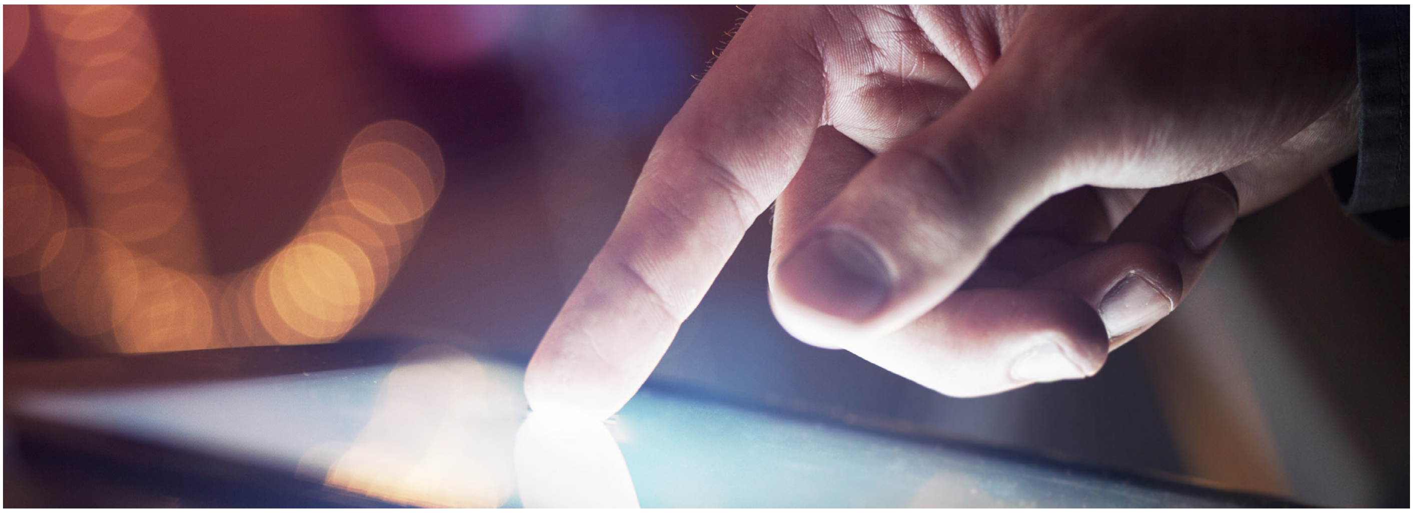

Cyber in real estate

The Commercial Real Estate sector is being transformed by technology

The rise of smart buildings is driving a rapid uptake of new interconnected technologies such as the Internet of Things (IoT), cloud and mobility. In parallel with this, the growing focus on the experience of occupants means that Construction and Real Estate companies are holding dramatically increasing volumes of regulated personal data relating to individuals.

The failure to detect and respond to security incidents could cause severe impact to the reputation of the industry, as gaining control of systems like a building management system (BMS) or building information modelling (BIM), can lead to more than just theft of data, it can also result in physical harm, safety issues or operational interruption.

What are the new tech trends?

Internet of Things: Increasingly, forward-thinking organisations are focusing their Internet of Things (IoT) initiatives less on underlying sensors, devices and smart things, and more on developing approaches for managing data, leveraging brownfield IoT infrastructure and developing new business models.

This is relevant because there is a growing desire to adopt emerging technologies for use in retail, commercial and residential development, operations and maintenance

Cyber implications: As companies put IoT to work, the smart, connected objects they deploy offer tremendous opportunities for value creation and capture. Those same objects, however, can also introduce risks – many of them entirely new – that demand new strategies for identification and value protection.

Reimagining Core Systems: Core systems that drive back, mid and front offices are often decades old. Today, many roads to digital innovation lead through these ‘heart of business’ applications. This means that there is a need for a significant adoption of new core solutions by the property industry.

Cyber implications: Efforts to reimagine the core can introduce both risk and opportunity. On the risk front, remediation efforts may add new points of attack with interfaces that inadvertently introduce issues or raise the exposure of long-standing weaknesses. Similarly, repurposing existing services can also create vulnerabilities when new usage scenarios extend beyond historical trust zones.

