



Digital risks in buildings

Global

1st edition, June 2025

Digital risks in buildings

RICS practice information, global

1st edition, June 2025

Published by the Royal Institution of Chartered Surveyors (RICS)

Parliament Square

London

SW1P 3AD

www.rics.org



No responsibility for loss or damage caused to any person acting or refraining from action as a result of the material included in this publication can be accepted by the authors or RICS.

ISBN 978 1 78321 549 2

© Royal Institution of Chartered Surveyors (RICS) June 2025. Copyright in all or part of this publication rests with RICS. Save where and to the extent expressly permitted within this document, no part of this work may be reproduced or used in any form or by any means including graphic, electronic, or mechanical, including photocopying, recording, taping or web distribution, without the written permission of RICS or in line with the rules of an existing licence.

This document applies globally. If any of the requirements contained in this document conflict with national legal requirements in the country or region in which the regulated member is operating, those national legal requirements take precedence and must be applied.

Acknowledgements

Technical author

Dan Hughes (Alpha Property Insight)

Expert group

Jonathan Avery

Andy Broad (Landsec)

Linda Chandler (Digital Place Expert)

Maddy Griffiths (Information Commissioner's Office)

Mark Hewitt (Digital Property Risk)

Chris Mather (Lloyd's Market Association)

Carlo Ramadoro (Lockton Companies LLP)

Sanjaya Ranasinghe (WiredScore)

Rick Robinson (Jacobs)

Robin Stevenson (Knight Frank LLP)

Matt Taylor (Clifford Chance LLP)

RICS professional practice lead

Paul Bagust

RICS project manager

Helvi Cranfield

RICS editor

Judith Frost

Special mention

RICS would like to thank Andrew Knight for his expertise and contribution to this paper.

Contents

Acknowledgements	ii
RICS standards framework	1
Document definitions	2
Foreword	3
1 Introduction	4
1.1 Scope and application	4
1.2 Background	4
2 Digital risks in buildings	8
2.1 Definition	9
2.2 Today's scope of risks	10
3 The future	20
3.1 The wider impacts	23
3.2 Identifying responsibility for digital risks	24
4 The implications for property professionals	26
4.1 The RICS member's role in digital risks and property management	28
4.2 RICS regulation	30
4.3 Other relevant regulations	32
5 Next steps	38
5.1 Building stakeholders	39
5.2 Industry bodies	42
5.3 Governments	44

RICS standards framework

RICS' standards setting is governed and overseen by the Standards and Regulation Board (SRB). The SRB's aims are to operate in the public interest, and to develop the technical and ethical competence of the profession and its ability to deliver ethical practice to high standards globally.

The RICS [Rules of Conduct](#) set high-level professional requirements for the global chartered surveying profession. These are supported by more detailed standards and information relating to professional conduct and technical competency.

The SRB focuses on the conduct and competence of RICS members, to set standards that are proportionate, in the public interest and based on risk. Its approach is to foster a supportive atmosphere that encourages a strong, diverse, inclusive, effective and sustainable surveying profession.

As well as developing its own standards, RICS works collaboratively with other bodies at a national and international level to develop documents relevant to professional practice, such as cross-sector guidance, codes and standards. The application of these collaborative documents by RICS members will be defined either within the document itself or in associated RICS-published documents.

Document definitions

Document type	Definition
RICS professional standards	Set requirements or expectations for RICS members and regulated firms about how they provide services or the outcomes of their actions. RICS professional standards are principles-based and focused on outcomes and good practice. Any requirements included set a baseline expectation for competent delivery or ethical behaviour. They include practices and behaviours intended to protect clients and other stakeholders, as well as ensuring their reasonable expectations of ethics, integrity, technical competence and diligence are met. Members must comply with an RICS professional standard. They may include: • mandatory requirements, which use the word 'must' and must be complied with, and/or • recommended best practice, which uses the word 'should'. It is recognised that there may be acceptable alternatives to best practice that achieve the same or a better outcome. In regulatory or disciplinary proceedings, RICS will take into account relevant professional standards when deciding whether an RICS member or regulated firm acted appropriately and with reasonable competence. It is also likely that during any legal proceedings a judge, adjudicator or equivalent will take RICS professional standards into account.
RICS practice information	Information to support the practice, knowledge and performance of RICS members and regulated firms, and the demand for professional services. Practice information includes definitions, processes, toolkits, checklists, insights, research and technical information or advice. It also includes documents that aim to provide common benchmarks or approaches across a sector to help build efficient and consistent practice. This information is not mandatory and does not set requirements for RICS members or make explicit recommendations.

