Initiating a dialogue about the security of digital built assets: a guide for managers
(with regard to PAS 1192-5, A Specification for security-minded building information modelling, digital built environments and smart asset management)

May 2015

Introduction

This guidance aims to help those with more general security responsibilities or estate management responsibilities start a dialogue within their organisation about the security of built assets. It sets out the questions which an organisation needs to ask of itself and its supply chain in order to gain an understanding of what information it, or others, holds in relation to its built assets. The questions will also assist in assessing that information's availability and accessibility, and therefore the potential impact on the security of the asset, its users or services.

The questions will be relevant where the built asset is the subject of a construction project or where the asset information is created, stored, processed and viewed in a digital format.

Clarification of terminology

A **built asset** may comprise a building, multiple buildings (e.g. on a site or campus), a portfolio or network of assets, or built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.) and may include associated land or water.

In this guidance, **asset information** refers to data or information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization. Asset information can include design information and models, documents, images, software, spatial information and task or activity-related information.

A **sensitive built asset** is one where the built asset, as a whole or in part, may be of interest to a threat agent for hostile, malicious, fraudulent and/or criminal behaviours or activities.

A **neighbouring built asset** is classed as a built asset that shares a boundary (including beneath it or overhead) with the built asset under consideration, or that is in the neighbourhood of that built asset but physically separated by a public or private street, public or privately-owned open space or similar features.

An organisation's **supply chain** will include its professional advisors (e.g. architects and engineers), facility managers and organisations providing built asset related goods and services.

Security of digital built assets

With the adoption of building information modelling (BIM) and the increasing use of digital technologies in the management of assets, (whether buildings or infrastructure), there is a risk that loss or disclosure of asset information could impact on the safety and security of:
- personnel and other occupants or users of the built asset and its services;
- the built asset itself;
- asset information; and/or
- the benefits the built asset exists to deliver, whether social, environmental and/or commercial.

There is a need to identify and implement appropriate and proportionate measures to reduce the risks arising from such loss or disclosure. This is particularly important for protection against the loss, theft or disclosure of valuable commercial information and intellectual property.

In order to adopt an appropriate, holistic approach to the security of data and information about their built assets, the security manager and estates team need to understand what information is being created, processed, viewed and stored regarding their built assets, who has access to it and at what locations. This guidance provides information to answer questions such as:
- How would we find out if our building had been modelled?
- How do I know if a neighbouring property has modelled our assets?
- Which of our professional advisors might have digitally held information on our assets?

Questions to consider

The following questions are intended to be answered as part of a discussion between the organisation's security manager and those responsible for managing the organisation's built assets.

1. Is the built asset a sensitive asset, in whole or in part?

2. Who is responsible for providing security advice regarding the built asset and the asset information?

3. Has any security advice been sought by the project sponsor?

4. In respect of its sensitive built assets, what asset information is held by the organisation, its advisors, consultants, and/or contractors?

5. In relation to the asset information:
   a. How current is the information?
   b. Does the level of detail held present a security risk?
   c. What, if any, of the information is accessible through open or public sources?
   d. Where is it stored and processed?
   e. Is any of the data creation, use, storage or processing occurring outside of the UK, and if so where?

f. Who has access to it?

g. What access rights do they have (create, read, update, and delete)?

h. What policies, processes and procedures are in place regarding the management and security of this information?

i. What policies, processes and procedures are in place to manage access to the asset information?

6. Who is responsible for information management and information security of the asset information?

7. Where the organisation has multiple built assets, how is the asset information accessed across the organisation's estate?

8. Is any asset information created, stored, viewed or processed on handheld devices and what, if any, security measures are employed to protect it?

9. Where the asset information is held or used by advisors, consultants, and/or contractors, at what locations is the information accessible?

10. Where scans or surveys of existing assets have been undertaken:

a. Who has access to the scan data?

b. Where is it used, stored and processed?

c. How is the data transmitted between parties?

d. What measures are in place or were taken to delete sensitive data from surveying equipment?

11. Are any of the IT systems that store, process or display the asset information accessible from outside of the organisation? If so what measures are in place to prevent unauthorised access to the systems?

12. What information, if any, has been supplied to neighbouring asset owners regarding the organisation's assets?

13. Where information has been supplied to neighbouring asset owners:

a. What information was supplied?

b. When was it supplied?

c. For what purpose was it supplied?

d. What restrictions, if any, were placed on the use or disclosure of the information?

e. What protective measures, if any, were required for the information?

f. Have those protective measures been put in place?

14. Is there a built asset risk management strategy in place, which includes:

a. an assessment of the security risks to the built asset, including risks associated with the asset information?

b. agreed mitigation measures?

c. a list of residual risks commensurate with the organisation's risk appetite?

15. What information, if any, has been sought and received from neighbouring asset owners?

16. Where information has been received from neighbouring asset owners:

a. What information was supplied?

      b. Is the information, as far as can reasonably be known, still current?

      c. What restrictions, if any, were placed on the use or disclosure of the information?

      d. What protective measures, if any, were required for the information?

      e. Have those protective measures been put in place?

17. What, if any, strategies and management plans are in place and how do they align with the requirements of PAS 1192-5?

Next steps

In light of answers to the questions in this guidance, your organisation should consider whether the availability and use of asset information, particularly that which is digital, increases the organisation's vulnerability to loss of sensitive information and hostile reconnaissance. PAS 1192-5, which is available from the British Standards website, details the approach to applying appropriate and proportionate measures to manage the security risks that affect a built asset, in whole or in part, asset data and information.

If there is any uncertainty as to whether:
- any of your built asset, in whole or in part, is sensitive;
- there is a need to protect particular asset information or information about a neighbouring built asset;
- there is a need for retrospective actions; or
- particular retrospective actions are appropriate

it is recommended that you seek appropriate security advice, and apply the security-minded process set out in PAS 1192-5.

Sources of further information

Depending on the nature, use or function of your built assets, there might be a number of sources of specialist security advice available to the employer or asset owner. This advice typically covers personnel, physical and cyber security. For sensitive built assets, advice will be available from the Centre for the Protection of National Infrastructure (CPNI), the National Counter Terrorism Security Office (NaCTSO), CESG and lead Government departments.

For other built assets, e.g. a high profile commercial building, the employer or asset owner's built asset security manager, along with the police architectural liaison officer (ALO) (or in London, the crime prevention design advisor [CPDA]), who will be embedded in the Local Authority Planning Office, and where necessary, specialist security advisors (e.g. an appropriate member of the Register of Security Engineers and Specialists [RSES][1]) should be able to assess the security threats and vulnerabilities to provide appropriate professional advice on security requirements and countermeasures.

---

[1] See http://www.rses.org.uk

RSES is sponsored by CPNI. The register was established to promote excellence in security engineering by providing a benchmark of professional quality against which its members have been independently assessed. Its members are engineers, applied scientists and specialists who apply their knowledge to securing the built environment and infrastructure.