks are needed to assess the vulnerability associated with the built asset and its electronic systems.

3.4 Balanced approach to safety and security

While developing and operating the built asset, a balance should be struck between safety and security on a case-by-case basis to ensure that that the measures employed to achieve one approach do not undermine the other.

Commentary

This is not an issue regarding one approach overriding the other, it recognizes the need for careful consideration of how specific safety measures affect security and vice versa. As noted in Section 2.2.3(h) avoiding loss of control is essential in maintaining safety functionality. IEC TR 63069:2019 *Industrial-process measurement, control and automation - framework for functional safety and security* provides guidance on balancing the requirements and conflicts between safety and security.

3.5 Managing change

The increasing integration and interoperability of built environment systems presents both threats and opportunities in respect of the security of the built asset(s). The security approach should aim to address and accommodate any new and/or emerging threats arising from convergence and hybridization of technologies, as well as those extant in current and legacy systems.

Commentary

In the built environment change is inevitable, whether arising from external factors such as the environment, economy, business needs or competitive/societal pressures, or from internal factors such as the difference in lifecycles of the asset itself and the digital technologies. These changes and trends involving the convergence and hybridization of information and operational technologies will result in new/emerging threats and may expose new vulnerabilities or increase the impact of known vulnerabilities. Senior management needs to research and understand the threats and opportunities that arise when adopting new digital technologies.

Section 4

Security over a built asset's lifecycle

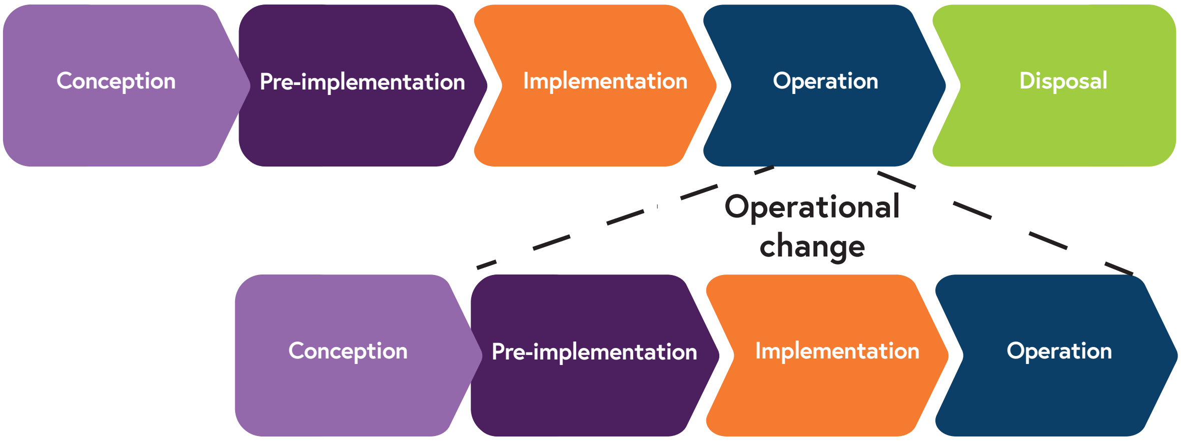
This Section describes the generic built asset lifecycle used in this Code of Practice. It explains what cyber security is and identifies typical cyber security needs across the asset lifecycle. It also examines the built asset-related stakeholder roles that are potentially involved in maintaining cyber security of a built asset.

4.1 The built asset lifecycle

Built assets typically have a lifecycle that can be measured in decades, unlike most digital technologies that experience refresh cycles in less than a decade. Apart from software patches and updates, which may introduce emergent risks, the core operational technologies in a built asset will change relatively infrequently. However, there will be elements connected to these operational systems that may change on a monthly or annual basis: for example, BYOD and equipment used by maintenance and facilities management personnel.

Built assets may undergo several changes during their lifecycle, including change of ownership and operational changes, such as change of use, physical reconfiguration and upgrades or refurbishment of structure, fabric, infrastructure and fixtures and fittings. For the purposes of this Code of Practice, the built asset will be discussed from the asset owner's perspective and will be considered to have the generic lifecycle shown in Figure 4.1.

Figure 4.1 Generic built asset lifecycle



The top-level elements of the asset lifecycle and their primary activities are:

(a) **Conception**. The initial identification of a business or operational need for a built asset or for an operational change affecting the asset, which could result in a decision to dispose of it.

(b) **Pre-implementation phase**. This phase of the lifecycle involves strategic decisions regarding the business or operational need and may lead to a decision to acquire an existing asset or commission the design (or redesign) and construction (or modification) of a new (or existing asset). From an asset owner's perspective, the lifecycle starts when there a need for a new or modified built asset is identified. From a tenant's or built asset occupier's/user's perspective, the lifecycle may start when they acquire the lease or the right to occupy the building.

During this phase, in addition to the development of the rationale or business case, work will be undertaken to develop the requirements or project brief along with the justifications for any change to the site occupied by the built asset, its structure, services, internal layout and/or use. The formality, scope and format of the strategy, business case and project brief will depend on the organization and the scale of the investment, or changes required.

(c) Implementation phase. Once a decision has been made to acquire an existing built asset, or commission the build of a new one (or modification of an existing asset), this phase encompasses the procurement and/or majority of the design activities. Typically, this involves the development of the project brief from the initial conceptual design of the built asset through to the detailed technical design. Depending on the complexity of the requirements and the scale of the work, the design may involve multiple stages, phases or iterations. Once the design work is complete, the acquisition and/or build/changes are implemented to fulfil the strategic/business requirement for the asset and prepare it for operational use.

(d) Operation phase. This phase encompasses the operational occupation/use of the built asset by the asset owner or tenant/occupier/user, and its maintenance. This phase of the lifecycle starts when the built asset is being used in the way it was intended.

During this phase, as illustrated in Figure 4.1, the built asset may be subject to a number of operational changes. These changes may be driven by a variety of factors, including change of use, changes to the fabric and changes to systems. These operational changes introduce security risks, as a result of changes in personnel, responsibilities and systems.

(e) Disposal phase. An asset owner may consider that ownership or use of a built asset is no longer justified on economic or business grounds and decide to decommission or dispose of it. Equally, a tenant or built asset occupier/user may consider the continued occupation or use of an asset is no longer required. From a built asset owner's perspective, the asset lifecycle ends when the asset has been decommissioned and its disposal or demolition is complete. From a tenant's or built asset occupier's/user's perspective, the lifecycle ends when they terminate the lease or cease to occupy the built asset.

4.2 Relationship of the built asset lifecycle to project lifecycles

The relationship between the first three stages of the built asset's lifecycle and a number of commonly used project lifecycles (or 'plans of work') is illustrated in Figure 4.2.

The security considerations across a generic built asset lifecycle are described in Section 4.3 and are based on implementation lifecycle stages shown in the first row of Figure 4.2. Examples of security-related deliverables across a built asset's lifecycle are shown in Table 4.1 (see page 35).

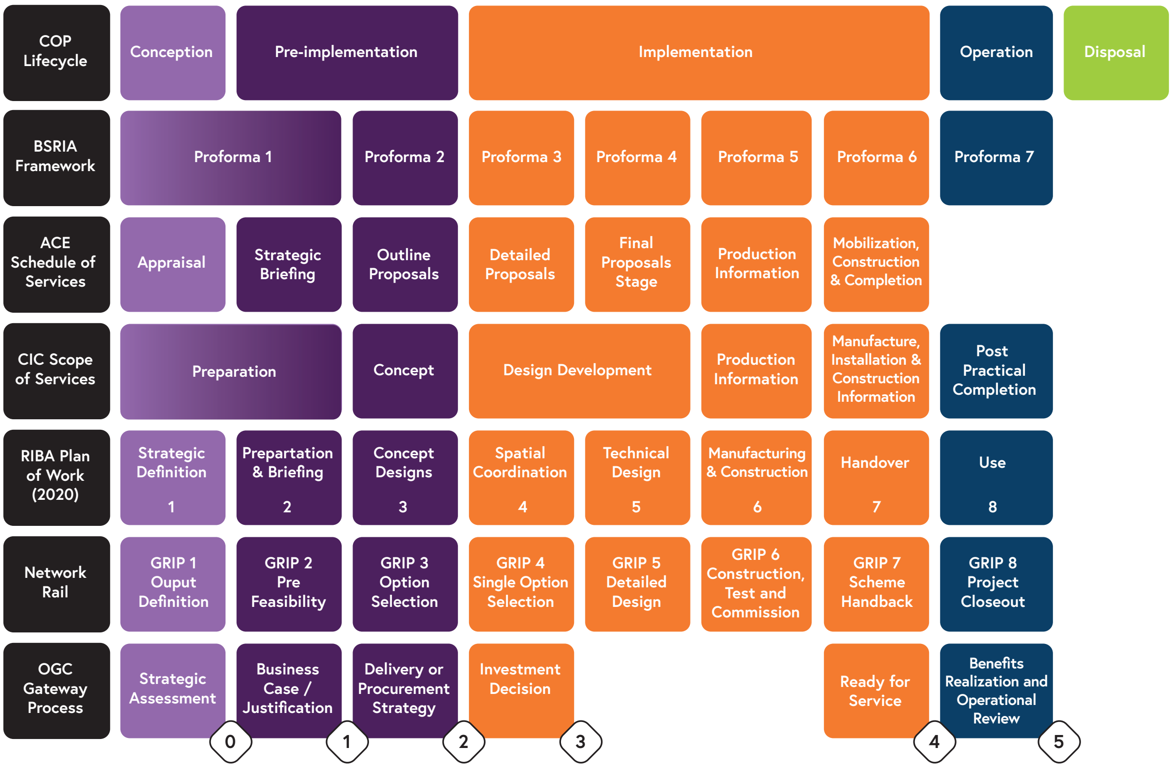
It is important to recognize that none of these plans of work are designed to accommodate the activities required during the disposal of a built asset. Secure disposal of a built asset can involve a significant range of security-related activities to ensure that sensitive data and/or information is appropriately handled, that personal data and commercially sensitive data is removed from built asset systems and that any connectivity to the asset owner's/occupier's/user's organization systems is securely disconnected. See Section 4.3.6 for further information.

4.3 Security considerations by lifecycle phase

The need for specific security measures will vary between built assets and across an asset's lifecycle. This Section addresses security from a holistic perspective and more information on the cyber security aspects is provided in Section 5. This Section outlines some basic requirements that are likely to affect

Section 4 – Security over a built asset's lifecycle

Figure 4.2 Relationship of the built asset's lifecycle phases to commonly used plans of work



COP Lifecycle	Conception	Pre-implementation		Implementation				Operation	Disposal
BSRIA Framework	Proforma 1		Proforma 2	Proforma 3	Proforma 4	Proforma 5	Proforma 6	Proforma 7	
ACE Schedule of Services	Appraisal	Strategic Briefing	Outline Proposals	Detailed Proposals	Final Proposals Stage	Production Information	Mobilization, Construction & Completion		
CIC Scope of Services	Preparation		Concept	Design Development		Production Information	Manufacture, Installation & Construction Information	Post Practical Completion	
RIBA Plan of Work (2020)	Strategic Definition 1	Prepartation & Briefing 2	Concept Designs 3	Spatial Coordination 4	Technical Design 5	Manufacturing & Construction 6	Handover 7	Use 8	
Network Rail	GRIP 1 Ouput Definition	GRIP 2 Pre Feasibility	GRIP 3 Option Selection	GRIP 4 Single Option Selection	GRIP 5 Detailed Design	GRIP 6 Construction, Test and Commission	GRIP 7 Scheme Handback	GRIP 8 Project Closeout	
OGC Gateway Process	Strategic Assessment 0	Business Case / Justification 1	Delivery or Procurement Strategy 2	Investment Decision 3			Ready for Service 4	Benefits Realization and Operational Review 5	

Note: The above plans of work are typical waterfall lifecycles, whereas the digital technologies employed in the built assets will often be delivered using more agile software development lifecycles, which may increase the integration risk.

most non-domestic built assets[8], where security of the assets depends on the creation and implementation of an appropriately governed security management regime based on:

(a) a regularly updated and reviewed security risk register addressing the four security domains (personnel, physical, process and technical);
(b) a security strategy for the built asset that is informed by the risks, including the information security, or lack of, both for existing assets and for new assets across their lifecycle;
(c) a security policy that is derived from the security strategy, reflecting the specifics of the built asset and its system design; and
(d) the design of appropriate security processes to implement the policy, supported by the appropriate use of repeatable security procedures.

A set of detailed security considerations for built assets and construction in the public realm is published by CPNI[9].

The following sub-Sections examine key security considerations across the lifecycle of a built asset.

4.3.1 Conception

At this point, the built asset owner (or occupier/user) will have identified a need for a built asset, or a change to a built asset they already own (or use). Any decisions will relate to the strategic needs of the

[8] The risks in individual domestic buildings are currently relatively low, as few homes have high levels of automation. Increased use of smart technologies within the home may change this in the future. This document is, however, applicable to large multi-occupancy residential buildings, for example, blocks of flats and student residences. Risks are now more likely to be introduced via individual IoT products.
[9] Security Considerations Assessment: https://www.cpni.gov.uk/security-considerations-assessment

potential built asset owner (or occupier/user). The key decision is often to undertake a more detailed study to develop a formal business case for the proposed action.

There will generally be a need for commercial confidentiality in this early phase of a major acquisition or construction project. Failure to maintain good security could result in the loss or premature disclosure of market-, price- or contract-sensitive information. In competitive situations where there is more than one party seeking to acquire the site or built asset, there may be the risk of commercial espionage. This is when a competitor or third party seeks to acquire commercially sensitive information to undermine or compromise one or more of the bids[10]. Good security needs to apply not only to the principals involved in the acquisition or commission, but to all professional advisers involved.

It is important to recognize at this early stage that information security (that is, the control over who has access to and needs to know about the strategy and the organization's intentions) is important. Disclosure of sensitive information through promotional channels, such as social media, press statements and corporate announcements, may alert competitors and/or those with hostile or malicious intent to the proposed investment (or disposal). Social media risks are applicable to employees of the organization, their professional advisers (dependent on the degree that they are aware of the plans) and those involved in the organization's supply chain.

4.3.2 Pre-implementation

Once an initial decision has been taken to commission, acquire or significantly modify a built asset, the next phase is the development of a detailed business plan. A number of commercially sensitive activities may be undertaken, with sensitive information being created, exchanged and stored electronically, including:

(a) development of outline design to inform costings, business case/plans, etc.;
(b) negotiations with financiers, investors and the existing site owner or their agent;
(c) preparation and submission of applications for planning consents;
(d) negotiation of options and/or contracts related to the purchase of the built asset, including obligations arising from planning applications or consents; and
(e) negotiations with existing occupiers of the site or built asset and with the owners and/or occupiers of neighbouring sites or built assets.

While pre-implementation has similar issues to conception (that is, the need to protect commercially sensitive information), if the business plans involve significant changes to staffing levels or relocation there may be an increased risk of an insider threat. This may arise from a disaffected employee or contractor wishing to undermine the business planning through unauthorized disclosure of sensitive information.

As this phase includes the development of the project brief, there will be a need to address the cyber security of any professional advisers involved. This is necessary to ensure adequate protection of:

(a) commercially sensitive data; and
(b) any sensitive data about an existing operational facility, where harm or loss could occur following unauthorized disclosure.

An example of the latter could include information relating to security features in an existing built asset, the location on site/floor plans of sensitive processes or the storage of hazardous materials, or the location of storage for valuable and/or attractive items.

[10] See The Economist and SANS websites for information on industrial and corporate espionage respectively:
http://www.economist.com/blogs/democracyinamerica/2014/05/industrial-espionage
http://www.sans.org/reading-room/whitepapers/engineering/corporate-espionage-201-512

For projects involving acquisition of a built asset there may be a need to consider what is already in the public domain regarding the asset. For example, if acquiring a lease on a built asset, what information is available regarding the construction, configuration and operation of the built asset? In some cases, there may be detailed site/floor layouts published on the internet from previous marketing activity or planning applications. While this may not be an issue for some asset occupiers/users, others may have to consider whether the published information increases their security risks.

If the project relates to an existing built asset that already has a security strategy, then the security strategy should be reviewed and updated during this phase. Where the project relates to the commissioning of a new built asset or significant modification to one that does not have a security strategy, then an appropriate risk-based security strategy should be developed during this phase.

A security strategy may require interventions that are specific to lifecycle phases, but there will also be interventions that can be made during any phase. Examples of the latter include interventions made:

(a) in response to a breach;
(b) when a new threat or change to an existing threat has been identified; or
(c) to address emerging threats from advances in the use or deployment of a new technology.

Implementation of security countermeasures may occur at any point in the built asset's lifecycle; some will be an integral part of a construction-related project, others may arise on an ad-hoc basis either due to changes in response to new or evolving threats (for example, changes in criminal activity) or because of the need for additional protective measures following an incident.

4.3.3 Implementation

4.3.3.1 Design

As the acquisition or project moves into the implementation phase the number of professional advisers and contractors involved will increase and there will be greater collaborative exchange of data and information between the implementation team. With the increased digitalization through the use of BIM, digital collaboration (email, audio and video conferencing) and the deployment of CDEs for document sharing, there are more opportunities for inadvertent or inappropriate disclosure of sensitive data or information.

Through this digitalization, the project brief and related design information may be widely available within the advisory and implementation team. Additional security measures may be required to protect certain aspects of the design (for example, physical security features, location and routes of alarm/CCTV cables and location of sensitive facilities/operations) and to protect commercially sensitive information. Additional measures may also be required to protect the data and information from unauthorized changes. The project owner needs to consider what security measures should be required of professional advisers and suppliers who have access to the built asset data, and how implementation of these requirements will be verified and/or enforced. As part of the implementation process, the security policy for the built asset should be defined.

4.3.3.2 Delivery

As the implementation phase progresses from design to delivery activities, the security needs will focus increasingly on:

(a) protection of commercially sensitive information, including tender pricing information, as the implementation team expands and additional personnel and professional advisers join the team;
(b) minimizing the security risks to any data, information, systems or infrastructure in an existing built asset that are either used as part of the existing design or are newly installed during implementation of the new design; and
(c) to prevent damage or unplanned disruption to existing systems and infrastructure.

The protection of commercially sensitive information is a continuation of the processes and practices involved from the earlier phases but must take into account the churn of personnel and advisers that join and leave the team throughout this phase. Minimizing the security risks to the built asset requires careful planning to avoid compromising or damaging existing systems or exposing new systems to a wide range of threats. The measures required will be determined by the detailed threat and vulnerability analysis undertaken as part of the security risk management process.