Foreword

Buildings are increasingly becoming more than just physical structures; they are evolving into smart, interconnected environments that use digital technologies to enhance functionality, efficiency and occupant experience. From automated lighting and HVAC systems to advanced security protocols and energy management, the integration of digital solutions has transformed the way we design, operate and interact with buildings.

This increasing reliance on digital infrastructure introduces a new set of risks that require careful management. These digital risks range from cybersecurity vulnerabilities and data privacy concerns to the potential for system failures and malfunctions that can have far-reaching consequences. These vulnerabilities pose growing concerns for building owners, occupiers and managers alike. As buildings become more interconnected, understanding and mitigating these digital risks is critical to ensuring safety, resilience and long-term sustainability.

This paper explores the various digital risks present in buildings, assesses their potential impacts and proposes strategies for managing these risks effectively in the face of rapidly evolving technologies.

Paul Bagust, Principal Head of Professional Practice at RICS

1 Introduction

1.1 Scope and application

This paper is for property professionals working on commercial properties globally. The term 'property professionals' can include, but is not limited to, commercial property surveyors, facilities managers, contractors, building managers and occupiers.

Many of the references in this paper are based on the UK market, but the themes and principles are applicable globally.

1.2 Background

The world is getting ever more digital, and as it does, professional advice in the real estate sector needs to remain in line with the latest digital trends. This includes both how advice is given and on what.

While there has been a lot written about the risk of technology to our jobs, less has been written about the risk it presents in buildings and how this is evolving.

There is little question that technology can deliver significant benefits when used appropriately and with care in buildings, but these benefits should be weighed against the potential downsides and the risks.

With the evolution of buildings from dumb concrete blocks into the smart platforms of tomorrow, technology has become woven into the fabric of buildings. Increasing amounts of data have been collected and used to inform decision-making by building users, occupiers and owners.

Operational technology (OT) – such as building management systems, Internet of Things (IoT) devices and access control systems – is becoming ever more widely adopted and closely linked with information technology (IT) – such as tenant management platforms, network infrastructure and wi-fi infrastructure.

These technologies bring many well-documented benefits, from user experience to efficiency gains and a reduced impact on the planet. However, whether in offices, retail, warehouses or residential properties, they also bring with them multiple and increasing risks.



'The UK real estate industry plays a huge part in all aspects of the economy and in the lives and businesses of millions of people.

The potential for even greater impact due to technology and data advances means that the digital footprint must be as protected as any other asset.

No new risk management methods need to be created – the solution can be achieved through greater awareness and maturity in the sector.'

Andy Broad
Head of Cyber Security, Landsec

Many of these risks simply did not exist until recently, and so today there is often a significant gap in understanding of their full scope and how to implement effective measures to mitigate them.

Large and small property companies tend to take different approaches to tackling these risks, and responsibility for the risks is often either unassigned or at best highly fragmented.

Even where these risks are considered and addressed, it tends to be on a case-by-case basis by a small number of individuals, as opposed to a system-wide approach at an organisational or building level. This is compounded by the uniqueness of each building and the ever-changing operating models and supply chains of each owner, layering additional complexity.

This is at a time when the expectations of customers, society, governments and regulators are all rising. Property standards are also evolving, and the way that professional judgement is applied, and to what, is changing day by day, driven by the adoption of technology.

Increasingly, legislation, regulations and voluntary standards that were originally targeted at the technology sector are imposing obligations on property businesses. Standards around cybersecurity, data privacy or technology products all now need to be considered in the context of their applicability to buildings.

