CILA & AIRMIC SEMINAR

Building Information Modelling

'Not Everything That Glitters is Gold'

by the CILA Construction, Energy & Engineering SIG and the Airmic Construction SIG

Speakers

Gary Holbrook, BAM
Phil Palmer, BAM
May Looi, Kennedys
John Farrell, Kennedys
Mike Skingsley, Crawford & Company

Introduction

Gary Holbrook, BAM

CILA & AIRMIC SEMINAR

Building Information Modelling

'Not Everything That Glitters is Gold'

John Farrell, Partner
Kennedys Law

Kennedys
Legal advice in black and white

BIM: As Safe As Houses?

John Farrell
Partner
Kennedys

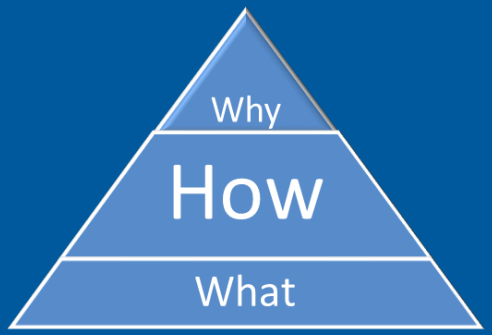
Kennedys
Legal advice in black and white

BIM – New vulnerabilities ?