During implementation there may be a number of transient risks associated with the construction activities that may affect the availability or integrity of systems, for example, the risk of a digger damaging buried power or communications cables. It is important to recognize that security is not just about preventing unauthorized access to tangible or intangible assets, but also about reducing threat and preventing harm.

4.3.4 Operation

This phase should be regarded as the steady state or normal operating state for a site or built asset. However, that does not mean that the security requirements are likely to be static. The protection of commercially sensitive information and systems will be part of the 'business-as-usual' function of operational departments and the organization's security and IT teams. From the perspective of the built asset and its systems, this phase requires vigilance to ensure that security measures in place are not compromised through ignorance, lack of maintenance, poor processes or lack of configuration and change control.

Security risks should be frequently reviewed to assess and, where necessary, address new or emerging vulnerabilities and changing threats, both internally and externally. Built asset owners/occupiers/users should monitor developments, assess the risk and update policies, processes and procedures where necessary or appropriate. There is also a need to implement security metrics to allow assessment of the effectiveness of existing procedures and countermeasures.

4.3.5 Operational change

Given the relative longevity of the operational phase of most built assets, it is inevitable that over the asset's lifecycle there will be a number of operational changes. These may range from relatively minor physical changes (for example, refits or refurbishment) to significant technology refreshes and reconfiguration of the built asset. A consequence of these changes is that they introduce the security issues outlined in Section 4.3.1, Section 4.3.2 and Section 4.3.3 into the relatively stable operational environment. This can increase the risk to the built asset and its operational use. Where the changes require part of the built asset to be vacated to permit construction works, the vacation of the area should be treated as a temporary disposal and the measures and security issues outlined in Section 4.3.6 should be addressed as part of the change project.

4.3.6 Disposal

During the disposal phase of a built asset, or part of it, there is potential for mistakes to be made, which could lead to serious security incidents. Before a site or built asset, or a part of a site or built asset, is disposed of, there is a need for decommissioning activities to ensure that security is maintained. The nature and scale of decommissioning will vary depending on the nature and use of the built asset, but may include:

(a) removal and secure storage or disposal of any special security equipment, for example, security cabinets, safes and cryptographic systems;
(b) removal and secure storage or disposal of any systems used to process or store personally identifiable or commercially sensitive data;

(c) removal and secure storage or disposal of all other IT equipment in the area;
(d) decommissioning of any public telecommunications network links or services;
(e) decommissioning of any network or communications links to other company or organizational sites;
(f) decommissioning of any network or communications links to the built asset management systems;
(g) removal and secure storage or disposal of all used media, paper records, etc., containing personally identifiable or commercially sensitive data;
(h) re-routing of sensitive communications and network cabling routes; and
(i) removal of signage showing the location of individuals or sensitive parts of the organization or system.

4.3.7 Examples of security-related deliverables across a built asset lifecycle

Table 4.1 lists examples of some of the security-related deliverables that may be produced across a built asset lifecycle. The precise nature of the deliverables will depend on the built asset, its use and the operational environment in which it is situated. For example, in the UK, if the built asset is classed as a crowded place there is guidance[11] on security measures to be implemented to increase protection from a terrorist attack. This includes guidance on the production of specific risk assessments, business continuity and evacuation/invacuation/lockdown plans, and the cyber security of venues.

Table 4.1 Examples of security-related deliverables across a built asset lifecycle

Stage	Examples of deliverables
Conception	Security considerations assessment, including threat, vulnerability and risk assessment (TVRA) Due diligence, including security triage process for existing and/or planned built assets and their use
Pre-implementation	Development of security concepts and governance arrangements Development and implementation of security policies and procedures for design and implementation phases Preparation of built asset security strategy covering physical, personnel and cyber security Preparation of information management and governance strategy, including information security requirements Specification of built asset security requirements
Implementation	Development of outline security design Development and implementation of security policies and procedures Development of full technical design, including security measures Implementation of built asset security measures Verification and validation that implemented security measures fulfil the security requirements
Operation	Implementation of built asset security measures Verification and validation that implemented security measures fulfil the security requirements Operation and maintenance of security measures in accordance with security strategy Review and where necessary the revision of security strategy, policies and procedures
Disposal	Security considerations assessment, including TVRA Due diligence including security triage process regarding existing and/or planned built assets and their use Specification of built asset security requirements related to disposal Implementation of specified security measures

[11] National Counter Terrorism Security Office *Crowded places guidance* https://www.gov.uk/government/publications/crowded-places-guidance

Section 5

Applying cyber security through the lifecycle of a built asset

5.1 Introduction

As illustrated in Section 4.1, built assets have complex lifecycles and typically undergo a number of change and technology refresh cycles. The use of the built asset may also change significantly over its lifecycle, as may the potential vulnerabilities and the threat landscape. Rapid changes in technology or business requirements can lead to changes to built asset systems and operations that were not, or could not have been, foreseen at the time it was designed, last refurbished or refitted.

An example of an operational change that introduces a new cyber security risk would be if a new facilities management contractor were to propose significant cost savings by implementing remote monitoring of built asset systems, plant and machinery. The potential presence of such remote connectivity may not have been considered during the original design of these systems, and appropriate countermeasures may not have been implemented to prevent or limit damage from attacks mounted via this remote connectivity.

Cyber security impinges on both new built assets that are still at a pre-implementation or implementation stage and existing built assets that are being acquired or changed. This Section considers the potential impact that poor cyber security can have on built assets and their stakeholders.

5.2 Who is accountable and responsible for the cyber security of built asset systems and data?

Accountability and responsibility for the cyber security of a built asset, its systems, associated business processes and the built asset data should be addressed in a cascading manner from the strategic accountability at senior management level to responsibility at the day-to-day operational activities level.

An example of accountability and responsibility is:

(a) strategic level:
   i. the senior management of the built asset owner is accountable for ensuring there is a cyber security strategy and supporting security policies covering the built asset systems and built asset data;
   ii. the built asset owner is responsible for ensuring that contracts relating to the construction, operation and maintenance of the built asset include security requirements that support the implementation of the security policies;
   iii. the senior management of the built asset occupier(s)/user(s) is accountable for ensuring that its personnel adhere to the built asset's security policies; and
   iv. the built asset occupier(s)/user(s) is responsible for including appropriate measures in their own security policies to fulfil their obligations to the asset owner.

(b) operational level:
   i. operational managers, in the asset owner and occupier/user organizations are responsible for ensuring appropriate and proportionate processes and procedures are in place to implement the built asset security policies; and
   ii. operational managers, in the asset owner and occupier/user organizations are accountable for ensuring that their personnel, including contractors, etc. adhere to the processes and procedures.

5.3 What built asset systems and information assets need to be protected?

The need to protect any of the types of asset or item listed below should be determined on a case-by-case basis. The built asset owner and relevant stakeholders should consider what value they place on an asset and its associated benefits to determine the potential impact of specific cyber security risks.

Depending on the built asset, its use and its stakeholder needs, the following types of asset or item may need to be protected:

(a) information assets (information or data) related to:
  i. an owner's or investor's business plans or strategy for a site or built asset;
  ii. the design and technical operation of the built asset;
  iii. contractual data regarding the design, construction and operation of the built asset and any changes to the built asset;
  iv. the use of the built asset and business operations within it; and
  v. personally identifiable information (PII) about built asset occupants or users.

(b) systems, in order to:
  i. prevent unauthorized changes to, or use of control and operation of, technical systems, including:
    - HVAC systems;
    - built asset management systems;
    - AACS;
    - CCTV and alarm systems; and
    - IACS;

  ii. prevent loss of commercially or operationally sensitive information or data from built asset-related systems; and
  iii. prevent loss of information affecting an individual's privacy or security, for example, images from CCTV systems or PII held in systems;

(c) operational information related to the use of the built asset or its occupiers, for example, where sensitive operations are housed, or where valuable items or dangerous materials are stored.

An important consideration when assessing the need to protect information assets is the nature of the assets and their value to both legitimate users (for example, the asset owner, operator or users) and to hostile or malicious actors. Unauthorized disclosure or use of the different classes of information asset may have significantly different consequences, both economically and reputationally for the legitimate users. Where an organization is making information assets public, it should be mindful of the need for security-minded communications[12] by reinforcing positive security messaging and avoiding disclosure of information that could aid hostile reconnaissance or enable highly targeted phishing campaigns.

5.4 What could adversely affect the built asset systems and data?

The increasing reliance of organizations on information and communications technologies means that interference with, or the failure of, electronic and computer-based systems can have a serious impact. In IT systems the primary security goal may be to protect the confidentiality of information assets. In OT systems there is often a need to protect the systems from the information assets. This means

[12] CPNI *Security Minded Communications Guidance for Virtual Tours* https://www.cpni.gov.uk/system/files/documents/93/4f/Security%20Minded%20Comms-%20Virtual%20Tours%20Guidance%20V3.pdf

preventing the delay, deletion or modification of data relating to the real-time operation of the physical components (for example, sensor reading and actuators settings) and preventing modification of master data (for example, configuration settings, set points and conversion tables).

The cyber security attributes outlined in Section 2.2.3 relate to things that can go wrong and that could adversely affect the built asset. The level of protection required will generally be determined by the potential impact on built asset owners and stakeholders, compared with the cost of implementing appropriate countermeasures. Examples of incidents that could affect these attributes include:

(a) confidentiality – the unauthorized disclosure of detailed business plans related to the acquisition and redevelopment of a site by a disgruntled employee has a substantial impact on commercial negotiations regarding its acquisition and use. It also has an impact on the disclosure of built asset/built asset system layouts or configuration, which could aid hostile reconnaissance.

(b) possession or control – the infection with encryption malware of computers used by a design team could result in critical design information being held to ransom: it is still in the possession of the team but they have lost control of it and cannot use it. The same situation could occur in an operational built asset with a ransomware infection of the BMS, resulting in loss of control of the built asset system.

(c) integrity – the control of lighting and ventilation in individual conference rooms is managed using wireless controllers. Their operation becomes intermittent and, on investigation, there is an electromagnetic interference problem caused by a local radio frequency (RF) source interfering with, and degrading, the control signals.

(d) authenticity – a purchase of heavily discounted software, which turns out to be counterfeit with malware included on the source disks, is installed on the users' organization or built asset networks and has spread to a number of clients/asset users, causing both reputational and financial damage.

(e) availability – the use of cloud-based energy management services is badly disrupted due to a denial-of-service attack on the cloud service provider, leading to energy savings losses and intermittent power outages;

(f) utility – file and data conversion process for the transfer of access control permissions results in corruption of critical data during installation and commissioning of a new site-wide access control system. The data has to be manually recreated and entered into new system disruption site operations, incurring significant extra costs.

(g) safety – hacking of remote support connection on fire alarm systems results in fire alarms being set off on three consecutive days, with a response by the fire and rescue service on each occasion. The fire certificate is withdrawn by fire authorities rendering the built asset unusable on safety grounds until the fire alarm system is modified to prevent reoccurrence of the security breaches.

The above examples illustrate that cyber security is not just about addressing the potential threats from malicious threat agents, such as hackers. Threats can emanate from defects in system or process design, or from human negligence or error.

5.5 Where are the built asset systems and data located?

The physical location of systems is a significant factor in the exposure of the systems, their components and infrastructure to a variety of threats. For example, unauthorized physical access to a workstation can allow the system to be compromised through use, intentional or otherwise, of malware infected removable storage media (for example, USB storage devices, SD cards and optical disks). The location can also determine the susceptibility of system components to physical damage or interference by accident or design or by natural causes. Depending on the nature of the built asset and the planned operation and maintenance arrangements for the systems, it may be appropriate to consider physically co-locating the processing elements of these systems with other central IT systems in the built asset, for example in computer rooms or network and telecommunications rooms.

The systems used to create, process, manage, store or display the built asset data may be located:

(a) within the built asset or site;
(b) in other accommodation used by the owner, operator or occupier; or
(c) with a third-party service provider, for example, the facilities manager or cloud service provider.

By understanding the location of a system's components and their criticality to the correct and continuing operation of the system, the risks can be assessed and appropriate controls or countermeasures adopted. Given the longevity of built assets, the limited lifetime of digital systems is also a significant risk. For example, commercial operating systems are generally only supported for 10 years or less. This means that, over time and as a consequence of software application updates or obsolescence, it may become increasingly difficult to access built asset data.

Identification of the location of the built asset systems enables protection of the built asset data that is generated, stored and processed on these systems, but that will not address all built asset data. For example, it is unlikely to cover some strategic information assets related to the design and operation of the built asset, or BIM-related information created as part of a design process, etc. Therefore, in addition to considering the location of systems, the location of built asset data throughout the built asset's lifecycle should be taken into account. This enables any risks to this information to be assessed and appropriate controls or countermeasures to be adopted.

The data used by the built asset systems or required for the design, operation and management of the built asset may be stored on-site in the built asset or in an adjacent built asset, or it may be held off-site:

(a) by the built asset owner, operator or occupier, or their advisers or representatives;
(b) by a built asset-related professional or supplier, for example, plans, detailed designs, configuration and maintenance information;
(c) by regulatory or statutory authorities, for example, planning applications and building regulations information;
(d) by suppliers or service providers; or
(e) by third parties, for archive, back-up or business continuity purposes.

The location of built asset data is likely to change throughout the asset's lifecycle. This should be addressed as part of the operational management of the data, which should include maintaining appropriate offline back-up to protect against corruption as a result of a cyber attack. The provision of a suitable environment for the management and security of the BIM-related information needs to be considered throughout the built asset lifecycle, which may be complicated by changes in built asset ownership, occupation and operation.

5.6 How should built asset systems and data be protected?

Our aim in managing cyber security is to retain control and coherence and enable trustworthy operation of the organization's and user's assets in the cyber environment. The measures required to achieve this fall into one of four categories:

1. physical – to protect the built asset systems and data from damage, theft or interference;
2. technical – the electromagnetic, physical and logical design and implementation to enable and achieve trustworthy operation of built asset systems;

3. procedural – the process and procedures relating to the use of built asset systems and data throughout their lifecycle; and
4. personnel – the background checks, vetting, training and education of individuals who will have access to, or use of, the built asset systems and data.

The choice of measures will depend on the built asset's cyber security context and the level of risk associated with perceived threats and vulnerabilities. In assessing the measures to be applied, consideration should be given as to the degree of alignment that may be practically achieved between those in place for enterprise systems and those applied to built asset systems.

Section 6

Managing technical aspects

6.1 Understanding the digital ecosystem within the built environment

The built environment is evolving into a digital ecosystem, where built assets are no longer standalone systems-of-systems, but increasingly linked to other systems. For example, the trend regarding integration of built asset systems with enterprise systems (for example, accounting, human resource and business operations management systems) to allow greater visibility to senior management of key performance indicators, such as asset operating costs, utilization or occupancy and energy consumption. The situation is further complicated where the asset owner and asset occupier or user are different organizations. Both may want access to combinations of the built asset data and/or information for their own management and corporate reporting purposes.

In addition to the enterprise-level connectivity, there is growth of smart asset-related services, which involve connection of built asset systems to external (third-party) systems (for example, remote monitoring and diagnostics or energy management purposes) and in some cases to obtain forecast environmental data (for example, wind speed, temperature, humidity and light levels). These predictions may be used to optimize a built asset's energy consumption while maintaining its operating environment within a desired range.

Historically, systems such as BMS – used to control the HVAC systems – and AACS were treated as effectively standalone systems with little or no external connectivity. They are now part of a built environment's digital ecosystem. Where asset owners occupy a portfolio of built assets, the individual BMS and AACS may be connected to a central monitoring and management hub, which in turn may be outsourced to a facilities management organization. This connectivity and integration, however, extends the attack surface that hostile threat actors may seek to exploit.

For infrastructure-related and linear built assets, the evolution typically relates to condition, capacity and utilization monitoring. For example, an increasing use of networked sensors to provide monitoring data, which are linked to analytic systems used to predict failures and schedule pro-active preventative maintenance. For these applications, the security considerations generally relate to the security goals of authenticity (understanding the source, provenance and limitations of the data), utility (particularly the long-term completeness, consistency and correctness of the data) and the possession/control (particularly information management and governance aspects).

6.2 Introduction and integration of new technologies

In parallel with the greater connectivity described above, there is a convergence of technologies. Historically, most built asset systems were constructed using specialist (industrial quality) components and sub-systems, such as the use of DIN-rail mounted assemblies. With the conception of the Industrial Internet of Things (IIoT), many industrial components are steadily being replaced by consumer and commercial grade IT components, for example, commercial rack-mounted computers rather than those housed in industrial cabinets. There is also a trend towards consumer grade sensors for use within built assets (where specific environmental protection or installation in hazardous environments is not required or anticipated). As a result of these developments, built assets systems may be physically more vulnerable to failure whether through attack, interference or environmental factors[13], regardless of source or intent. The case study below illustrates how a transition from industrial to commercial components can affect reliability and performance.

Case study: unintended consequences of cost engineering

As part of a refit programme, the environmental management of a plant room housing power generation equipment was being improved. Although there was an existing air extract fan in place the atmosphere was stuffy, and it was a hot working environment. At the built asset owner's request, design alterations were made involving the replacement of the extract fan with a new model. As part of the design process a cost engineering exercise was undertaken, which identified a significant saving through deployment of a replacement fan that met the required specification in terms of air handling performance, operating temperature range and fire safety, but unlike its predecessor it was contained in a plastic – rather than metal – housing.

In operation the new fan demonstrated an abnormal failure rate, with replacements required in a small fraction of the manufacturer's predicted operating life. The replacement activities were costly and disrupted the use of the built asset. After two replacements were complete, a detailed examination of a failed unit revealed significant damage to the fan's bearings.

What had not been taken into account in the product selection was the physical difference between the fans with plastic and metal housings. On paper both had comparable performance specifications in respect of air handling. The fans with a metal housing were intended for use in industrial environments and the housing was effectively a Faraday cage protecting the fan and its bearing from the electromagnetic environment created by the generating equipment. The plastic housing did not provide this protection and as a result eddy currents were induced in the fan's bearings, which led to their premature failure.

In addition to changes to the physical construction of devices and equipment, the software running within them is increasingly based on open-source and/or commonly available software libraries and is created and maintained using generic development platforms and file repositories. For example, user interfaces previously required extensive software development to create bespoke screen layouts, whereas use of embedded web servers enables rapid development of custom user interfaces using standard frameworks and libraries. However, as evidenced by the Open Web Application Security Project (OWASP) list of common vulnerabilities[14], many web servers are – from a security perspective – poorly configured and vulnerable to a variety of attacks. The extensive use of these technologies also means that the operational systems have inherited general IT sector vulnerabilities that are common and often readily exploitable.