**27% of respondents
said their building
had experienced a
cyberattack in the
past 12 months.**

RICS UK Facilities
Management Survey 2024

Cybercriminals are becoming more sophisticated, and the range of potential cyber-threats to buildings is expanding. Attacks on critical infrastructure, such as ransomware targeting building systems, denial of service (DoS) attacks and data breaches, are becoming more common.

The effects of digital risks are not limited to the digital world; they can have a material impact on building operation, health and safety, income and building value. These risks can often be relatively simple and inexpensive to mitigate in advance, whereas they are often difficult and expensive to deal with after an incident occurs.

There is little indication that the pace of change will slow anytime soon. The rising capability of AI is well documented and is allowing previously inconceivable use of data and technology to be within everyone's grasp.

In fact, by nearly every measure, the pace of change is expected to accelerate, making any delayed problem exponentially more challenging to address in the future.

In short, it is inconceivable to imagine a world where technology will not continue to pose a growing risk to a building's operation. It is equally inconceivable that the management of digital risks will not be needed as a service in the future.

This paper explores how the risk profile of buildings is evolving due to technology, the implications for property professionals and suggested next steps.

'The property industry is a sleeping giant in the world of cybersecurity risks.

We need to be more aware of the risks, how we can limit them and how we deal with them.

We need to have stronger and more robust security controls in place to protect our assets, clients and occupiers.'

Robin Stevenson
Partner, Knight Frank LLP



2 Digital risks in buildings

2.1 Definition

It is helpful to start by defining risk. According to the [Cambridge Dictionary](#), a risk is ‘the possibility of something bad happening’, and according to the [Institute of Risk Management](#) (IRM), a ‘risk can be defined as the combination of the probability of an event and its consequences’.

Generally, in the built environment there are many standards for data and technology (see [section 4](#)), although these are rarely aligned with each other. With regard to digital risks, property professionals tend to be reliant on applying a novel interpretation of existing principle-based standards, or transposing standards from outside the sector.

This paper will therefore consider digital risks in the broadest terms, i.e. the possibility of ‘something bad happening’ with or because of anything digital. This paper will also limit its scope to where the digital risks specifically impact on the effective operation of a building.

Without proactive technical management, buildings face escalating complexity and risks.

The convergence of new technologies and diverse stakeholder needs creates a challenging landscape.

However, a secure and technically well-managed building unlocks opportunities for faster integrations, lower running costs and increased flexibility.

Jonathan Avery

former Head of Technology and Data, Legal & General

2.2 Today's scope of risks

Technology in buildings is widespread. From wi-fi networks to smart sensors, there is now a digital element to the fabric of every building – some tangible and some not. This paper considers the digital risks through a range of different lenses, to allow them to be explored accurately. It should be noted that the lenses identified are not discrete, and for any one item there may be several risks. For example, a piece of hardware may depend upon software, may collect data and may be connected to a network.

To further complicate things, buildings are the product of complex supply chains, established over many years from a huge variety of suppliers and providers. Even if individual suppliers are working to best practice when it comes to minimising digital risks (and this should not be taken for granted), problems are even more likely to arise when risks are considered at a system level.

An individual piece of technology may be adequately secure, but not necessarily when used in conjunction with other technology. This additional risk is more likely to be the direct responsibility of those owning and managing the building, and therefore the way that all technologies work together should be considered – so-called [systems thinking](#).

It is helpful to map out all of the digital systems and assets within a building to identify who has legal responsibility for them at both an individual asset and a system level, including the connections between different assets that may be the responsibility of different parties.



2.2.1 Hardware

Hardware refers to the physical elements of technology related to the operation of a building. Examples include wires, computers and sensors. It may also be extended to a network of connected devices, often referred to as the Internet of Things (IoT). At its simplest level, there is a risk that the hardware stops working, and there are a number of examples where this may be seen, such as the following.

Copper wires

Since the 1990s and the birth of the World Wide Web, there has been a growing need for buildings to be connected to the internet. For years, this has been via wires, but some of the wires that have been in place for many years are becoming unsupported.

Example

In the UK, copper phone lines are gradually being phased out in favour of fibre optic connections. This transition is part of a nationwide shift to modernise telecommunications, driven by [Openreach](#) (a subsidiary of BT), which plans to switch off the public switched telephone network (PSTN) as Full Fibre is rolled out.