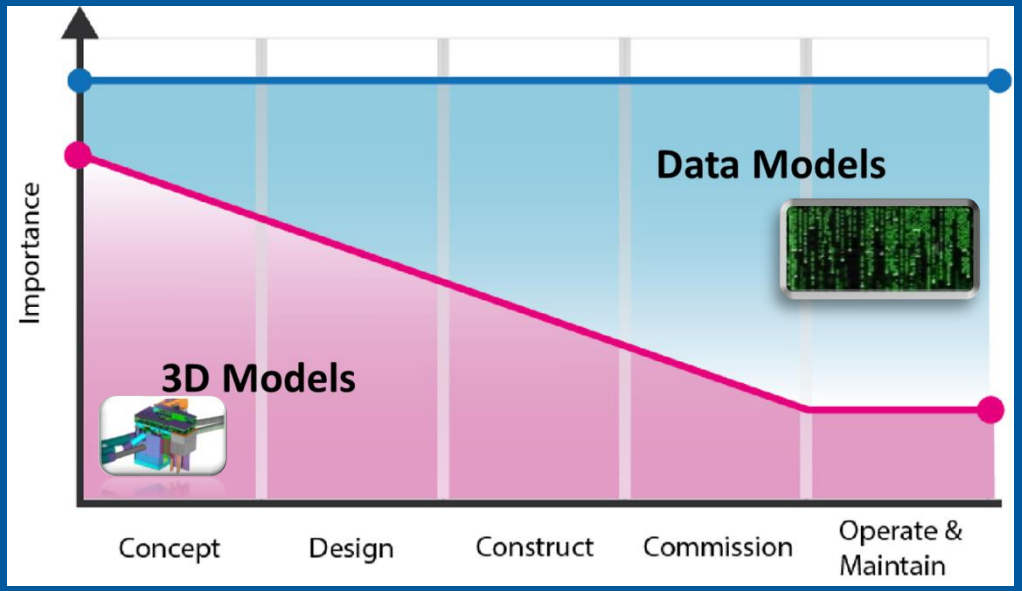
Introduction

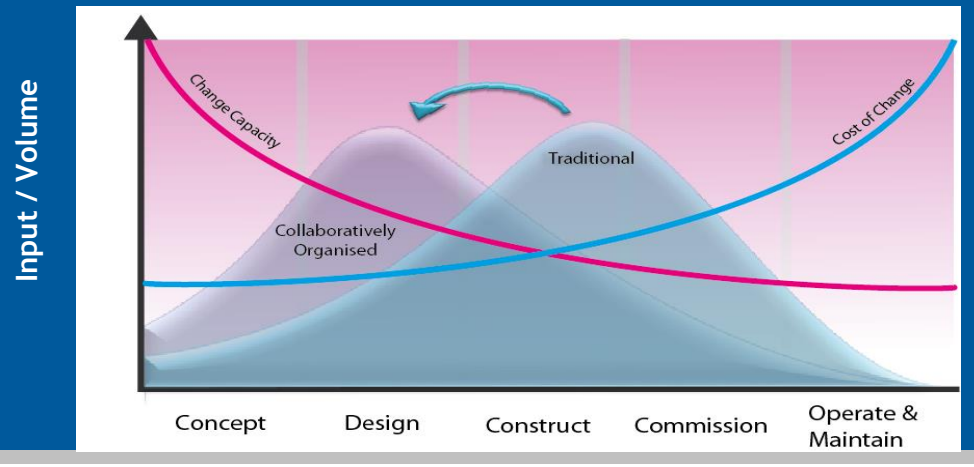
- BIM: a single network
- Common data environment shared between contractors
- Data does not stop at borders
- Described as a “Building Infiltration Model”
- Array of risks/threats:
  - Internal attacks
  - External attacks
- Leading to the compromise/loss of BIM data with consequential damage to the works, associated delay and disruption
- Potential damage to reputation/ third party claims

What is BIM: Recap



- Information
- Data environment
- Data integrity
- Collaboration
- Technology
- Asset life-cycle
- New processes
- New project culture