A further consequence of this technology commoditization is that, increasingly, these IIoT components exhibit short lifecycles similar to the consumer products on which their underlying technology is based. Therefore, when components fail it may be difficult to source original components, as they are no longer manufactured. If physical compatibility and functionality is to be maintained, there is a significant risk that replacements may be sourced from unreliable suppliers, for example, internet auction sites. It is essential that where second-hand or remanufactured components are to be used, appropriate due diligence is employed so that they are only sourced from trustworthy suppliers.

When faced with the need to provide cyber security protection for systems it is tempting to implement obvious countermeasures, such as installing firewalls and deploying anti-malware software. However, the indiscriminate deployment of countermeasures may not be the best use of scarce resources, finance or personnel and may create a false sense of security. It is considered good practice to start by fully understanding the risks faced by individual systems and the built asset as a whole. This can be achieved by following the risk management guidance outlined in Annex A. Once the impact of the risks, in isolation and combinations, is understood, pragmatic, appropriate and cost-effective decisions can be taken on the countermeasures that should be deployed.

[13] See new ETSI standard for consumer IoT security https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf and the proposed UK legislation that will initially define the minimal security requirements for consumer IoT products being sold in the UK https://www.gov.uk/government/collections/secure-by-design

[14] OWASP *Top 10 web application security risks* https://owasp.org/www-project-top-ten/

An important pre-cursor to the risk assessment process is the availability of information on the overall design of the systems, including all components, locations, system dependencies and the reliance of the built asset and its users on individual systems. The understanding of overall systems design should encompass the physical components, the software environment and the built asset data required or produced by the systems. The use of an appropriate enterprise architecture framework[15] can help to identify and document all relevant components. The enterprise architecture should encompass not only the technologies, but the human and process elements of the systems as well.

As part of the risk assessment process, the interfaces to, interconnections between, and integration of systems should be examined critically. These interfaces represent an attack surface that may be exploited by threat agents. The operational/business rationale for each interface should be documented along with any design assumption regarding their nature and performance, and the operation of the connected systems. A further consideration regarding connections from the built asset to remote monitor systems are planned changes in deployed technology, as telecommunications providers progressively withdraw analogue communications services and replace them with digital services to the premises. For example, the planned UK full fibre national programme[16] introduces new risk through the migration of legacy-wide area connections to internet protocol (IP)-oriented services, requiring local battery-back-up, and a wide-area network (WAN) router from a service provider which may be unprotected or insecure.

Once the enterprise architecture for the built asset system has been established and the risks assessment undertaken, steps can be taken to reduce cyber security risks and develop a secure architecture. This will encompass a variety of process, procedural and managerial countermeasures, in addition to the technical measures discussed in this Section.

6.3 Wireless technologies – implications for safety and security

Increasing use of wireless technologies is being made in infrastructure systems. This is driven in part by economic factors (for example, reducing or removing the costs and space associated with the installation of structured cabling systems to support elements of the built asset systems, such as sensors) and the flexibility the approach offers when reconfiguring the built asset. However, these benefits are not without risk, as use of wireless connectivity introduces specific vulnerabilities to the built assets systems, which can lead to increased safety and security risks. There is also the consideration of how frequently the batteries[17] in any wireless sensors may need replacing and this can be a significant operating (rather than capital) cost.

When considering whether to use wired or wireless connectivity, the following questions need to be considered:

(a) What is the impact of loss of connectivity?

This may occur through:

i. interference (for example, from RF noise generated by other equipment or systems in the vicinity, or from other legitimate devices that transmit in the same frequency range);

[15] Enterprise Architecture Center of Excellence (EACOE) *Enterprise framework* http://www.eacoe.org

[16] BT Openreach. Analogue line withdrawal. https://www.openreach.co.uk/cpportal/products/product-withdrawal/wlr-withdrawal

[17] **Note**: long-life lithium batteries may serve to reduce the total cost of ownership (TCO) by enabling certain low-power devices to operate maintenance-free for many years, but this depends on the design and operation of the sensors.

ii. jamming (the intentional disruption of the frequencies used by the connection, for example, global positioning system (GPS) jammers that also interfere with Wi-Fi signals); or

iii. blocking or shielding (the introduction of materials into the built asset that prevent or severely attenuate the signals from one or more devices, for example, the construction of a new concrete wall to replace a lightweight partition wall).

(b) What is the impact of insecure connectivity?

With wired connections, to access the traffic you generally need physical access to the cables or fibres, wireless connectivity removes this constraint allowing interception of the signals wherever the signal can be legibly received. This may occur through:

i. Implementing communications links with no encryption of the content. In this scenario, any party that can receive and process the communications will be able to read messages. This may allow a picture of the built asset's operational use or occupancy to be determined. For security-related systems, this could enable a malicious threat actor to determine whether the systems are detecting surreptitious attempts to access the asset or sensitive parts of it. Depending on the nature of the communication it could also result in loss of privacy, for example, if analysis of the content allows identification of the pattern-of-life of built asset users or occupiers.

ii. Implementing communications links with weak encryption of the content. This is not a serious deterrent to motivated hostile threat actors. Given the availability of open-source tools that allow the 'cracking' of weak security algorithms and protocols, this approach is little better than implementing the communications links without encryption.

(c) What is the impact of unauthenticated or unauthorized devices being added?

In a physically wired system, the connection of additional devices (such as a new device in a new location) requires detailed knowledge of the system to identify spare or unused connections, and avoid creating anomalies by disconnecting existing devices or disturbing their operation in a way that may lead to further investigation and detection of the additional device. In a wireless system, it may be much easier, as long as potential clashes of device identifiers can be resolved.

A related issue is the potential for unauthorized changes to be made to the location of wireless devices. The lack of communications cabling can allow devices to be moved/repositioned without the knowledge or approval of the system operator. This could significantly impact the integrity and operation of the built asset system. For example, relocating a temperature sensor could result in anomalous behaviour of the HVAC system as it attempts to reconcile temperature readings from several locations.

Having researched the potential impacts of the three questions above, consideration should be given to how they would affect:

(a) the security of the built asset, its users and/or occupiers;
(b) the safety of the users/occupiers/neighbours; and
(c) for infrastructure assets the safety of the environment, both built and natural.

A risk-based decision can then be made on the choice of wired versus wireless connectivity for the systems. This is not a one-off decision. Changes to the built asset and its environs may require reconsideration of the use of wireless technologies if there is, or is likely to be, a significant change to the RF environment in and around the built asset.

Next generation built asset sensors may communicate with cloud hosted systems using public wireless infrastructure (for example, LoRaWAN, 4G and 5G) connectivity. The security considerations of reliance on public wireless infrastructure needs to be considered as part of a holistic security strategy.

6.4 Security by design

Security by design, or security by default, takes a number of forms, but the underlying approach is one that builds-in risk thinking from the onset of the project. It is important to recognize that while a device may have been 'secured by design' at the time it was first installed, security threats evolve. Therefore, even though a built asset has been secured by design, there is no guarantee that the design is free from future vulnerabilities or risks.

From a physical perspective, Secured by Design[18] is the official UK police security initiative that works to improve the security of built assets and their immediate surroundings to provide safe places to live, work, shop and visit. Several design guides[19] have been produced, including guides relating to schools, hospitals and commercial built assets. Although the guide on commercial built assets aims to reduce crime in the commercial sector, its principles are relevant to the protection of built assets in all sectors and can discourage physical interventions by many threat actors. A failure to provide adequate physical security protection of a cyber asset, whether physical or intangible, will undermine the effectiveness of measures taken in the other security domains.

From a cyber security perspective, the National Cyber Security Centre (NCSC) recommends the following Secure by Default principles[20]:

(a) security should be built into products from the beginning, it cannot be added in later;
(b) security should be added to treat the root cause of a problem, not its symptoms;
(c) security is never a goal in and of itself, it is a process – and it must continue throughout the lifetime of the product;
(d) security should never compromise usability – products need to be secure enough, then maximize usability;
(e) security should not require extensive configuration to work, and should just work reliably where implemented;
(f) security should constantly evolve to meet and defeat the latest threats – new security features should take longer to defeat than they take to build;
(g) security through obscurity should be avoided; and
(h) security should not require specific technical understanding or non-obvious behaviour from the user.

The above principles can be applied in a wide variety of scenarios. It is not always obvious how to interpret them when considering systems, and systems-of-systems, where components may be secure as individual products, but vulnerable in specific configurations.

6.5 Privacy by Design

The concept of the Privacy by Design approach to systems engineering was initially developed and published[21] in 2009 by Ann Cavoukian, Information and Privacy Commissioner of Ontario. The approach is based on seven foundational principles:

1. proactive not reactive; preventive not remedial – anticipate and prevent privacy invasive events before they happen or privacy risks to materialize;

[18] Secured by Design https://www.securedbydesign.com/
[19] Secured by Design https://www.securedbydesign.com/guidance/design-guides
[20] NCSC *Secure by Default* https://www.ncsc.gov.uk/information/secure-default
[21] *Privacy by Design: The 7 Foundational Principles* https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

2. privacy as the default setting – ensure that personal data are automatically protected in any given system or business practice;
3. privacy embedded into design – privacy is integral to the system, both the architecture of systems and business practices;
4. full functionality (positive-sum, not zero-sum) – avoid the pretence of false dichotomies, such as privacy versus security (it is possible to have both);
5. end-to-end security (full lifecycle protection) – ensure the secure acquisition, processing, storage and (when no longer required) timely destruction of data;
6. visibility and transparency: keep it open – personal data is handled in accordance with stated promises and objectives, and subject to independent verification; and
7. respect for user privacy: keep it user-centric – system architects and operators keep the interests of the individual uppermost, employing strong privacy defaults, informed consent and user-friendly options.

From the perspective of the built environment and individual built assets, these principles should be applied to any built asset system that acquires, processes or stores personal data, as determined by the data protection and privacy legislation applicable to the jurisdiction in which the assets are located.

A key measure that can be applied in designing and operating these systems is to seek to achieve data minimization. For example, for a built asset system used to determine desk occupancy and aid hot-desk users to find an available desk, the system and associated business processes could be designed to avoid processing the name and other identifying data for a user. It would rely instead on pseudonymized one-time tokens that are not linked to individual usernames or identities.

6.6 Carbon net zero/low-carbon by design

In addition to privacy by design, the 'green' economy requires assessments of procurement and design that will go beyond compliance with standards and attract investment and occupancy. The green economy links to branding of companies and the appetite for structures and operations that reflect the values of investing in the green economy. Principles for cyber security in the green economy will influence choices in design. Three guiding principles are:

1. the comparative energy consumption tally for cyber security products and the operational energy cost of provision of security directly through the built environment;
2. the design of computer support systems, including heating and cooling using renewables; and
3. the cyber security supply chain interdependencies on energy and sourcing of materials.

6.7 Resilience of built asset systems

Resilience is the ability to rapidly adapt and respond to disruptions, while maintaining continuity of business operations. From a business perspective, resilience is generally about preparing for any potential threat to the delivery of a smooth, steady and reliable service to maintain the delivery of critical services. From a systems perspective, resilience is about:

(a) having fault tolerant systems, infrastructure and supporting processes that allow the built asset to continue to operate with minimum disruption in the event of the failure of a significant impairment of critical systems; and

(b) being able to recover in a timely and efficient manner from failure or serious impairment of critical business systems so that an acceptable level of functionality can be restored, and the built asset can continue to be used.

To achieve this, the potential causes of disruption, both manmade and by natural causes, will have been considered as part of the cyber security risk management process described in Annex A. Appropriate steps should have been taken as a result of this analysis to ensure that key systems and their associated processes are maintained to deliver business continuity and that, where necessary, back-up systems and disaster recovery processes are available and rehearsed to enable timely detection and response to disruptive events.

While the concepts of business continuity and disaster recovery are reasonably well understood by organizations in respect of their corporate IT systems and their business processes, the complexity of the systems and their dependencies may not be well understood by the organization's business continuity planners. For business continuity purposes, organizations that are heavily dependent on IT systems employ a range of provisions, including alternate/disaster recovery premises, such as off-site back-ups of business-critical data and diverse network and communication routes. These provisions will typically form part of an organization's disaster recovery, incident response and business continuity plans. The nature of these plans and the specific measures required will be determined by the nature of the business, regulatory and legal requirements, and a business impact analysis.

The resilience of systems, whether they are IT or built asset systems (for example, HVAC) is generally measured in terms of redundancy, of systems and sub-systems, and their availability under both fault and maintenance conditions. Table 6.1 details a classification mechanism used for data centres and industrial plants. A built asset or plant classified as Tier 1 will have minimal resilience, with single points of failure in critical systems, and is likely to be used by organizations that can tolerate some loss of operation in their IT or built asset systems. A built asset or plant classified as Tier 4, however, will have a high degree of fault tolerance and may be used by an organization that delivers critical national infrastructure services, or that supports regulated financial and banking organizations. A Tier 4 site should be able to accommodate varying levels of scheduled maintenance and systems failure without losing capacity.

Table 6.1 Tier classifications for site infrastructure performance[22]

Tier	Description	Performance
1	Basic infrastructure	Non-redundant capacity components and single non-redundant connection/ distribution paths
2	Redundant capacity components infrastructure	Redundant capacity components and single non-redundant connection/ distribution paths
3	Concurrently maintainable infrastructure	Redundant capacity components and multiple distribution paths
4	Fault tolerant infrastructure	Fault tolerant architecture with redundant capacity systems and multiple distribution paths

How resilient a built asset's systems need to be would generally be determined by its operational use. For example, data centres and acute health care facilities will have requirements for the continuity of critical built asset services, whereas a retail outlet or warehouse may only require the provision of emergency lighting to allow safe evacuation of the premises. In these examples there may be varying levels of resilience within a built asset, for example, the computer halls and plant rooms may have resilient power supplies, whereas the power load in ancillary office or storage accommodation may be shed in the event of the loss of incoming site power. The analysis of systems' criticality and dependencies can be used to determine which business systems need to achieve specific levels of resilience.

[22] Adapted from Pitt Turner W, Seader JH, Renaud V, Brill KG. *Tier classifications define site infrastructure performance* Santa Fe, NM: The Uptime Institute, 2008.

Case study: failure of back-up power supplies

An incident occurred at British Airways' Boadicea House data centre on 27 May 2017 that caused the airline's IT systems to fail. The data centre is alleged to have been non-operational for approximately 15 minutes and any failover systems did not operate. The resulting business impact over 3 days involved tens of thousands of passengers being stranded overseas, misdirected luggage and hundreds of grounded aircraft. The cause of the failure is attributed to a malfunction of the datacentre's UPS leading, initially, to a loss of power to critical systems, followed by an unplanned/uncontrolled restoration of power resulting in system damage. This illustrates how, even if an organization has dual data centres (live and hot failover), on-site generators and UPS, failures can still occur.

This issue was further illustrated in August 2019 during a power outage of part of the UK National Grid, where some site generators did not automatically start and UPS systems failed to respond to the loss of incoming site power. From a built environment and built asset perspective, there is a need to design built asset systems to accommodate unexpected failures of off-site utilities. The recent catastrophic fire in an OVHcloud data centre in Strasbourg illustrates why built asset owners and operators need to consider the resilience of built asset systems in terms of both on-site failures and off-site dependencies (for example, utilities and cloud-based services).

6.8 Systems engineering, architecture and interface strategy

While it is common practice to refer to built asset (or building) systems, in practice such systems are generally systems-of-systems that form the system-of-interest and comprise a portfolio of interconnected and interacting systems and system elements that collectively deliver the built asset's operational environment. In addition to the operational systems there may be a number of enabling systems that are part of the system-of-interest's lifecycle, training system, maintenance system, etc.

Just as the built asset has a lifecycle, so do the systems and system elements. A common abstract functional model for a system lifecycle can be represented[23] as the conception of a need for the system, its realization, utilization, evolution and disposal. During the conception and realization lifecycle stages the systems engineering process should evolve a system architecture from functional needs through to the instantiation and handover to operations of a technical solution. A component of this process should be systems security engineering[24], that is, the application of engineering practice to provide a fully integrated, system-level perspective of system security.

Systems security engineering aims to deliver asset-based protection, which is not limited to prevention of events but also considers a spectrum of mitigation, response and recovery options. In adopting this approach, rather than focussing on likely events, the objective is to address what can happen and mitigate the consequences. This can be done by adopting a proactive and reactive strategy in the form of a concept of secure function that addresses the spectrum of potential asset loss and associated outcomes. When analyzing potential cause of losses, the scope should include all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions. By addressing the broad range of disruptions, hazards and threats, the systems architects and security engineers increase the likelihood that a cyber secure and cyber resilient system-of-interest can be delivered.

During the system design and realization, a zone and conduit model[25] should be developed for the built asset's system-of-interest. This model will be used to describe the logical groupings of systems and systems elements within (and related to) the operation of the built asset. The systems and systems elements are grouped into entities (for example, enterprise systems/applications, facilities management, AACS, BACS and fire safety) that can be analyzed for the development of security policies and requirements.

[23] BS ISO/IEC/IEEE 15288:2015 *Systems and software engineering — System life cycle processes* Section 5.4, p14.
[24] National Institute of Standards and Technology (NIST) SP 800-160 Vol. 1 *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* Gaithersburg MD: NIST, 2018.
[25] IEC TS 62443-1-1:2009 *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

This type of model supports the assessment of common threats, vulnerabilities and opportunities. The model can be used to develop countermeasures needed to attain the level of security (target security level) that are required to protect the system elements grouped in zones. This grouping allows a security policy to be established for all elements that are members of a zone and from this appropriate protection can be determined, taking into account the activities and built asset functions performed in the zone. Aligning security zones with physical areas within a built asset or its environs is advantageous, particularly when taking account of security holistically.

Each zone should have a set of characteristics and security requirements that are defined during the system engineering process, and recorded as:

(a) zone security policies – a controlling document that describes the overall security goals and how to ensure the target security level is met; and
(b) zone access requirements and controls – articulating the access required for the zone to meet its business objectives, and how this access is to be controlled.

The conduits are security zones providing the connectivity and interface between the security zones, providing both the physical and logical protection of the data and information being communicated between the zones. They are in effect the interface between zones and may comprise several sub-conduits providing one-to-one connectivity or one-to-many connectivity. The interface strategy should be documented alongside the zone security policies, access requirements and controls.

Each conduit should have a set of characteristics and security requirements, that are defined during the system engineering process, and recorded as:

(a) conduit security policies – a controlling document that describes the overall security goals and how to ensure the target security level is met; and
(b) conduit interface strategy – articulating the physical and logical standards, and data models, supporting the interface(s) between the connected zones.

The conduit interface strategy is effectively an interface-control document that defines the physical, electrical and logical connections, for example, the use of specific wired or wireless technologies, protocols, encryption or privacy protection required. The data model is an important component in change management, allowing the impact of control and operational functions or processes to be analyzed. For example, during a retrofit of new wireless IoT sensors that are replacing hardwired conventional sensors, the security impact of changes in the transmission mode, data content and end-to-end protection can be assessed and, where necessary, new protection measures developed and deployed.