BMS: Building Management Systems are deployed across most office, industrial, residential and retail buildings. These computer-based control systems control and monitor the building's mechanical and electrical equipment including ventilation, lighting, and power, fire, and security systems. With the expansion of the cyber footprint and attack vectors, real estate companies are struggling to have full visibility of their connected devices - the necessary first step to protecting them from the new cyber threats and risks.

Cloud first: Increase in cloud adoption with a cloud first strategy. This means that there is a critical need to refresh your cyber strategy to take into account identity management, monitoring, data leakage and information protection across cloud platforms.

IT unbounded: As organisations modernise their IT operating and delivery models, some are creating multifunctional teams and breaking down silos across IT. This includes looking beyond organisational boundaries to explore the open talent market and form new relationships with vendors, incubators and academics. Services become 'unbounded' and more efficient, transforming the IT organisation.

Cyber implications: IT unbounded can benefit an organisation's cybersecurity through initiatives such as 'bug bounty' programs. The challenge is to manage the increased risk brought about by allowing new, external users into the wider IT environment of an organisation.

How would these trends change the threat and risk landscape?

In addition to the real opportunities garnered by these trends, the Real Estate industry is already experiencing an increase in the attack surface from potential new threats and risks. These become critical as many companies own hundreds of connected buildings through thousands of technology systems and IoT devices that collect sensitive information for their customers and operations.

Some of the main cyber threats to look out for:

IoT

- IoT based distributed denial-of-service (DDoS) attacks will continue after the success of the Mirai botnet's model, and may begin to more frequently target e-commerce sites and others that heavily depend on uptime for profitability. DDoS attacks may also serve as a diversion for simultaneous exfiltration attacks.
- The mass compromise of IoT devices will be used for financial gain in ways beyond DDoS attacks. This could mean large privacy leak incidents involving location data, camera videos and health-related information.
- Attackers may begin to exploit IoT vulnerabilities to take control of property, for example by stealing a drone or taking control of a smart car's steering wheel.

Data breaches

- Internal and external actors will contribute to the continuous and exponential rise of data breaches across different industries and countries.

Ransomware and malware

- The movement to ransomware-as-a-service (RaaS) will continue to make ransomware available to a broader range of less-sophisticated cyber threat actors, who are starting to use additional deployment techniques as malware to infect more devices infecting a broad spectrum of networks.
- Attackers will begin to use malware to take control of IoT devices and demand ransom as soon as those devices reach greater saturation in households and corporate environments.
- Ransomware attacks will become more creative as attackers identify more repositories of valuable data that they can exploit.
- Email will continue to be a highly effective distribution vector for ransomware as companies scramble to put more effective advanced threat prevention systems and employee training procedures in place.
- Encryption of data and information is no longer the only consequence of being infected. Destruction of sensitive and critical information is becoming more and more popular.
- New generation of sophisticated and specific attacks have replaced the old generic ones.

The three main risks related to the threats detailed above are:

- Theft or destruction of personally identifiable information (PII) and sensitive data
- An attack on tenants through building systems
- Destruction of physical infrastructure.

How can we address these new threats and risks?

As a starting point we highly recommend conducting a comprehensive asset discovery process to identify which systems are critical for the business, from an information collection or operation perspective. Understanding the criticality of the information that is being stored and processed by these systems is extremely important for a proper risk and threat assessment.

Once you have an inventory of technology assets and collected the necessary information you can run various cyber threat intelligence and monitoring activities to help reduce the risks of being attacked and getting your operational systems compromised.

David Owen is a Partner in the Cyber Security and Privacy practice within Deloitte Australia's Risk Advisory business. David spent five years leading information security in the UK for Europe's largest guided weapon and missile producer. David specialises in cyber security and privacy management, risk assessment, governance and strategy development in large and complex organisations.

About Deloitte

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 244,000 professionals are committed to becoming the standard of excellence.

About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 7,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au.

MCBD_HYD_02/18_55350