Sensors

Sensors are increasingly used in buildings to collect data to inform decision-making. However, sensors only have a finite lifetime. This does of course depend on the type of sensor, the environment it is used in and how it is maintained, but it would be wrong to assume that sensors can continue indefinitely.

Example

Most indoor sensors typically have a life expectancy of around 15 years, although this is not always the case.

A desk occupancy sensor may only have a lifetime of up to nine years.

Building access

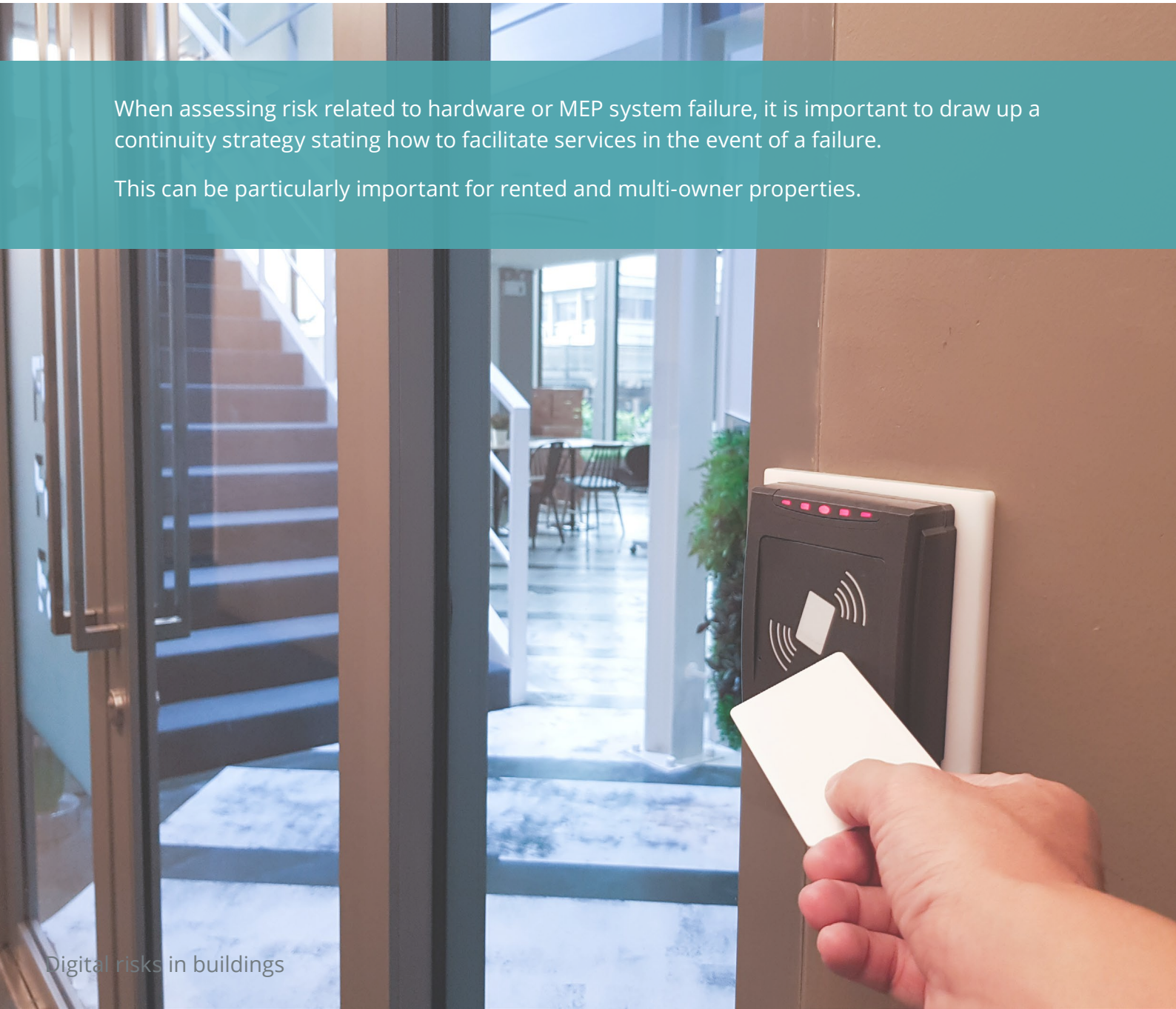
Technology is often used for access to a building or part of a building. Should this fail, access may become either too easy or impossible.