6.9 Network segmentation, segregation and separation

Use of a combination of network segmentation, segregation and separation is a highly effective strategy that enables an organization to limit the impact of a network intrusion, including the spread of malware (for example, ransomware such as Wannacry). Use of these techniques can make it significantly more difficult for an adversary to locate and access an organization's most sensitive data and/or information; and they also increase the likelihood of detecting malicious activity in a timely manner. Implementation of these techniques should be considered early in the design lifecycle and reviewed/updated as designs progress or changes to planned or actual designs/implementations are reviewed. The techniques, implemented with appropriate network monitoring enable detection of the early stages of lateral movement by an attacker or malware, and can reduce the potential for serious damage[26].

[26] NCSC *Preventing Lateral Movement* https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

Commentary

WannaCry is an example of ransomware, a type of malicious software (malware) used by cyber criminals to extort money. Wannacry targets computers using Microsoft Windows with an unpatched security vulnerability. Designed to spread quickly among computers on the same network, it encrypts files using strong encryption, thus enabling perpetrators to demand ransom from users to then decrypt the files. On 12th May 2017, Wannacry caused significant disruption to a variety of organizations including severe disruption to parts of the UK NHS which led to cancellation of operations and appointments. The malware was reported to have spread to over 150 countries.

The concept of network segmentation involves partitioning a network into a set of smaller networks. For example, placing finance and human resource departments on separate segments from customer- or supplier-facing business operations. Network segregation involves developing and enforcing rules that are applied to control communications between specific network hosts and applications services.

In a built asset context significant benefits are derived from maintaining separation of an organization's IT networks from the OT networks in any built asset(s) they occupy or use. Where there is a need to transfer data between the IT and OT networks, an appropriate secure interface should be engineered and deployed. Guidance on security architectures for OT networks is provided by the IEC 62443 standards series *Industrial communication networks – IT security for networks and systems*, in particular IEC 62443-1-1:2009 *Terminology, concepts and models*.

6.10 Systems maintenance

Over the lifecycle of a built asset system it is inevitable that system components will require patching, replacing or upgrading so as to maintain the operation and security of the system.

While applying patches is a basic security principle, it is not always easy to do in practice, particularly for the complex cyber-physical systems. NCSC guidance on patching recommends the development of a patching plan that aims to reduce the overall business risk to acceptable levels [https://www.ncsc.gov.uk/blog-post/the-problems-with-patching].

Over time it is likely that various components of a system may become obsolete, i.e., original new components are no longer available. When procuring control system components the requirements and controls in BS EN IEC 62443-4-2:2019 *Security for industrial automation and control systems. Technical security requirements for IACS components* should be considered taking into account an appropriate security capability level for the component. These controls are intended to address the security practices of system integrators, component vendors and their respective supply chains. Simply buying from a 'trustworthy' vendor does not eliminate vulnerabilities. The vendors should be required to tell you when their products (hardware, software and firmware) are vulnerable and provide a patch.

From a maintainer's perspective it needs to be possible to apply the patch in the operational system and processes need to be in place to provide reports about which devices, products and systems are up to date. If for safety/availability/cost reasons, you decide not to install patches this should be documented and appear in the relevant risk registers (i.e., asset owner, asset user, etc).

If significant upgrades are planned for a system or to system components, the principles set out in Sections 6.1 to 6.9 should be applied.

Section 7

Managing process and procedure aspects

7.1 System operations

System operations encompass the strategic and tactical management of the system-of-interest to deliver the required built asset functionality and business outcomes. Appropriate and proportionate processes and procedures should be implemented to cover:

(a) systems administration, such as routine operational tasks, including managing system users, maintaining access controls and system back-ups;
(b) systems management, such as planning and managing changes to the system;
(c) system-related procurement and supply chain management; and
(d) system-related security operations, such as audits and security testing of systems, both on a routine and ad hoc basis (for example, following significant changes to the system-of-interest).

7.2 Systems and infrastructure documentation

A possible cause of resilience and cyber security failure is a lack of up-to-date documentation on built asset infrastructure (external and internal), systems design and configuration. Out of date or incomplete documentation can lead to operator errors, damage to underground assets and internal cabling or pipes, and the compromise of security and operational controls. An essential operational control for all built assets is the availability of up-to-date documentation for systems, covering hardware and software assets, interconnection and configuration information. An important part of the documentation is an accurate, up-to-date inventory of system elements (hardware, software, configuration and master data).

Use of BIM to develop an as-built repository of information about the built asset and its infrastructure may help to alleviate cyber security failure, but it does not address gaps in the documentation for many existing built assets. Additionally, it does not address the information management issues regarding the curating of built asset data to reflect operational and organizational changes to systems and post-handover changes to design or internal configuration of the built asset and its infrastructure. The capture and maintenance of this design, construction and operational information is an essential part of the 'golden thread' regarding the safety and security of built assets.

The process of updating built asset information with in-service changes needs to follow well-defined procedures that address the:

(a) governance of built asset information management;
(b) security measures relating to the authorization of individuals to access and make changes; and
(c) quality control measures to validate and verify the changes.

In addition to the need to maintain the built asset information, there is also a need to promote security-minded practices and to maintain effective information security regarding the built asset, built asset systems and infrastructure documentation. Guidance[27] is available regarding security measures that are applicable to the CDEs typically used to host the built asset data. Failure to ensure appropriate security will allow a potential threat agent to conduct hostile reconnaissance and therefore establish weaknesses or single points of failure in the built asset, its systems and the related infrastructure.

[27] CPNI *Common Data Environments - A guide for BIM Level 2* https://www.cpni.gov.uk/system/files/documents/8b/2b/20170309_Common_Data_Environments_A_Guide_for_BIM_Level_2.pdf

For business continuity purposes an up-to-date copy of essential safety and security documentation should be held securely at a location outside of the built asset. The CDE may fulfil this function providing it has a suitably high level of availability, with appropriate business continuity measures in place.

7.3 Built asset and systems maintenance

The way in which a built asset and its systems are maintained can have a profound effect on the overall security, including cyber security and protection of the built asset. Complex control systems require extensive maintenance across their lifecycle, including replacement of failed system elements (for example, sensors and actuators), installation of patches and minor configuration changes to maintain service quality or functionality. Depending on the built asset's threat profile there may be a need for detailed policies and procedures relating to the maintenance of critical built asset systems. For example, where changes are required to access control systems, an appropriate testing process should be implemented to ensure that system operation is not compromised.

Based on the risk assessments undertaken while preparing or updating the built asset's security policies, appropriate cyber security processes and procedures should be adopted for the maintenance of the built asset and its surroundings, its systems and infrastructure. If maintenance activities are being undertaken by third parties, appropriate security briefings should be provided, along with copies of relevant policies, processes and procedures. The built asset owner/occupier/user should also put mechanisms in place to ensure that the third parties adhere to these requirements.

For all but the simplest built assets, a systems maintenance strategy should be established that takes into account the decisions made regarding systems architecture, security engineering and interface strategies (see Section 6.8). The systems maintenance strategy should comprise a set of policies, procedures and actions designed to support, promote and implement the following maintenance objectives:

(a) to keep built asset systems' hardware in good working order;
(b) to keep built asset-related software, operating systems and system environments in good working order, with all security-related patches implemented;
(c) to assure that the status of the built asset-related systems meets existing organizational, industry, and other accepted best practice, as they relate to operational and security requirements; and
(d) to maintain up-to-date configuration information, settings and documentation for the built asset, its systems and any related infrastructure.

The strategy should address the three major categories of maintenance:

1. planned preventive maintenance (PPM) – tasks performed to correct or prevent degradation of performance, and to prevent minor issues or degradation from becoming a larger problem. This should include documentation updates and controls reflecting modifications to the built asset and its systems.
2. scheduled maintenance – performing ongoing, routine maintenance procedures at periodic scheduled intervals. The purpose behind scheduling routine maintenance tasks such as upgrades, patches, cleaning and installs is to provide a measure of predictability, and to move any expected downtime to off-peak hours.
3. corrective maintenance – maintenance of last resort, where a system or service is broken and must be repaired or replaced. Corrective maintenance can range from replacing failed components and assemblies to replacement of an entire system or service.

From a cyber security perspective there is a need to ensure that maintenance activities do not degrade the security of the built asset, its systems, infrastructure and data, both during the maintenance and on restoration of normal operations. For example, when IT or OT components are being replaced, care should be taken to ensure genuine components are being installed, that the provenance of the replacements is understood, and that the any digital configuration of the replacement (for example, software, firmware and master data) is authentic, correct and complete.

Case study: replacement of lift management server

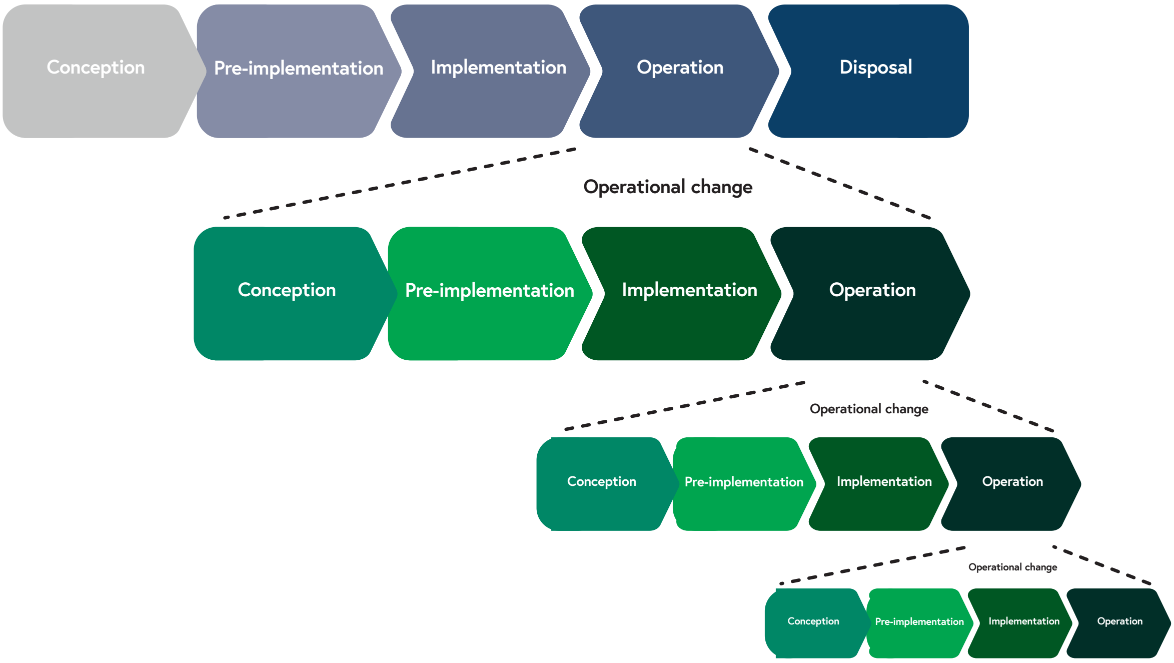
The lift system in an office building failed and a maintenance contractor identified the cause as a hardware failure of the lift management server. The server installed in the building was no longer manufactured so the contractor procured a replacement from an internet-based auction site. The contractor installed the replacement in the system and reconnected it to the building's AACS. The contractor was unaware that the replacement unit contained malware, which subsequently spread via the industry standard transmission control protocol (TCP)/IP connection between the lift system and AACS to other organization-wide systems. The malware infection was only detected when it spread onto the organization's network via its connection to the BMS.

The lesson learned from this case study is that failure to observe good cyber hygiene regarding replacement of built asset system components can result in significant disruption, potential losses and reputational harm.

7.4 Management of change

Over the operational lifecycle of the built asset, changes will inevitably be required affecting both the built asset and its systems. For example, Figure 7.1 shows that over the built asset lifecycle (shown in blue) there may be a number of operational changes (shown in green) affecting systems and the built assets infrastructure. In planning, designing and implementing changes, the impact on decisions and assumptions in the system-of-interest's architecture and interface strategy (see Section 6.8) should be reviewed and the impact of the change(s) assessed.

Figure 7.1 Operational changes over a built asset's lifecycle



This is where up-to-date documentation (see Section 7.2) is essential because the original security-engineered architecture and interfaces may have been subject to subsequent modifications that change the security profile of specific zones or conduits. Of particular importance is the interface strategy for the system-of-interest, particularly the:

(a) zone security policies;
(b) zone access requirements and controls;
(c) conduit security policies; and
(d) conduit interface strategies.

These documents will contain design assumptions and decisions that affect the security of system elements, individual systems or sub-systems, and the overall system-of-interest. Of particular note are those assumptions or decisions where there has been no mitigation of a known security vulnerability because the treatment was to isolate the vulnerable system elements from potential threat sources. For example, by not connecting or interconnecting specific system elements, systems or sub-systems. As described in the following case study, changes can have a significant impact on the security of the built asset.

Case study: security engineering assessment of a proposed change

A design assumption when the built asset was constructed was that equipment located in a local control zone within a plant room would employ dedicated, hard-wired connections with the interface to the supervisory computer located in the building control room. In addition, it was assumed that this building control room would be protected by a firewall that was designed for use in IACS. A proposal under consideration involves the retro-fitting of IIoT sensors on the equipment in the plant room. The proposed sensors would be wireless devices connected to a local wireless hub that relays the sensor data to a cloud-based energy monitoring service. These sensors will potentially open to the internet a system that was designed to be the closed.

A security engineering review needs to consider the following aspects:

(a) information management. Who needs access to this information, for what purpose and with whom may it be shared?
(b) information security. Is the information sensitive, would it reveal commercially or security sensitive information in isolation or when aggregated with other built asset data?
(c) cyber security. How does the introduction of wireless technology and a connection to the internet affect the security of the plant room and the systems in it? If it does, what additional countermeasures (physical, personnel, process or technical) may be required?

If, following an assessment, the proposed change is implemented the systems documentation, including the interface strategy, should be updated to reflect the impact on the systems architecture and operation. The system engineering solution will need to address what measures are necessary to prevent access to the control system from the internet.

7.5 Procurement and supply chain security

The business environment is a complex world, where an organization's supplier of goods, systems or services is increasingly reliant on a web of connected and interconnected companies spread across multiple jurisdictions. Few, if any, companies produce all of their own hardware or software and are solely responsible for service delivery. Companies increasingly buy in services and may hire contractors, consultants or agency personnel to provide specialist knowledge or skills. All of these external bought-in services are subject to threats across the four security domains, as are the suppliers themselves. Their security, or lack of it, can affect their technology, personal and physical assets, which in turn compromise your security.

The digitalization of the built environment exposes built assets to a wider range of threats as suppliers (and often their suppliers and the onward supply chain) obtain wide-ranging and long-term access to information about built assets, their owners, operators and users. This access is often largely unnoticed, unmonitored and may, over the duration of a contractual relationship, escalate significantly beyond any originally planned boundary.

Examples of this access may include:

(a) 'as a service' provision, such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), all of which may be storing or processing your sensitive corporate and built asset data and information;
(b) IT, OT and built asset maintenance contractors simultaneously working with multiple clients, some of whom may be competitors;
(c) service providers operating off-site call centres, helpdesks or security operations centre functions, both in the UK and offshore;
(d) vendors who supply and maintain built asset systems, employing remote monitoring and diagnostics to provide early warning and response to maintenance needs from a location outside of the built asset;
(e) third party recruitment consultancies, who hire staff on behalf of yourself, your clients and competitors and have access to sensitive personnel information.

In the above examples, poor security can put the built asset's and its stakeholders' security, resilience, compliance or stability at risk. Suppliers with a poor security culture may cause incidents, for example, by failing to manage their own security, irresponsible actions, unauthorized information disclosure and employing rogue staff who exploit their positions.

Due to the extensive use of contractors and consultants throughout the lifecycle of a built asset, there is an increased risk that the security policies become diluted or confused as obligations are passed down the supply chain. It is therefore important that the top-level contracts (Tier 1) make explicit provision for the cascading, ideally without modification, of a contract's security terms down the supply chain.

7.5.1 Supply chain security principles

CPNI and NCSC have jointly published[28] a set of 12 supply chain security principles, which are divided into four stages representing the process of securing the supply chain for a built asset:

1. understand the risks:
  (a) understand what needs to be protected and why;
  (b) know who your suppliers are and build an understanding of what their security looks like; and
  (c) understand the security risk posed by your supply chain;

> **Commentary**
>
> The asset owner and/or operator need clarity on where the legal responsibility for failure of supply chain will reside in relation to requirements under national and international laws. This should remove any obscurity or false understanding about the use of outsourced services to reduce the risk liability.

2. establish control:
  (a) communicate your view of security needs to your suppliers;
  (b) set and communicate minimum security requirements for your suppliers;
  (c) build security considerations into your contracting processes and require that your suppliers do the same;
  (d) meet your own security responsibilities as a supplier and consumer;
  (e) raise awareness of security within your supply chain; and
  (f) provide support for security incidents;
3. check your arrangements:
  (a) build assurance activities into your approach to managing your supply chain; and

[28] NCSC *Supply chain security guidance* https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

4. continuous improvement:
   - (a) encourage the continuous improvement of security within your supply chain; and
   - (b) build trust with suppliers.

7.5.2 Procurement of built assets, built asset systems and services

At the heart of effective supply chain risk management is good procurement practice throughout the lifecycle of selecting, contracting and the ongoing management of suppliers and service providers. The foundations are laid from the start of the procurement process (the identification and specification of the contract security requirements). This requires the client organization to consider what sensitive or valuable assets the supplier or service provider could have access to, or adversely affect, and how poor security on the supplier's behalf could damage the client's reputation. In essence, this is a security risk assessment of the proposed contract.

Having considered the risks, the client needs to add appropriate requirements into the procurement documentation and the contract. While the specific requirements will vary between situations, the following aspects that should be covered as a minimum are:

(a) physical security – control of access to sites, built assets, etc, protection of the client's assets (for example, data, information and physical goods/systems when in the care of the supplier) and any geographical limitations on where work on the contract may be undertaken (including processing and storage of data);
(b) personnel security – background checks, security clearances, requirements for security awareness and training;
(c) security processes – requesting access to sites, built assets and systems, and policies on publicity regarding the contractual relationship with the client and the work being undertaken; and
(d) technical security – such as the security certification of the supplier's operations and systems (ISO 27001, Cyber Essentials+) and the protection of the client's information in transit and at rest.

Table 7.1 provides an overview of a typical procurement process and details how a range of security-related activities align with the stages in the process. It is important to recognize that these activities are not finished when the contract is awarded, there are ongoing monitoring, auditing (see Section 7.7) and incident response (see Section 7.6) activities that will be required, as well as a periodic review of any significant changes to the contract term, scope or delivery.

