ProtectUK

Digital built assets and environments

Original publication date

02/11/2020

1. Introduction

A built asset could include a building, multiple buildings such as on a site or a campus, a portfolio or network of assets, or a built infrastructure, such as roads, railways, pipelines, dams, docks etc. and may include associated land or water.



Digital built assets and environments generate digital representations of, and data about, physical and functional aspects of a built asset. The effective management and security of these assets require a cross-sector collaborative approach, traditionally seen within the architectural, engineering and construction industries. This approach involves a more transparent way of working, by openly sharing detailed models and large amounts of digital asset information.

Asset information refers to data relating to the specification, design, construction/acquisition, operation and maintenance, and disposal/decommissioning of an item, thing or entity that has potential or actual value to an organisation. Asset information may include design information and models, documents, images, software, spatial information and task or activity-related information.

The planning, design, construction, operation and maintenance of built assets is increasingly making use of digital engineering and placing greater reliance on digital technologies. It is important that security managers understand the inherent vulnerability issues which may result. These vulnerabilities may present in number of ways, including through the unauthorised, or malicious use of authorised access to systems.

This may subsequently cause:

- a compromise to the safety, security and resilience of
    - personnel and other occupants or users of the built asset and its services
    - the built asset itself
    - the asset information

Additionally:

- a compromise to the benefits the built asset exists to deliver, be they societal, environmental and/or commercial.

Policies and processes should therefore be in place to encourage the use of appropriate and proportionate controls if the trustworthiness and security of digital built assets is to be maintained.

2. Security of digital built assets

The models and the associated databases will likely contain significant amounts of aggregated information about a built asset.

Such Information may include:

- its design and associated specifications
- the construction process
- component assets, their precise location and interconnectivity
- product data about component assets including specification, design and maintenance information

- the services or function the built asset provides
- its occupants or users
- operational and management procedures, including those relating to safety and security

Alongside developments in digital engineering, there is a drive to make public data more easily accessible, unless there are clear and specific reasons not to do so. This is likely to increase the amount of information available in the public domain.

The use of building management systems (BMS) is already commonplace. However, with technology used by most BMS and third-party systems starting to converge, the increasing use of Internet Protocol (IP) networks by systems to communicate internally and with the outside world, and the use of commercial off-the-shelf IT products, software and operating systems as key components, a number of potential vulnerabilities are created.

3. PAS 1192 – 5:2015

Access to any of the types of information and systems described above would greatly assist those engaged in a range of criminal activity, espionage and terrorism. In order to understand and address those potential vulnerabilities, NPSA (formerly CPNI) and the British Standards Institution (BSI) have produced guidance, PAS 1192 – 5:2015, a specification for security-minded building information modelling, digital built environments and smart asset management.

The standard sets out effective and proportionate ways to enable the safe and secure sharing and publication of digital asset information. It is supported by a suite of related guidance documentation available on the NPSA website.

Go to: NPSA PAS: 1192-5:2015 webpage to learn more about how this specification can keep an organisation safe.

KEYWORDS
DIGITAL
SECURITY
PHYSICAL SECURITY
PUBLICLY ACCESSIBLE PLACES
RISK MANAGEMENT
PALS GUIDANCE
PALS
PUBLICLY ACCESSIBLE LOCATIONS