UK BIM Alliance – BIM Security Guidance

Outsourcing IT Management

Title of guidance:	Outsourcing IT management
Author:	Nathan Jones
Company:	Turner & Townsend
Email:	Nathan.jones@turntown.co.uk
Objective of guidance:	To provide a brief understanding of what to look for if procuring an IT Managed Service.

Abbreviations/acronyms	**Full name**
AV	*Anti-Virus*
BAU	*Business as Usual*
BYOD	*Bring Your Own Device*
CE/CE+	*Cyber Essentials/Cyber Essentials Plus*
NCA	*National Crime Agency*
NCSC	*National Cyber Security Centre*
SIEM	*Security information & Event management*
SLA	*Service Level Agreement*
VLAN	*Virtual Local Area Network*

Keywords:	*Outsource, security, risk*

Briefing note text

This briefing note offers a high level awareness on the considerations prior to the procurement of an IT managed service (it does not replace any guidance given by NCSC or NCA). It provides guidance on what questions organisations might consider asking a managed service provider prior to entering into a contract. A Managed IT service does not necessarily mean any risk has been 'transferred' so understanding the limits of the service is sacrosanct.

It is also important to note that this briefing note provides guidance on *baseline* measures and the assumption is that for any sensitive project, the correct advice and guidance will be sought.

As the use and reliance on IT systems increases exponentially, so does the number of cyber-attacks on organisations. Whether through ransomware or denial of service the threat to UK business is not going away; it is more important than ever to understand what IT services you are procuring and what responsibilities the managed service provider has signed up to (or not) in the Service Level Agreement (SLA).

Outsourcing IT services is becoming increasingly popular within the construction industry for a number of reasons. Similar to Cloud services, it enables the 'flexing' of resources (increase/decrease) requires little or no active equipment (servers etc.) on site and places the responsibility of the management of the equipment onto the service provider.

As ever, an SLA is generally put in place when the managed service is procured, but what should you look for? Listed below are a number of questions or points for consideration that might be asked/understood prior to engaging into a contract:

- Is the provider ISO27001 accredited?
- Is the provider CE+ accredited?
- What tier level is the data centre where the active equipment is stored?
- How often is storage 'backup' performed?
- What is the period 'backups' are kept for?
- Is there a 'mirror image' of the storage drive, if so, where is that kept?

- What is the policy and procedure of software patches (including firmware upgrades) to be applied to the system including active equipment and end user devices? How is this communicated?
- What AV and Firewall is applied and how are they managed?
- Will the service be GDPR compliant in terms of response times to data loss/threat?
- Is SIEM in use?
- If no SIEM, how is the network monitored to mitigate unknown devices connecting to the service?
- Do you have unique access to your service and how is segregation to others put in place?
- How is a 'whitelist' managed?
- Is there 24/7 – 365 days support? Where?
- Are there separate guest/BYOD networks?
- How does the provider keep current with the latest threats?
- Can the provider exercise continuous improvement?
- Has the provider ever been exposed to a cyber-attack?
- What internal staff will have access to the service?
- Are removable media devices (USB memory sticks etc.) allowed on the system?
- How are files introduced to the system?
- Are incoming emails checked for potential viruses?
- Will the system block un-known files and programmes that run on the system?
- Are device types in segregated VLANs?
- How are the VLANs managed?

As ever, it is a balance between security and business as usual; security (in terms of baseline considerations) should not hamper your day-to-day activities and working practices but it is known that cyber attackers will generally go for the softer target. An understanding of your IT systems is essential.