Table 7.1 Security aspects through the procurement process

Procurement stage	Security-related aspects of procurement
Business requirement identified	Security risk assessment Identify security-related aspects of the procurement and level of sensitivity of any data and/or information involved Identify contractual security requirements (**Note**: depending on the nature of the requirement, the personnel security requirements outlined in Section 7.5.3 may be applicable to the supplier or service provider. Security-related aspects should be informed by and derived from a security risk assessment)
Statement of requirement (SOR) developed	Develop/define/refine security requirements across the four security domains Define information security requirements for procurement-related data/information
Requests for information and/or expressions of interest issued	For sensitive procurements, pre-engagement screening and use of a non-disclosure agreement(s) to protect client and/or built asset information

Table 7.1 Cont.

Procurement stage	Security-related aspects of procurement
Development of invitation to tender (ITT)	Ensure security is addressed covering functional, non-functional and contractual requirements Establish security evaluation criteria For sensitive data/information establish sharing arrangements for bidders (for example, a secure room for briefings and viewing material that is not issued as part of ITT and clarification questions
ITT issued	For sensitive procurements, pre-engagement screening and use of a non-disclosure agreement(s) to protect client and/or built asset information
Bid submissions received	Ensure appropriate security measures are in place to protect and control access to security and commercially sensitive information
Bid evaluation (against SOR)	Review compliance with security requirements Obtain and review any security-related clarifications
Due diligence/award approval	Ensure that responses to all mandatory security requirements are compliant in winning bid. If not, address shortcomings before contract award
Contract award	Ensure bidders comply with any security requirements regarding publicity Initiate any background checks, clearance requests
Supplier/service provider delivery	Implement contact security requirements throughout delivery Monitor compliance with security requirements Manage any security breaches Monitor any significant changes to supplier(s)/service providers that could affect security, for example, takeovers, joint ventures and corporate publicity
Completion/handover/contract exit	Ensure arrangements for secure destruction and/or return of sensitive materials is completed Where contract personnel had access to the built asset, its systems and any CDE, revoke access and where applicable obtain return of passes, security tokens, loaned equipment, etc.

To mitigate supply chain security risks, the top-level contracts, meaning those between the client (who may be the built asset owner/operator or in some situations the occupier/user/tenant) and principal suppliers (whether contractors, consultants, product/system suppliers or service providers), should explicitly address:

(a) the security controls required, both pre-engagement and on an ongoing basis, of the supplier and that they are cascaded and upheld throughout the entire contracting chain;
(b) who is responsible for any lapses of security and what actions or measures must be taken in the event of a lapse or breach;
(c) the right of the client to approve any subsequent choice of replacement supplier; and
(d) the right of the client to audit (see Section 7.7) the implementation of security standards and controls at any point in the contracting chain and, if issues are identified, to require them to be addressed by the relevant suppliers.

7.5.3 Managing consultants, contractors and agency staff

To manage the insider threat (see Section 8.2) posed by built asset or facilities-related contractors, consultants and agency personnel, organizations should implement the following measures as part of their contracting process:

(a) risk assessment – to identify and assess the insider risk arising from the use of contractors and agency personnel in specific roles or for specific duties;

(b) pre-engagement screening – to ensure that only trustworthy and competent contractors and agency personnel are engaged;
(c) communicating security requirements to contractors – this should address the required pre-engagement screening and personnel, physical and cyber security measures that will apply to the contract, any sub-contracts and to all contractor or agency personnel;
(d) embed ongoing personnel security into contracts and practice – ensure that contracts include appropriate measures and controls and establish the practices required to minimize opportunities for contractors and agency personnel to abuse the organization's assets, including built asset systems, associated processes and data once engaged;
(e) ensure that security requirements, procedures and any required pre-employment screening are cascaded throughout the entire contracting chain;
(f) ensure that there is contractual clarity about any responsibility for damage from security lapses or breaches, including the right to approve choice of sub-contractors and to require contract termination in the event of poor security performance; and
(g) establish and implement audit procedures – use periodic audits to encourage compliance with security policies, processes and procedures throughout the contracting chain.

It is important to recognize that the risk from contractors, consultants and agency staff is not confined to those who work in, or have regular physical access to, the built asset. It is becoming increasingly common for technical support to the built asset and its OT to be provided in part through remote connections by the service engineers and technicians. These largely invisible individuals may have considerable control over these systems and, due to the nature of their work, may be subject to minimal supervision by the organization's own personnel.

While the steps described above address the needs for the contracting process, the behaviour of these individuals needs to be addressed. There are a number of steps that should be taken:

(a) include a security briefing as part of the contract induction required for non-employees who work at the site/built asset, or who have access to the systems;
(b) include them in any regular awareness and security training;
(c) ensure that they are aware of any acceptable use policies and cyber security policies if they have access to the built asset's or the organization's systems;
(d) ensure that they understand any rules relating to the handling and, where necessary, the destruction of sensitive information;
(e) ensure that they understand site/built asset security procedures, including rules relating to the handling of removable media and personal IT equipment; and
(f) ensure that there are effective exit procedures to be applied when an individual ceases to work on the contract. These should include revoking access to the site/built asset, return of passes, keys, remote access tokens, equipment and contract-/built asset-specific clothing or personal protective equipment, removal of any built asset or organization data from any removable storage or personal IT equipment used during the contract, return of documents (physical or electronic) and removal of access to built asset systems (including any remote access).

7.5.4 Appointing and working with security consultants

Organizations commissioning built asset projects, and those owning, operating or using built assets will require security expertise that encompasses:

(a) security risk assessments;
(b) developing a security strategy;
(c) creating and maintaining a security plan;

(d) identifying and specifying security aspects regarding the project and built asset design; and
(e) providing assistance or guidance in the procurement, technical design and construction, and subsequent phases (operation and disposal).

Depending on in-house resource availability, knowledge and expertise, the security or project manager of any significant built asset venture may need to consider procuring the services of one or more specialist security consultants. CPNI has published guidance[29] on procuring the services of a specialist security consultant when undertaking a a built asset project.

In appointing a specialist security consultant, it is important to select and appoint those who demonstrate their sustained ability to apply their skills, knowledge and expertise in real-world situations. Both CPNI and NCSC advise appointing suitably qualified and experienced consultants. CPNI supports chartered security professionals (CSyP) and the Register of Security Engineers and Specialists' (RSES) members. NCSC[30] has a certified professional scheme in recognition of competence in information assurance and information security.

7.6 Incident response, investigation and management

Incidents happen: security incidents, including cyber incidents, are a daily occurrence, although many go unreported. There is a need to maintain situational awareness to enable risk management of emerging vulnerabilities and threats. This situational awareness should apply to the organization, the built asset, its systems, and their associated business processes, data and information.

The impact of incidents on both an organization and its reputation are often determined by the organization's preparedness, and its response to the unplanned event. The organization's business continuity plan and the built asset's cyber security policy should establish responsibility for developing and implementing an incident response infrastructure (for example, plans, defined roles, training, communications, and managerial oversight) that deals with failures of cyber security. The effectiveness of this infrastructure will determine the speed of the response following the discovery of an attack, and thereafter how effectively damage is contained, the attack terminated and normal operations restored. Incident planning and response should include considerations of the impact and potential mitigation that different types of incident may have on safety, security and resilience as they affect the built assets and its use. To the extent that is practically achievable, built asset systems should fail secure as well as fail safe.

Preparation is essential; when an incident occurs, it is too late develop new procedures, consider reporting and data collection, and worry about management responsibility, legal issues and the organization's communications strategy. A cyber attack can be as much of a business continuity issue as a major fire or flood, particularly if the incident causes a built asset to be harmed or makes it uninhabitable. Evidence from studies of cyber security breaches suggests that there is often a significant period, usually measured in months, between an attacker gaining access to a system and the attack being detected. To minimize impact, the organization needs to follow good practice, identify and contain the damage, remove the attacker(s) from the systems, and recover in a safe and secure fashion. In the event of a cyber attack on a built asset, or one of its systems, it is not just about the potential risk of exfiltration of sensitive data, it is also about restoring the trustworthiness of the systems. Consideration also needs to be given to the capture of any forensic data following a cyber security incident. This is a particular

[29] CPNI *Procuring the services of a specialist security consultant when undertaking a project relating to a built asset, Version 7* London: CPNI, 2020.
[30] NCSC *Certified Professional scheme* https://www.ncsc.gov.uk/information/about-certified-professional-scheme

issue with control systems, for example the built asset management systems, where the opportunity to collect evidence may be reduced due to a need to restore or maintain systems operations so that the built asset can continue to function.

Cyber security of built assets is not just about defending the built asset's systems from hackers and hacktivists, it is also about the continuity of operation of the systems in the face of adversity. This should include addressing the potential security and safety issues arising from natural events, for example, severe weather, earthquakes and solar storms. Some of these incidents will have a direct impact on the built asset itself, others may affect, for example, the continuity and availability of mains power as demonstrated by Hurricane Katrina and its impact on buildings in New York.

Key steps in preparing an effective incident response plan include:

(a) pre-planning for mitigation (including systems adjustment to compensate for loss of operational elements) will be different to traditional structures and should take account of:
   i. machine learning development to automate reporting and automated adjustments at the systems level and to provide new pathways for communications, operations and outputs of the organization;
   ii. understanding the level to which AI will assist with the recognition, diagnostics and rebalancing of the operations and making contingency plans for where the event may be outside the scope of the design risks; and
   iii. the dependencies of the systems on external interfaces and creating an automated dynamic assessment of changes in interface elements, which may have time delays through dependence on traditional crisis management procedures.

(b) creating written incident response procedures, which will include definition of personnel roles for handling incidents and define the phases of incident handling.

(c) assigning job titles and duties for handling built asset systems and related infrastructure incidents to specific individuals.

(d) defining which management personnel will support the incident handling process, identifying their key decision-making roles and their key contacts with the suppliers responsible for supporting the built asset, its systems and infrastructure.

(e) defining escalation procedures and identifying the circumstances under which regulatory and security or law enforcement bodies need to be notified.

(f) devising standards for the time required for facilities managers, built asset systems suppliers and support contractors to report anomalous events to the organization's incident handling team. The mechanisms to be used for this type of reporting should be clearly identified, as should the kind of information that must be included as part of the incident notification.

(g) creating and maintaining up-to-date information on third-party contacts that may be required to assist in the event of a cyber security incident. It may be prudent for hard copies of this information to be securely held by the built asset's security and facilities managers, so that it is still accessible even if the built asset systems are inoperable.

(h) publishing information for all personnel using the built asset, including employees, agency staff and contractors, about the arrangements for reporting anomalies and incidents affecting built asset systems to the organization's incident handling team. This information should be included in the new joiners' pack and provided to occupants/users as part of the routine security and business continuity awareness activities.

(i) conducting periodic incident management rehearsals, which include cyber security-related scenarios. These sessions should involve personnel and contractor representatives associated with the incident handling team. This will help them to understand current threats and risks, as well as ensuring their familiarity with their roles and responsibilities in supporting the incident handling team. The testing or rehearsals should include all pre-defined communications, command and control processes, and identify who should deal with the issue, who should manage the teams and who should manage stakeholders (for example, personnel, contractors, customers, press, security services and police/

law enforcement). For major organizations, the testing should also include a review of press releases and other pre-planned communications to verify that it is fit for purpose and conveys the right message should a cyber security event disrupt day-to-day operations.

To investigate security incidents, there may be a need for investigators to have access to items of personal IT equipment that have been brought into the built asset or connected to built asset systems. Provision should be made in employment and supplier contracts for digital forensic examination in the event of a cyber security breach.

Further guidance from the NCSC on this subject can be found online at: https://www.ncsc.gov.uk/collection/incident-management

7.7 Auditing for accountability

Evidence for insider incidents suggests that two common factors are poor management practices and the poor use of auditing functions. Given the important roles that personnel security has in both the overall security and the cyber security of an organization and built asset, there is a need for appropriate quality assurance measures to ensure compliance with policies. From a personnel security perspective this should cover:

(a) pre-employment screening of employees, agency staff and other temporary workers;
(b) pre-engagement screening of contractors and consultants;
(c) compliance with, and implementation of, ongoing security requirements, for example, the handling of disciplinary or other personnel-related actions following investigation of security breaches or incidents; and
(d) monitoring of security awareness training.

The right to audit must be specified in contractual documentation, which should also address any termination and compensatory arrangements in the event that an organization or individual is in breach of their security obligations. The specification should include the right to audit where international suppliers, operators or personnel are located abroad and include transparency of audit results or findings. Where local laws deny access for audit or prevent transparency, arrangements should be included whereby there is mediation or contractual arrangements that ensure control over audit remains with the asset owner.

The organization should have clear policy, processes and procedures for the handling of audits. The process should be transparent and, wherever practical, conducted by an independent party. The terms of reference and scope of any audits should be agreed in advance and, with the exception of situations where urgent action is required to investigate a security breach, reasonable notice should be given. Audits should address both the effectiveness of the process and procedures in use and adopt a sampling approach to ensure that processes have been completed to the required standard.

Section 8

Managing 'people'

8.1 Appointments, roles and responsibilities

Effective security protects the assets, people, reputation and profitability of an organization, but is dependent on good governance, which in turns requires clear accountability for security at board or executive level. There should be clear reporting lines for all personnel with security responsibilities, whether staff or specialists are employed in advisory roles. Just as safety is, or should be, a regular topic for senior management, security should similarly be subject to regular top management attention.

The board or executive-level manager responsible for security should monitor the effectiveness of security management across the organization, including the security relating to the built assets that it owns, operates or uses. As part of this role the individual should maintain awareness of threats that can affect the organization and its assets and regularly review the effectiveness of the measures in place to mitigate them.

There is published guidance on good security[31] and effective cyber security[32] that can inform the organization's security management and provide a basis for staff security awareness and role-based training.

8.2 The insider risk and factors contributing to insider attacks

8.2.1 What/who is an insider?

An insider is a person connected with the built asset's owner/occupier/user or supporting consultant, contractor or supplier. In essence, this is a person who has been granted some level of authorized or privileged access to the built asset, the built assets or built asset data and puts their privileged access to a use that is not intended or allowed.

8.2.2 The nature of insider risk

Insiders are a major source of risk and their actions may or may not be malicious. This Section considers some of the steps that can be taken to reduce the risk of a cyber security incident caused by an insider. Five main types of insider activity have been identified[33]:

1. unauthorized disclosure of sensitive information (either to a third party or to the media);
2. process corruption (defined as illegitimately altering an internal process or system to achieve a specific, non-authorized objective);
3. facilitation of third-party access to an organization's assets (including premises, information and people);
4. physical sabotage; and
5. electronic or IT sabotage.

[31] CPNI *Passport to Good Security, For Senior Executives* London: CPNI, 2015. https://www.cpni.gov.uk/system/files/documents/b0/69/CPNI_Passport_to_Good_Security.pdf
[32] NCSC *10 Steps to Cyber Security* London: NCSC, 2018. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security
[33] CPNI *CPNI Insider data collection study* London: CPNI, 2013. https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

Section 8 – Managing 'people'

As part of the built asset security risk analysis, the issue of insider risk can be considered by undertaking a role-based security risk assessment[34]. This assessment should be undertaken to identify 'high risk' roles, for example those roles with administrative privileges for built asset systems.

The most frequent types of insider activity identified by the CPNI Insider Data Collection Study were unauthorized disclosure of sensitive information (47 %) and process corruption (42 %). From a built environment perspective, examples of these activities could include:

(a) unauthorized disclosure of sensitive built asset plans relating to security measures, or PII regarding employees and visitors;
(b) corruption of access control and pass issuing processes to allow escalation of access privileges or to remove evidence of unauthorized access to sensitive areas;
(c) sabotage of built asset systems by physical or electronic means; and
(d) manipulation of other employees or contractors (such as deliberate attempts to acquire information or access by manipulating staff).

Almost all cyber attacks can be assisted or conducted by an insider, whether motivated by criminals, terrorists or competitors seeking a business advantage. This could be anyone with authorized access to the built asset, its systems, the associated process or built asset data, including employees or any contract or agency staff (for example, cleaners, caterers and security guards). An insider may already be working for the built asset owner/occupier/user or may have recently joined to infiltrate the organization specifically to exploit the access that the job or role might provide.

Case study: disclosure of sensitive building-related information[35]

In January 2008, a former agency worker was found guilty (along with five other members of a criminal network) for the £53 million robbery of the Securitas depot in Kent in 2006. The agency worker based at the depot was on a low wage, but worked in the cash-handling operation and had extensive access to a facility that dealt with hundreds of millions of pounds in cash. He was accused of providing information to the criminal network ahead of the raid, using a hidden camera to film the inside of the depot.

Case study: attempted sabotage of building infrastructure[36]

In August 1999, a former security guard who had worked at the stadium of Charlton Athletic Football Club was found guilty of a conspiracy to cause a public nuisance with regard to a plot to sabotage the floodlighting at the stadium during a Liverpool FC versus Charlton Athletic FC fixture. The scam was discovered when two individuals from Malaysia and a UK businessman were caught with a circuit-breaker at the stadium three days before the match. They had planned to plant the electrical device to sabotage the floodlighting. It was to be triggered by a remote-control unit when the score favoured a betting syndicate. The potential for huge profits meant they could promise a lowly paid security guard a significant bribe to allow them into the ground to plant the device.

In addition to the malicious insider threat there is always the risk of non-malicious insider actions. These threats typically arise from factors such as errors, omissions, ignorance or negligence. Social engineering attacks on an organization tend to rely on naive behaviour by insiders, who may fail to follow security processes and procedures. Examples of insider behaviour that can be exploited by cyber attackers include:

(a) compromising physical security measures by allowing tailgating into sensitive or restricted areas or leaving security doors and fire exits propped open;

[34] CPNI *Role Based Security Risk Assessment* London: CPNI, 2020. https://www.cpni.gov.uk/insider-risks/role-based-security-risk-assessment
[35] http://news.bbc.co.uk/1/hi/england/7214598.stm and http://news.bbc.co.uk/1/hi/uk/7154191.stm
[36] http://news.bbc.co.uk/1/hi/uk/426092.stm

(b) gratuitous disclosure of information about built asset systems on social media sites, for example, information about using specific systems on LinkedIn or posting pictures on Twitter or Instagram that aid hostile reconnaissance;
(c) disclosing account security information in response to a phishing or other social engineering attack; and
(d) careless use of email, which results in sensitive information being sent to incorrect addressees.

