OCCUPIER SERVICES

Colliers INTERNATIONAL

Accelerating success.

The Internet of Things – what could go wrong?

Understanding the Internet of Things and the implications of Cyber Security for real estate owners and occupiers.

By Kevin Burman
National Director | Technology Solutions
kevin.burman@colliers.com

Miniaturisation of electronics over the past decade has enabled sophisticated and powerful devices to emerge; today we see computers, high definition cameras, GPS receivers, radios, music players, sound recorders and telephones all combined in small hand-held smartphones that are used everywhere.

As the power of individual components has increased exponentially, their cost has reduced dramatically. Computers are being built into almost everything; the Internet of Things, "IoT" has been born.

The growth of the Internet of Things

The IoT is a rapidly expanding network of smart inter-connected computerised devices that allow us to monitor, control, better understand and improve our daily lives.

As opposed to smartphones, smart TV's, PC's and tablets, the IoT describes computers that are embedded within vehicles, security systems, environmental control systems, even household appliances, all capable of communicating with each other over the public Internet.

By 2020 there will be 10 billion traditional computers and mobile devices in the world (an average of 3 per adult!), and almost 30 billion IoT devices. The real estate sector is currently experiencing massive growth of IoT, in both corporate and residential.

Source: 'The Internet of Things' Cisco

Benefits of IoT for Commercial Real Estate

IoT devices can constantly monitor buildings and their surroundings, interacting with one another to learn and automatically control temperature, humidity, air quality and lighting levels. IoT in buildings creates a better quality environment, more productive and contented occupiers, efficient operations and cost savings. Building management systems can be inter-connected to tenants' own systems, allowing a level of control, monitoring and efficiency that has not previously been possible.

The benefits to property owners and occupiers are easy to identify; no longer do technicians need to spend time travelling to the site, connecting physically to the control panels and making manual changes to air-conditioning, power, security and fire systems. Instead, by replacing traditional proprietary systems with internet enabled controllers and sensors, these systems can be monitored in real-time and updated remotely.

The threat of cyber-crime and cyber security

Cyber security is the fastest growing sector in IT, fuelled by the rapid growth in the number of networks and inter-connected devices, the rapid expansion of products and services available over the internet, and the emergence of cyber criminals who set out to exploit any weaknesses for their own gain. Recent worldwide cyber-attacks on corporate and government computer networks have highlighted the financial and reputational risks.

There are risks for commercial real estate owners and occupiers - IoT devices in buildings are vulnerable to attack. Their deployment in large numbers, frequently out of sight in plant rooms and ceiling voids, increases the chance of being compromised. Cross-connection to centralised building management systems and corporate networks could dramatically increase the scope and seriousness of a successful attack.

Accessing the IoT devices could for example be used to set off nuisance alarms or interfere with environmental settings. More serious intrusions might result in locking out authorised users or enabling access by unauthorised visitors.

Data theft and security breaches are of particular concern to corporate and government tenants; “Trojan horse” devices could be installed in the network to eaves-drop and transmit sensitive data to remote locations.

How can you minimise the risk of cyber crime?

Given the growth of IoT and the benefits to building owners and occupiers alike, these devices will continue to be installed in ever-increasing numbers. We recommend a collaborative approach between IT and property / real estate teams to manage and control the threats posed by IoT.

Our clients are encouraged to:

1. Update cyber security policies and procedures to embrace IoT
2. Ensure that IoT devices and systems have been independently tested before installation
3. Recognise risks – conduct regular reviews, penetration tests, password changes
4. Encrypt all sensitive communications
5. Avoid cross-connecting networks and ensure physical and logical separation where possible
6. Seek specialist advice, recognising Information and Communication Technology as an essential engineering discipline.

To speak with a Colliers International expert, contact Kevin Burman, National Director of Technology Solutions today.

Kevin Burman
National Director
Technology Solutions | Occupier Services
kevin.burman@colliers.com
+61 2 9249 2079
+61 413 623 362