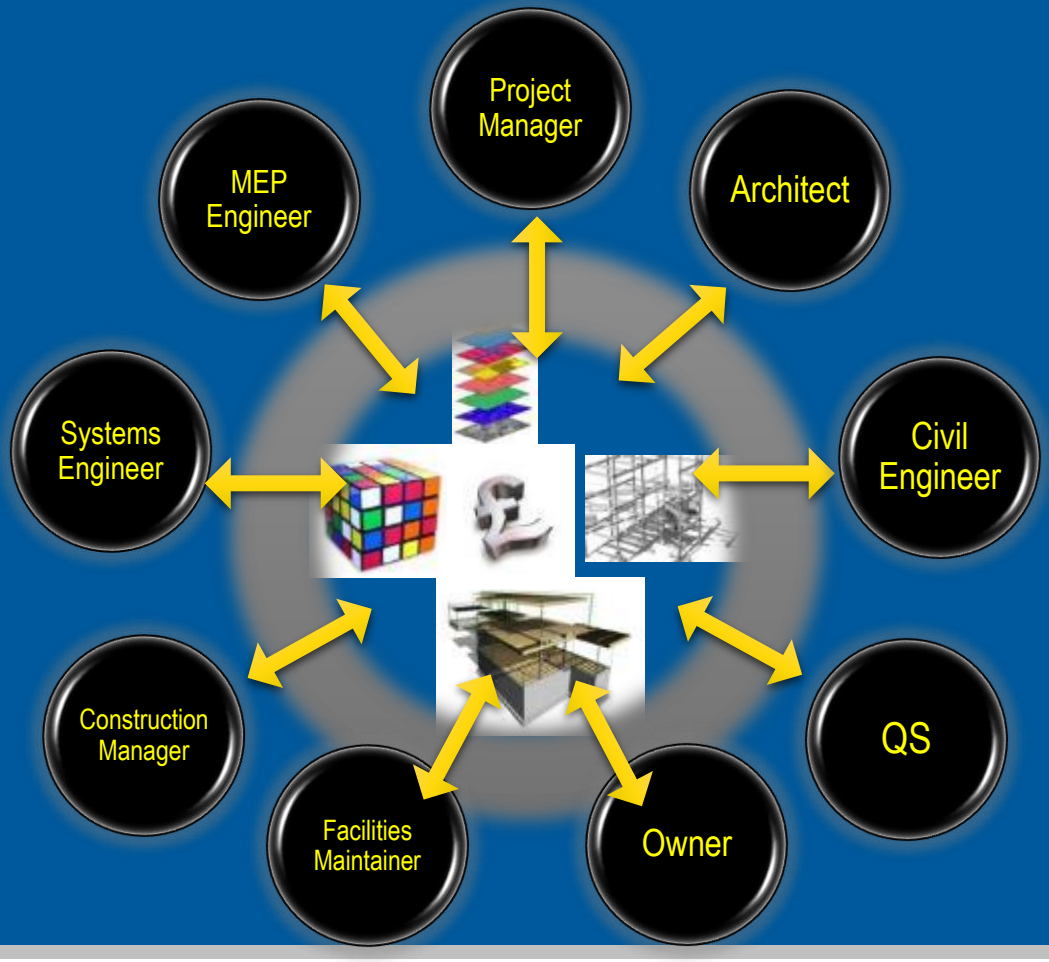




Why is BIM vulnerable to a cyber attack?

- A common data environment – held on a single network where critical data is held

Why is BIM vulnerable to a cyber attack?



- Numerous parties to the project have access to the network through various devices: desktops, tablets etc

Why is BIM vulnerable to a cyber attack?

- Once the network is compromised intruders can identify the data they want to use to carry out an attack

The Threats

- External: Intruders, Terrorists
- Examples of internal threats:
  - IT Departments
  - Suppliers
  - Subcontractors
  - Executives
  - Employees
  - Internal threats can be malicious or non-malicious: error, ignorance, negligence causing corruption/loss of data

Types of Attack

- Direct Access – e.g. through Wi-Fi or Bluetooth
- Trojans/Worms/Viruses
- Denial of service (DoS)
- Phishing
- NB: Is the Cloud safe? What happens if the data centre is hacked?

Types of Attack – Direct Access

- Direct access – involves an individual gaining access to data and misusing material.
- Portable devices are vulnerable through Wi-Fi.
- Bluetooth – is it secure?
- E-cigarettes – USB chargers were encoded with malware.

What could be compromised during a hack?

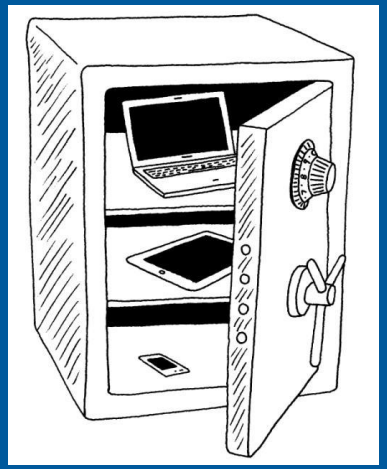
- Design Phase - Plans/drawings/specifications could be altered
  - M&E services are repositioned to cause a clash
  - Reduce load bearing capabilities below acceptable safety levels
- Construction phase - a section of the works collapses due to the design being compromised
- During testing phase - M&E services fail: electrical fault, arcing, a pump is activated to cause flooding
- Delay and disruption to project, increased costs of working, contractual penalties etc.

Hack? Post Construction/Operational period

- The network is accessed to find O&M manuals to select location for a physical attack
- Fire damage - Disable the sprinkler systems, fire alarms, thermostats
- Flooding – By ramping up the cold water booster set to cause water hammer in the top of the building/basement
- Theft - Identify the locations of the security cameras

How can you make BIM more secure?

- Assess the threats your project faces
- Have clear cyber security policies/procedures
- Educate staff at all stages of the project
- Protect the project's BIM infrastructure
- Control confidentiality/access



THANK YOU

John Farrell, Partner
Kennedys
25 Fenchurch Avenue, London EC3M 5AD
John.Farrell@kennedyslaw.com
020 7667 9108

Kennedys
Legal advice in black and white

CILA & AIRMIC SEMINAR

Building Information Modelling

'Not Everything That Glitters is Gold'

by the CILA Construction, Energy & Engineering SIG and the Airmic Construction SIG

Speakers

Gary Holbrook, BAM
Phil Palmer, BAM
May Looi, Kennedys
John Farrell, Kennedys
Mike Skingsley, Crawford & Company