8.2.3 Factors contributing to insider attacks

There a clear link between insider acts taking place and the presence of exploitable weaknesses in an organization's protective security and management processes. The organizational-level factors include:

(a) poor management practices;
(b) poor use of security and systems auditing functions;
(c) lack of protective security controls;
(d) poor security culture;
(e) lack of adequate, role-based, personnel security risk assessment;
(f) poor pre-employment screening[37];
(g) poor communication between business areas;
(h) lack of security awareness of people risk at a senior level; and
(i) inadequate corporate governance.

8.3 Managing personnel security

To protect a built asset from insider-related cyber security threats, it is important to put in place an effective and holistic scheme to manage personnel security. An example of an effective framework is the Holistic Management of Employee Risk (HoMER) developed by CPNI[38]. This framework aims to reduce the risk of employees' behaviour damaging an organization. The term 'employee risk' is defined as counter-productive behaviour, whether inadvertent, negligent or malicious, that can cause harm to the organization.

The HoMER guidance leads an organization through the key stages of a people risk management lifecycle:

(a) vision and leadership – sound and engaged leadership, corporate governance and transparent policies in managing people risk and strengthening compliance;
(b) assess – adoption of a demonstrable risk-based approach and the implementation of reliable asset, access and identity management;
(c) protect – developing compliant policies and procedures for protective monitoring;
(d) respond – preparation in advance for handling employee incidents, including guidance on the best way to manage an incident to minimize damage and maintain stakeholder trust; and
(e) recover – effective steps for post-incident recovery, including a process for maximizing lessons learned to improve security.

The principles set out in the HoMER guidance can be used to reduce the personnel risk to the built asset if they are applied to the facilities management and IT teams responsible for the management of the built asset, its systems, associated processes and data. While the HoMER guidance was developed for use with employees, its principles could be applied to all contractor, sub-contractors and agency personnel who are normally working in the building and its surroundings.

[37] See BS 7858 *Security screening of individuals employed in a security environment - Code of practice*
[38] CPNI *Holistic management of employee risk (HoMER)* London: CPNI, 2012. https://www.cpni.gov.uk/system/files/documents/62/53/Holistic-Management-of-Employee-Risk-HoMER-Guidance.pdf

8.4 Awareness, training and education

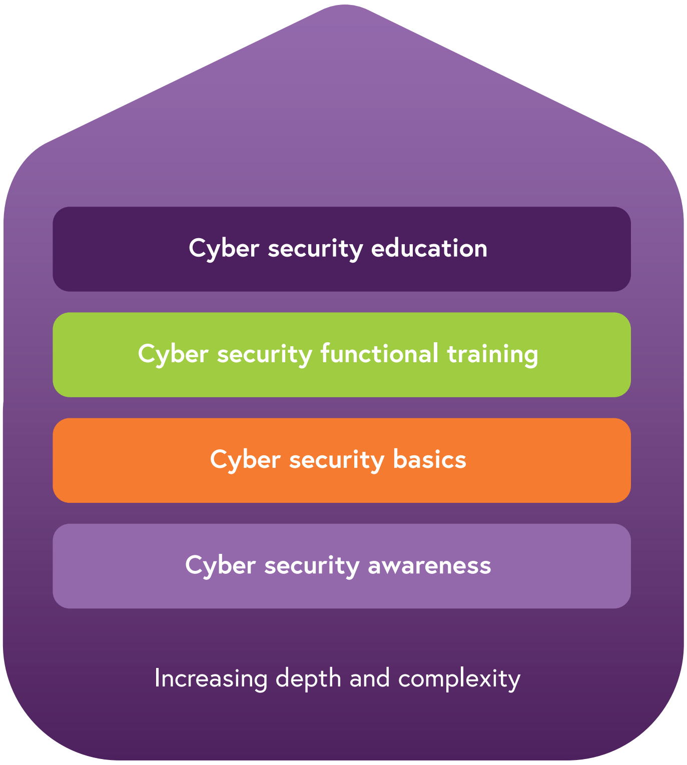
8.4.1 Developing a security culture

A successful and effective security programme for an organization and the built asset(s) it owns/operates/uses, or plans to, is an essential part of security governance and should be founded on a clear security strategy and its supporting policies. Section 9 describes the development and implementation of a security strategy and policies, and their subsequent monitoring and review. The strategy should include cyber security and information management provisions that reflects business needs, based on known risks to the built asset, its systems, associated processes and data.

Implementation of the security strategy may require changes to, or reinforcement of, existing practices or behaviours, as well as informing built asset occupiers/users and related contractors of their security responsibilities. Adopting and maintaining an appropriate security culture will require a range of security awareness, training and education. This should be an ongoing programme that responds to changes and learns from experience (such as addressing shortcomings identified during the investigation of security breaches and near-misses). Given the increased digitalization of the built environment, a core aspect of the security culture is cyber security, both in terms of the protection and use of digital systems, and the understanding of information management so that sensitive data and information is appropriately handled and protected.

Cyber security awareness, training and education are a progression or continuum as shown in Figure 8.1. The development of an awareness and training programme should be linked to a training needs analysis, which in turn will relate to the built asset's cyber security strategy, policies, processes and procedures. It may be possible to use and/or adapt awareness and training material available within the built asset owner/occupier/user organizations to provide suitable material that includes and addresses the built asset systems.

Figure 8.1 Cyber security progression through awareness, training and education



© The Institution of Engineering and Technology

8.4.2 Cyber security awareness

Awareness, shown at the lowest level in Figure 8.1, is not related to training. The objective of an awareness presentation is simply to focus attention on cyber security. Following an awareness presentation, individuals should be able to recognize cyber security concerns and act or behave appropriately.

Cyber security awareness design should flow top-down from the cyber security education that is designed to enact the policy and strategy. The top-down approach ensures that the elements of awareness can feed up to the top level and strengthen recognition of changes in patterns, despite awareness being uneducated in the broader elements of the cyber security strategy. This is important for resilience.

A significant number of topics could be covered in any awareness session. From a built asset cyber security perspective, topics may include:

(a) physical security – access control, visitor badges for parking and deliveries, bomb threats;
(b) password use and management - apply NCSC guidance on choice of passwords https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words and use of password managers https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers;
(c) protection from malware – scanning of removable media, updating definitions;
(d) internet and email use – allowed versus prohibited, monitoring of user activity;
(e) social engineering – phishing, spear phishing and handling of unwanted emails/attachments;
(f) incident response – who to contact and what to do;
(g) changes in system environment – increases in risks to systems and data (for example, water, fire, dust or dirt or physical access);
(h) inventory and property transfer – identifying responsible organization and user responsibilities (for example, media sanitization);
(i) handheld device security issues – addressing both physical and wireless security issues;
(j) access control issues – addressing least privilege and separation of duties;
(k) individual accountability – explain what this means in the organization;
(l) security minded communications – reducing the amount of sensitive or potentially sensitive information that leaks out of an organization through a variety of channels, including marketing and recruitment material; and
(m) duty to report changes in the environment, external technical interfaces or people that may be anomalous or 'unusual' for any reason. This can provide early warning of an impending security problem, discourage potential insiders and increase the risk to those conducting hostile reconnaissance.

Awareness presentations should be given as part of the site/built asset induction session for all personnel working in the facilities management and/or built asset management teams, and also their associated contractors and agency staff. Refresher training should be delivered periodically to update individuals on changes and reinforce their overall cyber security awareness.

The cyber security basics level shown in Figure 8.1 is effectively an extension of any material used in any awareness presentation or briefing. The basic level content will typically address a topic in slightly more detail and acts as a bridge to the formal security training. For example, the basic training on passwords might provide more detailed advice on how to create passwords that conform to the organization's policy and/or the use of two-factor authentication for protection of more sensitive systems, or as part of a remote access cyber security regime.

8.4.3 Cyber security training

Cyber security training strives to produce relevant and needed security skills and competencies that will be used by functional practitioners outside of the cyber security area. For example, operations and maintenance personnel being taught specific systems administration skills. Aside from the depth of coverage of a topic, the principal difference between awareness and training is that the latter is intended to teach specific skills that are required for an individual's job role, whereas awareness focuses an individual's attention on a specific issue or set of issues. Training courses may be delivered at various levels, for example, basic, intermediate and advanced.

Training needs will vary between built assets, but might typically include:

(a) systems administration for built asset-related systems;
(b) development of cyber security policies, processes and procedures;
(c) risk assessment and management;
(d) maintenance and configuration of physical and cyber security systems;
(e) personnel security;
(f) business continuity and contingency planning; and
(g) incident management and investigation.

Training will generally not lead to any formal qualifications, but may provide credits towards, or some exemptions from, a formal educational course or can be used in support of an individual's continuing professional development.

8.4.4 Cyber security education

Cyber security education aims to integrate all of the security skills and competencies of the various functional specialties into a common body of knowledge to produce cyber security specialists and professionals with the knowledge and understanding to provide a proactive response to new situations. A cyber security education programme will generally be offered by a university or college and may result in the award of a certificate or degree, depending on the nature of the course. A key difference between training and education is that the latter should provide the student with an understanding of the underpinning knowledge and principles behind the techniques they are taught as part of a training course.

Section 9

Applying this Code of Practice

When considering how to apply this Code of Practice to a built asset, the comprehensive definition of cyber security published by the International Telecommunications Union (ITU)[39] provides an indication of the potential breadth of activities required:

> *Cybersecurity 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 organization and user's assets.*

For the purposes of this Code of Practice, the organization's assets and user's assets include the built asset and environment as well as the broad range of IT and OT systems that form part of the built asset and its operational ecosystem. The term 'security' has been used throughout this document to highlight the need to address physical and personnel security issues as they impinge on the cyber environment, and process security to prevent or deter subversion of business processes that affect the security and cyber security of built assets.

9.1 Security governance

The starting point for achieving effective cyber security in the built environment is to establish the security governance and leadership in respect of a built asset and for the responsible and accountable individual to adopt a security-minded approach. Security responsibility for a built asset and its built asset systems will depend on the relationship between a built asset owner and the occupiers or users of the built asset – and whether these are different or related legal entities. For some occupiers or users, their security needs may be higher and therefore take precedence over the needs of the asset owner. For example, a high-profile tenant or one who will attract the attention of specific threat agents may require deployment of specific countermeasures. Whatever the specific situation for a built asset, one of the parties needs to be the lead organization, and the security governance should flow from this lead organization.

Good governance starts by identifying who is accountable for security at board or executive level, where applicable in a lead organization, and ensuring that they have clear reporting lines to all staff with security responsibilities. This accountable individual should establish appropriate and proportionate monitoring of the effectiveness of security management as it affects the built assets and its systems. If a built asset is not owner occupied, the lead organization will be required to establish enforceable agreements with the other organizations involved.

The accountable individual should establish a security strategy for the built asset and ensure that it is reviewed and updated at regular intervals. As part of the review an update process they should seek regular briefings on the threats to the built asset and the organizations involved.

Note: Clause 5 of BS EN ISO 19650-5 provides a specification for initiating a security-minded approach for built assets. For linear built assets and those involving sensor networks, additional security guidance is available in PAS 7040:2019 *Digital manufacturing. Trustworthiness and precision of networked sensors.*

An important part of the leadership role is establishing a strong security culture. This may include a mixture of hard and soft measures, for example:

[39] International Telecommunication Union (ITU) *Clause 3.2.5 – Series X: Data networks, open system communications and security: Overview of cybersecurity* Geneva: ITU, 2008. https://www.itu.int/rec/T-REC-X.1205-200804-I

(a) leading by example;
(b) promoting clear and fit-for-purpose security policies that are supported by appropriate training, awareness and communication;
(c) establishing robust procedures for dealing with poor security behaviour;
(d) visibly and quickly enforcing security policies where non-compliance occurs; and
(e) ensuring that in the event of a security incident, or suspected incident, personnel know how to respond and who to report to.

9.2 Security leadership

Security leadership requires all levels of management, and not just technical specialists, to demonstrate commitment and support so that security good practice is integrated into all aspects of a built asset's systems, associated processes and built asset data. Strong leadership on the importance of security matters is likely to engender a positive approach, good awareness and reduce the risk to the organization and the built asset.

Key requirements for achieving security leadership include:

(a) ensuring that requirements for security management are included in job descriptions;
(b) recognizing and understanding security issues that may affect the built asset;
(c) having relevant security targets;
(d) ensuring that there is appropriate engagement with the workforce, including both employees and contract staff;
(e) allocating appropriate resources and time to addressing built asset-related security matters;
(f) ensuring appropriate actions are taken to remedy identified security issues and that the actions are implemented; and
(g) ensuring good two-way communication with the workforce so that security issues can be highlighted and discussed, and commitment can be obtained to resolve the issues.

An important leadership issue is addressing the management of security across organizational boundaries. These can include the boundaries between IT and facilities management departments, between the owner's or occupier's workforce and suppliers or contractors, and between different occupiers in a multi-occupancy built asset.

9.3 Developing the built asset security strategy

The starting point for developing the built asset security strategy is considering the strategic importance, risks to and sensitivity of the built asset, its use or operation, and its occupiers or users. CPNI has developed a triage process[40] that organizations can use to systematically assess the sensitivity of the built asset and asset-related information.

The security strategy should, as a minimum, include:

(a) the outcome of assessing the strategic importance, risks to and sensitivity of the built asset, its use or operation, and its occupiers or users;

[40] CPNI *Triage process for publication or disclosure of information* London: CPNI. 2021 https://www.cpni.gov.uk/system/files/documents/06/e9/Triage%20Process%20for%20the%20publication%20or%20disclosure%20of%20information.pdf

Note: The risk assessment should include any security risks arising from the greater availability of built asset information, the integration of built asset systems and services, and any increased dependency on digital systems, whether located in the built asset or remotely. In assessing risks, it is important to adopt a holistic approach, this is illustrated in Annex A.

(b) the governance, accountability and responsibility arrangements for security of the built asset (see Section 9.1), including the review and approval of the security strategy;

(c) an associated risk register that identifies the planned treatment of identified risks, which may include specific mitigation measures or treatments for risks both individually and where there are applicable compositional or cascading risks; and

Note: It is good practice for the risk register to record what risks, including residual risks, are being accepted or tolerated by the accountable individual (on behalf of the asset owner, asset occupiers/user and other relevant stakeholders). This demonstrates that these risks have been considered and not ignored.

(d) the frequency and/or triggers, parties involved and mechanisms for reviewing and updating the security strategy.

Note: For many built assets it may be acceptable to review the strategy only on a periodic basis. There may be specific events or changes of circumstance that require an unscheduled review, for example, a change of occupancy or use, developments in the threat landscape, or a serious incident affecting another built asset of a similar type, nature or use.

For built assets requiring more than the most basic of security measures, the contents of the security strategy will themselves be sensitive information. Access to the strategy should be managed on a strict need-to-know basis, with its contents as a whole, or in parts, subject to security measures, appropriate to the level of risk associated with inappropriate, unauthorized or unrestricted.

9.4 Relationship of security strategy, policies, processes and procedures

The successful safe and secure ownership, occupation and operation of a built asset requires a systemic approach to the creation of a security management plan; effectively, a set of rules relating to its use. The built asset's security strategy should be translated into practical, actionable steps by the creation of a suitable security management plan that encompasses the mitigation measured and identified in the strategy. The plan should comprise a coherent set of security policies, processes and procedures, as shown in Figure 9.1. Where appropriate, the plan may cross-reference other security and/or relevant management policies, processes and procedures that are in place in respect of the built asset and its occupancy or use.

While these terms are too often interchanged, policies, processes and procedures should be three distinct types of documentation. All three will address their related subject matter, but at different levels of detail and with different types of content. Each level has a unique purpose that drives the content contained in each type of document as illustrated in the example below. This cascade from the strategy through the policy to process and individual procedures is important as it provides an auditable trail that links specific actions and activities to the overall vision of how the built asset security risks will be managed and mitigated.

Example: steps from security strategy to security policy, processes and procedures

An organization has performed a security risks assessment and identified a threat to one of its sites that contains significant volumes of sensitive material. If this material were lost, stolen or misused it would have severe reputational, commercial and legal consequences for the organization. The security strategy for the site requires that access to the site is controlled.

Controlled Access Policy – Access to site Is determined by role and need. The policy sets out level of access to the site (such as unescorted or escorted) and sensitive areas within it (such as, permitted unescorted, permitted escorted,and not permitted) and the associated security screening and vetting requirements. The policy is supported by several processes such as:

(a) request for approval to visit site; and
(b) visitor management

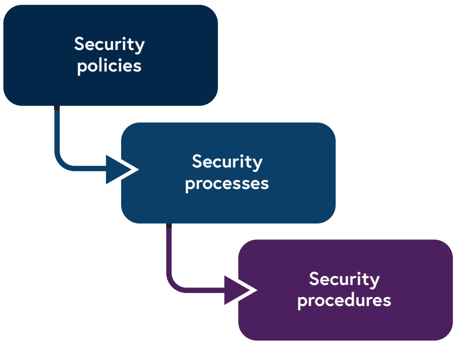
Process - Request for approval to visit site – The process sets out the high level steps to be followed by the visit sponsor and site security team in handling a visit request. The steps largely represent procedures to be followed, such as:

(a) application to vist site (completed by visit sponsor);
(b) security screening and vetting of visitors (performed by site security);
(c) retention of visit application records (managed by site administration team); and
(d) handling of emergency or exceptional applications (for use by site manager)

Procedure – Application to visit site – this details how an application is to be submitted, the details required (standard template), who can submit or approve the submission of an applications, the notice periods for different types of visit, etc.

The ultimate accountability and responsibility for the strategy and policy is determined by the organization's governance arrangements (see Section 9.1). Where the built asset is not owner occupied, the apportionment of security accountability and responsibility between owner and occupiers/users should be addressed during any contract or lease negotiations to ensure that obligations and responsibilities are clearly understood and documented.

Figure 9.1 Actionable steps for policies, processes and procedures as part of a built asset security strategy



9.5 Security policy objectives and scope

The objective of the security policy is to provide the guidelines under which the built asset's security procedures are developed. It should state what the policy is, the line of accountability, who is responsible for the execution and enforcement, why the policy is required, and where applicable, its classification. A security policy may be:

(a) specific to a security domain, for example, a policy concerning access to the built asset; or
(b) it may cut across more than one domain, for example, the policy regarding access to server and network/communications rooms may cover physical access and prohibit individuals from taking certain items, such as mobile phones or BYOD into those rooms.

The security policy will relate not only to the built asset, but to the built asset systems, associated business processes and built asset data. For single occupancy built assets it may be aligned to, or part of, the organization's security policies, including the cyber or information security policy. For multi-occupancy built assets it will need to be a standalone policy managed by the built asset's owner. In both scenarios it needs to be in a form that, where appropriate, allows it to be shared with third parties, such as those responsible for, or contracted to provide, design, construction, operations and maintenance services.

The security policy should set out the business rules and guidelines that ensure consistency and compliance with the strategic direction and risk appetite of the built asset owner and/or occupiers/users. Given the cross-functional nature of a built asset's security strategy, ownership should be aligned with the governance arrangements described in Section 9.1.

The security processes and procedures documentation should translate policy into working processes and clearly defined procedural steps to enable a reliable and consistent delivery of the policy.

9.6 Standards, frameworks, guidance and good practice

There is a wide range of security-related standards, guidance and best practice available that apply to IT and industrial control systems. The bibliography in Annex D lists a number of potentially relevant documents.

A key consideration when implementing security-related standards and guidance is how the integration and interaction between different operational domains will be addressed, for example IT and OT systems. There is no single standard or group of related standards that will address the full range of physical, personnel process and technical threats to the security of a built asset. Therefore, it is necessary to adopt appropriate and proportionate controls (which may be from multiple sources) when developing a security management plan to support the security strategy.

9.7 Legislation, regulation and systems

Built asset systems and built asset data can be affected by a variety of legislation and regulation. The impact and controls that may be required will vary from system to system. The cyber security policy may need to address a combination of the following types of legislation:

(a) health and safety – where the failure, misuse or modification of a built asset system could affect a person's health or lead to injury or loss of life, the system has safety-critical features and appropriate measures as protection from adverse conditions as a result of a cyber security incident. For safety-critical systems, the cyber security measures should be consistent with the objective of reducing the risk of harm to as low as is reasonably practicable.

(b) data protection – where PII is stored or processed in built asset systems. Examples of where PII may be used in built asset systems include the use of biometric data identification and access control, information about any special facilities or support required by individuals with health problems or disabilities and personal data associated with access control systems. The collection, storage and analysis of PII can also have privacy implications.

(c) criminal legislation – depending on the legal jurisdictions in which the built asset, the built asset systems and the built asset data are located, there is often legislation relating to unauthorized access to, or use or modification of, computer systems and their data. For example, in the UK the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorized access to computer material, to gain unauthorized access with intent to commit or facilitate commission of further offences or to make unauthorized modification of computer material. Therefore, it is an offence to:

   i. use another person's username and password without proper authority to access built asset data or built asset systems;

   ii. alter, delete, copy or move a program or data;

   iii. output a program or data to a screen or printer; or

   iv. impersonate that other person using e-mail, online chat, web or other services.

(d) corporate governance – for example, the Sarbanes-Oxley Act 2002. This US legislation introduced major changes to the regulation of financial practice and corporate governance of US organizations, both within the USA and their global operations. Security and governance of risk, particularly those risks with significant financial consequences, are key parts of this legislation.

(e) civil legislation – a failure to take appropriate steps to manage the cyber security of built asset systems, their associated processes and built asset data could expose any of the parties involved to claims for compensation as a result of negligence, such as breach of contract.

(f) specific legislation or regulations – some built assets, due to the nature of their use, ownership or occupants, may be subject to additional legal or regulatory requirements, for example, sensitive governmental built assets may be required to comply with specific national security-related regulations. In the UK, sports grounds and stadiums have specific legislation covering their safe use, for example, the Safety of Sports Grounds Act 1975, the Fire Safety and Safety of Places of Sport Act 1987 and the Safety of Places of Sport Regulations 1988. Many of these documents will not contain specific cyber security requirements, but there is still a need to consider these requirements. More recent guidance from the National Counter Terrorism Security Office (NCTSO) on crowded places[41] does contain advice on information security, but this is primarily aimed at the business and administrative systems rather than the built asset systems.

Example: specific legislation with cyber security implications

In *Guide to Safety at Sports Grounds (Green Guide)*[42], guidance is provided on the principal means of communication required in a sports ground. It lists eight principal means:

1. radio communications;
2. telephone communications (internal and external);
3. public address systems;
4. CCTV;
5. scoreboards, information boards and video boards;
6. signs;
7. written communications (for example, tickets, signs and printed material); and
8. interpersonal communications.

Of the principal means listed, the first five are susceptible to cyber security incidents. Given the extensive use of information and communications technologies in stadiums and sports grounds, the operator needs to consider the cyber security risks associated with this critical site infrastructure.

[41] NCTSO *Guidance Cyber Security* 2020 https://www.gov.uk/government/publications/crowded-places-guidance/cyber-security

[42] Sports Grounds Safety Authority *Guide to Safety at Sports Grounds 'Green Guide'* https://sgsa.org.uk/greenguide/

Annex A

Assessing built asset security risks

A.1 Introduction

When identifying security risks affecting the built environment, individual built assets or groups of built assets, it is appropriate to consider the risks from a number of perspectives. Typically, these might include:

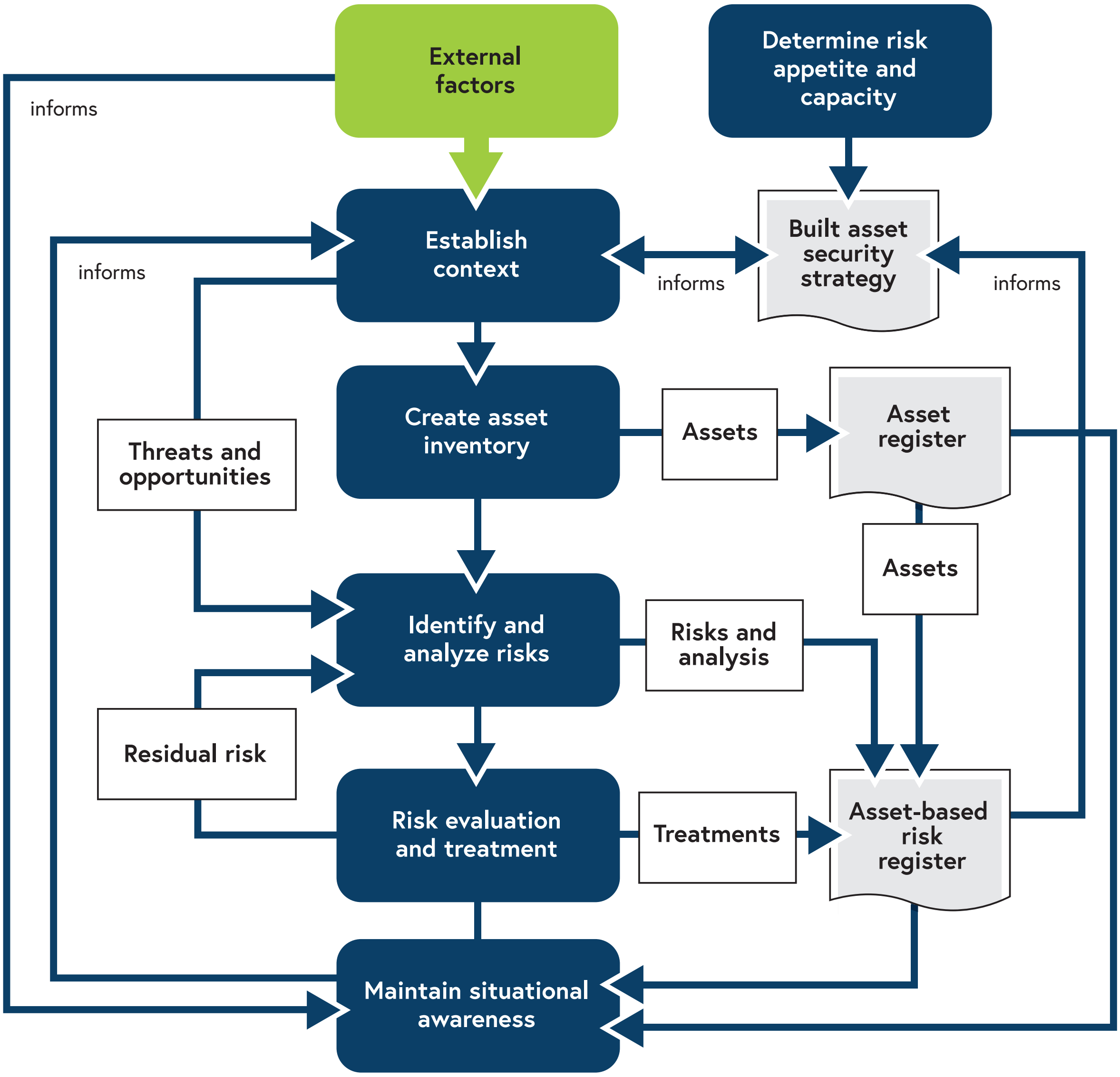
(i) operational – the potential impact on the built asset(s) arising from disruption of its construction, operation or maintenance and the consequential impact on its owners/occupiers/users, including the potential for reputational damage;
(j) confidentiality and privacy – the loss of, or unauthorized access to, sensitive information about the built asset itself, its use and/or PII relating to the occupiers or users;
(k) safety – the potential harm to individuals, the built asset(s) and/or the environment arising from the failure, in whole or in part, or misuse of built asset systems or any related services;
(l) financial – this could include consequential losses or remediation costs if the incident causes damage to the built asset or its systems, as well as costs associated with managing a security incident or near miss;
(m) legal – arising from non-compliance with legislation or regulations, for example, subsequent legal costs and fines; and
(n) third parties – arising from harm caused to one or more third parties, for example, spreading malware to third party products or systems and provision of inaccurate or misleading data and/or information leading to corruption of databases.

A.2 Risk management approach

There are numerous ways of approaching risk management, including the standards listed in Annex D. The choice of approach or method may be determined by an organization's established practice.

The risk management approach illustrated in Figure A.1 and described in this Annex provides a systematic asset-based approach that can be used to manage security risks in the built environment, whether at scale (for example, a campus) or focussed on a single built asset, either in part or as a whole. When considering what assets are in scope, this should be based on the nature and use of the built asset, its owners, occupiers and/or users. The assets that may be fixed, mobile or movable, and which could be physical (tangible) or digital (intangible). The assets should include data and/or information about the built asset and its operation, which may be in digital or printed form, and may be localized (for example, a CDE containing built asset design and construction data) or distributed across multiple sources and locations. A key test in considering whether to include an asset is whether its loss, destruction, inappropriate use or disclosure represents a security risk.

Figure A.1 Asset-based risk management approach


External factors
Determine risk appetite and capacity
informs
Establish context
informs
Built asset security strategy
informs
informs
Create asset inventory
Assets
Asset register
Threats and opportunities
Assets
Identify and analyze risks
Risks and analysis
Residual risk
Risk evaluation and treatment
Treatments
Asset-based risk register
Maintain situational awareness

Prior to starting the risk management process, or when reviewing the built asset security strategy and any supporting risk register, the senior accountable individual (see Section 9.1) should determine the risk appetite and capacity of the organizations involved in securing the built asset, the built asset systems and the built asset data. The risk appetite and capacity should guide development of the built asset security strategy and be taken into account when evaluating and treating risks.

A.3 External factors

A starting point for the risk assessment is developing an understanding of the external factors that may create security risks and opportunities. For example, a political, economic, sociological, technological, legal and environmental (PESTLE) analysis could be undertaken to analyze the key factors that may affect or influence the security of a built asset and the built asset systems.

When considering the external factors, those of particular interest and that warrant additional attention are likely to be related to:

(a) legislation and regulatory requirements – both in general and specific to the built asset, its use and its occupiers or users. For example, a built asset that forms part of the networked infrastructure covered by the Network and Information Systems (NIS) Regulations[43] may be subject to specific cyber security reporting requirements.
(b) the operating and business environment – this will be determined by the nature of the built asset and its use. For example, the potential security threats, both cyber and physical, to an airport terminal building will generally be different to those of a block of flats. The nature of the threat environment will be determined by the attractiveness to potential threat actors of the built asset, the built asset systems and the owners, occupiers or users.
(c) stakeholder needs and expectations – these may shape the risk appetite of the built asset owner or operator. For example, a built asset owner may seek to reduce the potential reputational harm that would arise from a serious security incident affecting a high-profile built asset or its occupier.

The threat environment is constantly changing through the emergence of new or potential vulnerabilities, the shifting attention and priorities of threat actors and the disclosure of new tools and techniques to exploit vulnerabilities. As the external factors are not static, situational awareness should be maintained through the built asset's lifecycle.

A.4 Establish context

The context is the circumstances that form the setting of the built asset and can include:

(a) its location and relationship to other elements of the built environment;
(b) the nature of the built asset(s);
(c) the owner, operator, users and/or occupiers;
(d) the significance of its business function and the consequence of any loss or degraded functionality;
(e) the built asset systems, their location, connectivity and integration;
(f) the built asset data and/or information;
(g) the extent to which appropriate and proportionate security measures have been implemented; and
(h) the existence of any safety-related systems that should be included in the risk assessment.

A combination of the above factors will determine the potential attractiveness of the built asset as a target for threat actors.

In considering a built asset's context, an additional factor to address is the complex relationship between safety (hazards) and security (threats) in all cyber-physical entities, that is, the built assets and the built asset systems. Both safety and security can result in adversity. Unless they are appropriately secured, built assets and/or built asset systems, and any related services, are unlikely to be safe. The aim of the built asset's security strategy is to reduce the risk that a threat actor can exploit a vulnerability.

Case study: damage to a manufacturing plant

In December 2014, the German government released an annual report, in which they noted that a threat actor had infiltrated a steel manufacturing facility by using a spear phishing email to gain access to the corporate network and then moved laterally though the infrastructure to gain access to the plant network. According to the report, the threat actor was able to cause multiple components of the system to fail. This security incident specifically impacted critical process components to become unregulated, which resulted in massive physical damage to the asset[44].

[43] UK Government *The Network and Information Systems Regulations 2018* https://www.legislation.gov.uk/uksi/2018/506/made
[44] For further information on this incident see https://www.bbc.co.uk/news/technology-30575104

A.5 Create asset inventory

The next stage in the risk management process is to create an asset inventory, beginning with the built asset itself. This involves the identification and decomposition of elements of the asset, the built asset systems and the built asset data. Section 5.3 lists some examples of types of assets that may need to be reviewed and, where appropriate, decomposed. For complex or hybrid assets, techniques such as failure mode effects analysis may be used to identify and disaggregate functional and/or constituent parts. The objective of any decomposition is to identify the lowest level at which risk is going to be managed.

For example, in a built asset system there is a need to consider the risks associated with the physical elements (sensors and actuators), the cyber (digital) elements and their combination. When considering a cyber element such as the operator console, the minimum decomposition may include applications, the operating system, processing hardware, any networking or communications connectivity and the system's operational and configuration data.

The output of this process is known as the asset register, or an updated asset register if the process is reviewing and updating the risk register. The asset register should identify the nature and location of the listed assets and provide information on the adjacencies and functional relationships between assets (for example, composition, dependencies and connectivity).

A.6 Identify and assess risks

For each of the identified assets, this stage of the process should identify and assess:

(a) its value;
(b) for a data asset, the criticality and impact of its loss, corruption, compromise or disclosure;
(c) for a built asset, the criticality and impact of its compromise and/or failure, either partially or as a whole;
(d) for a built asset system, its criticality and the impact of:
  i. its loss, corruption or compromise;
  ii. its failure, either partially or as a whole;
  iii. its misuse or abuse (whether unintentional or malicious); and
  iv. its incorrect or inappropriate operation.
(e) its vulnerabilities;
(f) its hazards; and
(g) potential threats and opportunities.

The assessment process should determine the attractiveness of each asset to specific threat actors by considering their motivation and capability, as well as the likelihood that individual types of threat actor could exploit the vulnerabilities.

Note: While there are a variety of numerical risk scoring approaches, care needs to be taken in assessing cyber-physical risks to understand the impact and recovery time. This is particularly relevant with regard to cyber risks that cause physical damage to the built asset and/or its systems, or could result in harm to asset users/operators.

Using the information gathered in **(a)** to **(g)**, the risk analyst should synthesize and prioritize the potential risks to the built asset, the built asset systems, built asset data and the relevant stakeholders. While it is common practice to primarily assess risks in isolation, given the nature of built assets and their systems, consideration should be given to security risks that arise through the composition, integration and/or interaction of built assets and their components, sub-systems and systems and, where appropriate, their interaction as systems-of-systems. This type of risk can arise from complementary weaknesses in two or more elements that are being integrated. The effect of exposure of a combined vulnerability and its subsequent exploitation may be significantly greater than the exploitation of the individual vulnerabilities.

The identified and assessed risks should be added to the asset-based risk register (see Annex A.8) for evaluation and treatment in the next stage of the process.

A.7 Risk evaluation and treatment

In this stage of the process the identified risks are systematically evaluated, both as standalone (individual) risks and as groups of two or more sets that may give rise to combinational or cascading effects. When considering the risks relating to built asset data, the impact of aggregation by volume and by association should be considered, including the effect of data that has been published or disclosed (whether intentionally or as a result of an earlier security incident).

It is important that risks are not considered and treated in isolation, as there may be considerable interaction between risks. In a cyber incident there may be an 'attack path', which has been enabled by combinational effects arising from a linear path of negative events. This is a common feature of many significant security breaches: it was not the failure of one security measure, but failure of a series of measures that enabled the breach.

In complex systems (systems of systems) relationships between systems or sub-systems may be non-linear. Cascading effects can occur in these systems, including amplification and subsidiary negative events or outcomes. The effect of the non-linearity is that, rather than risk spreading in a simple longitudinal fashion, the effects spread in a ripple and affect multiple assets that might not be directly connected to each other. The scope of the risk, which is determined by the boundaries of the impact, is an important factor – particularly in situations where there is a systemic exposure through one or more vulnerabilities in multiple items, such as the Wannacry incident.

When evaluating and treating risks, the risk appetite and available risk capacity of the responsible organization(s) should be taken into account. The risk appetite and available risk capacity should be determined by the senior accountable individual (see Section 9.1) taking into consideration the built asset's context and the relationship(s) between built asset owner, operator and occupiers/users, as appropriate.

As part of an iterative process of taking each risk in turn, its acceptability should be considered by taking into account any combinational or cascading effects of the risks. If a risk is acceptable, the capacity of the entity/entities bearing the risk should be updated to reflect the risk that is being carried.

For a risk that is considered unacceptable, its potential treatment through the adoption and application of mitigation measures should be assessed. If appropriate, proportionate and cost-effective measures can be identified. These measures should be recorded in the risk register and any residual risk returned to the identification and assessment process. If no appropriate measures can be identified or the level of residual risk remains unacceptable, the senior accountable individual needs to raise this at board or executive level as strategic decisions may be required to bring the level of risk within an acceptable level.

A.8 The asset-based risk register

The risk register should encompass all known security risks to the built asset, built asset systems and built asset data, as well as those which could be reasonably anticipated.

Depending on the nature of the built asset, its systems and use, it may be prudent to conduct annual or biennial risks reviews. However, the frequency should be determined by the rate at which changes are being made to the built asset and its systems, as well as how dynamic the threat environment is. The rate of change to the assets is significant as this can create new vulnerabilities and may increase the level of supply chain risk as suppliers are provided with information or access to physical assets.

The asset-based risk register, as a whole or in part, is sensitive information and access to it should be managed on a need-to-know basis. Security measures implemented to protect the register should be appropriate to the level of risk, in terms of its creation, storage, distribution and use.

A.9 Maintain situational awareness

Over the lifecycle of the built asset, the built asset systems and the built asset data, external changes will inevitably occur, some of which will change the security risks and associate threat environment. To address this, situational awareness should be maintained by monitoring:

(a) security risks and opportunities;
(b) emerging threats and vulnerabilities; and
(c) the scope and security context of the built asset, the built asset systems and the built asset data.

The monitoring should focus on triggers such as:

(a) the emergence of a new threat actor;
(b) changes in the security context;
(c) the identification of new/emerging vulnerabilities;
(d) the identification or publication of new exploits enabling easier access to vulnerabilities or increasing their impact; and
(e) changes to legislative and regulatory provisions.

These triggers may be set out in the built asset security strategy or in the risk management policy. When one or more of the triggers occurs, an ad hoc review of some or all of the risk portfolio may be necessary to assess whether additional risk mitigation measures are required or changes should be made to existing measures.

In a similar fashion to asset-related risks, the supply chain risks should be linked to the relevant assets and reviewed periodically in response to changes in external factors.

The nature, scope and scale of the situational awareness monitoring should be consistent with the perceived level of risk, as documented by the risk portfolio in the asset-based risk register (see Annex A.8).

A.10 Supply chain security risks

In developing the asset-based risk register, consideration should be given to potential supply chain risks as they impact on individual or combinations of assets identified in the asset register (see Annex A.5).

Annex A – Assessing built asset security risks

The asset register should include an inventory of software/firmware to the extent that suppliers are willing or able to disclose. However, as the Heartbleed[45] incident demonstrates, this can be difficult to establish where suppliers bundle open-source or other third-party software with their products.

Note: The UK Ministry of Defence operates a supplier risk assessment process, where the cyber security requirements for various risk profiles are set out in Annex A of DEF STAN 05-138:2017 *Cyber security for defence suppliers*. The approach set out in this Annex may inform an organization's development of its own supplier security requirements. The risk assessment process is applicable to all suppliers (cover hardware, software and systems).

Over the lifecycle of the built asset most, if not all, of the identified assets will require the attention of a supply chain. The asset register provides a starting point for developing and maintaining an understanding of the supply chain, which is generally multitiered in nature. Depending on the nature of each supplier's services or products it might be necessary to obtain information from the supplier, or potential supplier. This will allow decomposition and security risk assessment of the supplier's own inputs into the contracts, including organizations that support the supplier's operations.

Note: If the organization is supplying sensitive data and/or information to a supplier who is processing it in a cloud-based SaaS, the organization should consider applying the NCSC's cloud security guidance[46] to assess the level of risk this processing might pose in respect of the sensitive data and/or information. This assessment requires information about the SaaS provider's technology, hosting and security arrangements.

The security measures that suppliers may be required to implement should encompass personnel, physical, process and technological aspects. The measures required should be informed by the level of the supplier's risk profile in respect of the built asset, its systems and data, and the specifics of the risks that are to be mitigated. Supplier contracts should clearly specify the required security measures and include appropriate provisions for flow down of these measures along the subsidiary supply chain. The measures should typically include provisions regarding notification of security incidents and near misses, and an obligation to assist in the investigation and resolution of such events.

[45] ICS-CERT Monitor (Jan-April 2014). *Internet accessible control systems at risk ('heartbleed')*. https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf
[46] NCSC *Cloud security guidance* https://www.ncsc.gov.uk/collection/cloud-security

Annex B

Glossary

Term	Definition	Source (where applicable)
AACS	automatic access control system	
asset	Item or entity that has potential or actual value to an organization	BS ISO 55000:2014, **3.2.1**
asset data (or information)	Data (or information) relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item or entity that has potential or actual value to an organization	PAS 1085:2018, **3.1.2** and **3.1.3**
BACS	building automation and control system	
BIM	Building Information Modelling	
BMS	building management system	
BYOD	bring your own device	
CAFM	computer-aided facilities management	
CDE	common data environments	
context	Circumstances that form the setting for an asset, event, data and/or information, which allow its significance and/or meaning to be better understood	PAS 1085:2018, **3.1.4**
CPNI	Centre for the Protection of National Infrastructure	
DCS	distributed control system	
disclosure	Action of making sensitive, classified or private data and/or information known	PAS 1085:2018, **3.1.10**
enabling system	System that supports a system-of-interest during its lifecycle stages but does not necessarily contribute directly to its function during operation	
HoMER	Holistic Management of Employee Risk	
hostile reconnaissance	Activity of acquiring information about a target with the view to planning to attack, compromise, disrupt or destroy that target	PAS 1085:2018, **3.1.11**
HVAC	heating ventilation and air conditioning system	
IaaS	infrastructure as a service	
IACS	industrial automation and control system	
ICT	information and communication technologies	
IIoT	Industrial Internet of Things	
information management	Policies, processes, procedures and tasks applied to the data and/or information across its lifecycle to ensure its accuracy, authenticity, confidentiality, integrity and utility	PAS 1085:2018, **3.1.13**
IoT	Internet of Things	
IT	information technology	
ITT	invitation to tender	
ITU	International Telecommunications Union	
LIDAR	light detection and ranging	
ML	machine learning	
NCSC	National Cyber Security Centre	
near-miss	Incident in which a security incident is narrowly avoided, either by chance or through deliberate action	PAS 1085:2018, **3.1.15**
need-to-know	Grant of access to data and/or information relating to assets for an individual or organization where such access is necessary for them to perform their role satisfactorily and safely	PAS 1085:2018, **3.1.16**

(*continued*)

Annex B – Glossary

Term	Definition	Source (where applicable)
operational technology (OT)	Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the organization	PAS 1085:2018, **3.1.17**
OT	operational technology	
other system	System that interacts with the system-of-interest in its operational environment	
OWASP	Open Web Application Security Project	
PaaS	platform as a service	
pattern-of-life	Identification of habits, routines and preferences of individual(s) or group(s) that enable prediction of future actions and/or behaviour	PAS 185:2017, **3.1.31**, modified
pattern-of-use	Identification of routine actions in the handling, operation and management of assets	PAS 185:2017, **3.1.32**
PESTLE	political, economic, sociological, technological, legal and environmental (analysis)	
PII	personally identifiable information	
PLC	programmable logic controllers	
PPM	planned preventive maintenance	
RF	radio frequency	
risk appetite	Amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives	Chartered Institute of Internal Auditors
risk capacity	Resource(s), including financial, intangible and human, that an organization is able to deploy in managing risk	
risk universe	Full range of risks that could impact, either positively or negatively, on the ability of the organization to achieve its long-term aims	
SaaS	software as a service	
sabotage	Deliberate, malicious action carried out with the aim of weakening, obstructing, disrupting, damaging or destroying an asset, activity, service, organization or other entity	PAS 1085:2018, **3.1.31**
safety-related system	A designated system that both implements the required safety functions necessary to achieve or maintain a safe state; and is intended to achieve, on its own or with other safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions	Source IEC 61508-4 3.4.1
SCADA	supervisory control and data acquisition	
security	State of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts, including sabotage	Engineering Council, 2016[47]
security incident	Event or events during which the security of an asset, organization or person is, or might be, compromised, either accidentally or deliberately	PAS 1085:2018, **3.1.34**
SoR	statement of requirement	
supply chain	Network of organizations, directly or indirectly interlinked and interdependent, resources, activities and technology involved across the lifecycle of a built asset and/or built asset system, and any associated data or information	
system	Combination of interacting socio-technical elements organized to achieve one or more stated purposes, or self-organized to produce effects or outputs that differ from the stated purpose.	

(*continued*)

[47] Further information is available from http://www.engc.org.uk/security

Annex B – Glossary

Term	Definition	Source (where applicable)
system element	Member of a set of elements that constitute a system	
system-of-interest	System that is the focus of the systems engineering or security effort	
TCP	transmission control protocol	
threat	Potential cause of an incident which might result in harm to an asset (s), individual(s) and/or organization(s)	PAS 1085:2018, **3.1.43**
threat actor	Person or organization that can adversely act on assets	PAS 1085:2018, **3.1.45**
TVRA	threat, vulnerability and risk assessment	
UPS	uninterruptible power supply	
vulnerability	Weakness that can be exploited by one or more threats	PAS 1085:2018, **3.1.46**
WAN	wide-area network	

Annex C

References and footnotes

Website references were last accessed and correct at May 2021.

1. FireEye *Blog on SolarWinds attack* https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

2. Microsoft *Blog on SolarWinds attack* https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

3. The term Building Information Modelling potentially covers a wide range of digital engineering activities, ranging from the electronic exchange and collaborative storage of design documentation, 3D graphical modelling of built assets, which may be purely representational (for example, a visualization of building design) or simulations (for example, presentation of pedestrian or traffic flows, CCTV fields of view, etc). The term digital twin is a currently being used, often indiscriminately, to encompass a variety of models ranging from design simulations to more complex built asset control systems.

4. Radichel T. *Case study: Critical Controls that Could Have Prevented Target Breach* Bethesda, MD: SANS Institute, 2014. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

5. CPNI *Security-Minded approach to Digital Engineering* https://www.cpni.gov.uk/security-minded-approach-digital-engineering and CPNI *Security-Minded approach to Information Management* https://www.cpni.gov.uk/security-minded-approach-information-management

6. 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. Part 5: Security-minded approach to information management*

7. Government Security Classifications https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

8. The risks in individual domestic buildings are currently relatively low, as few homes have high levels of automation. Increased use of smart technologies within the home may change this in the future. This document is, however, applicable to large multi-occupancy residential buildings, for example, blocks of flats and student residences.

9. CPNI *Security Considerations Assessment* https://www.cpni.gov.uk/security-considerations-assessment

10. See The Economist and SANS websites for information on industrial and corporate espionage respectively: http://www.economist.com/blogs/democracyinamerica/2014/05/industrial-espionage
 http://www.sans.org/reading-room/whitepapers/engineering/corporate-espionage-201-512

11. National Counter Terrorism Security Office (NCTSO) *Crowded places guidance* https://www.gov.uk/government/publications/crowded-places-guidance

12. CPNI *Security Minded Communications Guidance for Virtual Tours* https://www.cpni.gov.uk/system/files/documents/93/4f/Security%20Minded%20Comms-%20Virtual%20Tours%20Guidance%20V3.pdf

13. See new ETSI standard for consumer IoT security https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf and the proposed UK legislation that will initially define the minimal security requirements for consumer IoT products being sold in the UK https://www.gov.uk/government/collections/secure-by-design

Annex C – References and footnotes

14. OWASP *Top 10 Web Application Security Risks* https://owasp.org/www-project-top-ten/

15. Enterprise Architecture Center of Excellence (EACOE) Enterprise framework http://www.eacoe.org

16. BT Openreach Analogue line withdrawal https://www.openreach.co.uk/cpportal/products/product-withdrawal/wlr-withdrawal

17. Note: long-life lithium batteries may serve to reduce the total cost of ownership (TCO) by enabling certain low-power devices to operate maintenance-free for many years, but this depends on the design and operation of the sensors.

18. Secured by Design https://www.securedbydesign.com/

19. Secured by Design https://www.securedbydesign.com/guidance/design-guides

20. NCSC *Secure by Default* https://www.ncsc.gov.uk/information/secure-default

21. *Privacy by Design: The 7 Foundational Principles*. https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

22. Adapted from Pitt Turner W, Seader JH, Renaud V, Brill KG. *Tier classifications define site infrastructure performance* Santa Fe, NM: The Uptime Institute, 2008.

23. BS ISO/IEC/IEEE 15288:2015 *Systems and software engineering — System life cycle processes* Section 5.4, p14.

24. National Institute of Standards and Technology (NIST) SP 800-160 Vol. 1 *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* Gaithersburg MD: NIST, 2018.

25. IEC TS 62443-1-1:2009 *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

26. NCSC *Preventing Lateral Movement* https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

27. CPNI *Common Data Environments - A guide for BIM Level 2* https://www.cpni.gov.uk/system/files/documents/8b/2b/20170309_Common_Data_Environments_A_Guide_for_BIM_Level_2.pdf

28. NCSC *Supply chain security guidance* https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

29. CPNI *Procuring the services of a specialist security consultant when undertaking a project relating to a built asset, Version 7* London: CPNI, 2020.

30. NCSC *Certified Professional scheme* https://www.ncsc.gov.uk/information/about-certified-professional-scheme

31. CPNI *Passport to Good Security, for Senior Executives* London: CPNI, 2015. https://www.cpni.gov.uk/system/files/documents/b0/69/CPNI_Passport_to_Good_Security.pdf

32. NCSC *10 Steps to Cyber Security* London: NCSC, 2018. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

33. CPNI *CPNI Insider data collection study* London: CPNI, 2013. https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

34. CPNI *Role Based Security Risk Assessment* London: CPNI, 2020. https://www.cpni.gov.uk/insider-risks/role-based-security-risk-assessment

35. http://news.bbc.co.uk/1/hi/england/7214598.stm and http://news.bbc.co.uk/1/hi/uk/7154191.stm

Annex C – References and footnotes

36. http://news.bbc.co.uk/1/hi/uk/426092.stm

37. See BS 7858 *Security screening of individuals employed in a security environment - Code of practice*

38. CPNI *Holistic management of employee risk (HoMER)* London: CPNI, 2012. https://www.cpni.gov.uk/system/files/documents/62/53/Holistic-Management-of-Employee-Risk-HoMER-Guidance.pdf

39. International Telecommunication Union (ITU) *Clause 3.2.5 – Series X: Data networks, open system communications and security: Overview of cybersecurity* Geneva: ITU, 2008. https://www.itu.int/rec/T-REC-X.1205-200804-I

40. CPNI *Triage process for publication or disclosure of information* London: CPNI. 2021 https://www.cpni.gov.uk/system/files/documents/06/e9/Triage%20Process%20for%20the%20publication%20or%20disclosure%20of%20information.pdf

41. NCTSO *Guidance Cyber Security* 2020 https://www.gov.uk/government/publications/crowded-places-guidance/cyber-security

42. Sports Grounds Safety Authority Guide to Safety at Sports Grounds 'Green Guide' https://sgsa.org.uk/greenguide/

43. UK Government *The Network and Information Systems Regulations 2018* https://www.legislation.gov.uk/uksi/2018/506/made

44. For further information on this incident see https://www.bbc.co.uk/news/technology-30575104

45. ICS-CERT Monitor (Jan-April 2014). *Internet accessible control systems at risk ('heartbleed').* https://us-cert.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf

46. NCSC *Cloud security guidance* https://www.ncsc.gov.uk/collection/cloud-security

47. Further information is available from http://www.engc.org.uk/security

Annex D

Bibliography

The documents listed below are to varying degrees relevant to the design and operation of digital systems used in the management and operation of the built environment and the protection of data and information assets.

D.1 General IT and cyber security standards

Reference	Title/Description
ISO/IEC 13335	Information technology. Security techniques. Management of information and communications technology security
ISO/IEC 15408	Common criteria for information technology security evaluation
ISO/IEC 27001	Information security management systems requirements
ISO/IEC 27002	A code of practice for information security management
PD ISO/IEC TS 27100	Information technology. Cybersecurity. Overview and concepts
Critical Security Controls	CIS controls. Version 8.0 (28 May 2021) A reference set of recommendations for methods to address risks to enterprise data and systems. Published by the Center for Internet Security [http://www.cisecurity.org/controls]
NCSC Risk management guidance V1.0	Guidance to help organisations make decisions about cyber security risk https://www.ncsc.gov.uk/collection/risk-management-collection
DEF STAN 05-138:2017	Cyber security for defence suppliers
BIS/12/1120	10 Steps to cyber security: executive companion Provides guidance for business on how to make their networks more resilient and protect key information assets against cyber threats.
BIS/12/1121	10 steps to cyber security: advice sheets Provides detailed cyber security information and advice on the 10 steps described in BIS/12/1120.
MITRE ATT&CK®	MITRE ATT&CK® https://attack.mitre.org/
CVSS	Common vulnerability scoring system (CVSS) special interest group https://www.first.org/cvss/
Cloud Security Alliance	Big data security and privacy handbook. 100 best practices in big data security and privacy https://downloads.cloudsecurityalliance.org/assets/research/big-data/BigData_Security_and_Privacy_Handbook.pdf
NCSC Connected Places Cyber Security Principles	Secure design, build and management of public realm technology, infrastructure, and data-rich environments for local authorities https://www.ncsc.gov.uk/collection/connected-places-security-principles
NCSC 10 Steps to Cyber Security	Guidance on how organisations can protect themselves in cyberspace https://www.ncsc.gov.uk/collection/10-steps

D.2 Security and safety of IACS and SCADA

Reference	Title/Description
IEC 62443	Security for industrial automation and control systems
ANSI/ISA-99.00.01	Part 1: Terminology, concepts, and models
NIST IR 7176	System protection profile. Industrial control systems (V1.0). Incorporates industrial control systems into common criteria
NIST SP 800-82	Guide to industrial control systems (ICS) security
IEC 61508	Functional safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
IEC TR 63069	Industrial-process measurement, control and automation – Framework for functional safety and security
ATT&CK® for ICS	ATT&CK® for industrial control systems https://collaborate.mitre.org/attackics/index.php/Main_Page
NCSC Operational technologies	Making sense of cyber security in OT environments https://www.ncsc.gov.uk/guidance/operational-technologies

D.3 Business related security guidance

Reference	Title/Description
BIS/12/1119	Cyber risk management: a board level responsibility Explains the benefits of cyber risk management to senior executives
ISO 20000 BS 15000	IT service management standards Based on Information Technology Infrastructure Library (ITIL)
BS 7858	Code of Practice for security screening of individuals employed in a security environment
Control Objectives for Information and Related Technology (COBIT) 5	A business framework for the governance and management of enterprise IT
PAS 555: 2013	Cyber security risk. Governance and management. Specification

D.4 Other standards and guidance

Reference	Title/Description
PCI DSS	Payment card industry data security standard
NIST SP 800-61	Computer security incident handling guide
PAS 97: 2012	A specification for mail screening and security
RFC 2196:1997	The Internet Engineering Task Force (IETF): Site security handbook
RFC 2350	The Internet Engineering Task Force (IETF): Expectations for computer security incident response
BS ISO/IEC 42010	Systems and software engineering. Architecture description
EACOE	Enterprise framework

Index