Example

According to [media reports](#), in October 2021 an outage left Facebook employees unable to access their office building due to the outage affecting their security passes.

When assessing risk related to hardware or MEP system failure, it is important to draw up a continuity strategy stating how to facilitate services in the event of a failure.

This can be particularly important for rented and multi-owner properties.



2.2.2 Software

Ultimately, buildings are largely dependent on software to run effectively. Whether mainstream software or a mobile phone app, software needs supporting and regularly updating.

This is part of everyday life now, with laptops and mobile phones regularly carrying out automatic updates, but manufacturers only support this process for a finite length of time.

Given the combination of the multitude of suppliers and the long lifespans of buildings, it is likely that software in a building may cease to be supported or may not be updated appropriately.

It is helpful to keep a record of when key software will become unsupported (if known), in order to plan ahead and ensure continuity of service provision.

Obsolete systems will not receive security upgrade patches, creating a vulnerability. Resources are available to help provide this information, for example endoflife.date.

Example

A building that opened in 2013 would still be considered by most as a relatively new building. It is quite feasible that a building of this age would be reliant on Microsoft Windows 7 software.

However, Microsoft stopped selling this software in 2014 and it has not been supported since the start of 2020. If there are no updates or support for the software, the building and its users may be left at risk.

2.2.3 Data

Technology collects data, and data requires careful management. The most crucial elements to consider are personal data and privacy. According to RICS' [Data handling advice](#):

'Depending on your business, your surveying firm may collect various types of data from different sources.

You might collect personal data from:

- employees
- clients
- prospective clients
- tenants of properties you manage or
- third parties involved in matters where you are providing a service.

Personal data is any information that can identify an individual, including name, address, date of birth, etc. as well as images captured on photos or CCTV. It also includes reference numbers; for example, if you allocate case numbers to individuals you work with/represent.'

However, even when information has had identifiers removed or replaced in order to pseudonymise the data, it can still be considered personal data. Sometimes assessment can be complex, particularly when a combination of information and datasets means that anonymised data from a building can actually be personal data when considered as a whole. The Information Commissioner's Office (ICO) provides detailed guidance on how to identify personal data. Note that data from buildings may be collected and stored on site ('on-prem') but also elsewhere, such as in data centres or 'in the cloud'.

Personal data is covered by the [UK General Data Protection Regulation \(UK GDPR\)](#), the UK-specific version of the GDPR legislation used in Europe. Some personal data requires even more careful handling under the legislation. '[Special category data](#)' needs extra protection due to the higher potential for detriment if this data is accessed, used or otherwise disclosed unlawfully. The ICO also provides [guidance](#) on processing biometric data, which some buildings collect through, for example, door entry systems.

It is also important to consider commercially confidential or sensitive data collected from a building, that may not be considered personal data. This can theoretically extend to data that is relied on in the market to make decisions about a building.

If market data, footfall or air quality data were to be manipulated, could this influence customer decisions or the valuation process? If so, with whom does responsibility sit regarding third-party data that might influence a building's performance?

Example

A number of companies have been reprimanded for improper use of facial recognition technology (FRT) that risked breaching data privacy rules.

In 2019, a developer was reported to have been investigated by the Information Commissioner for the use of FRT at its [King's Cross development](#), and in 2022 a privacy rights group complained to the Information Commissioner about the installation of FRT in [retail stores](#).

The management of data and legal requirements is a fast-moving topic.

In the UK, for example, the [Data \(Use and Access\) Act 2025](#), which provides a range of changes that may affect the property sector, was announced in October 2024 and received Royal Assent in June 2025.

The owners of some real estate assets also now have to comply with the [Digital Operational Resilience Act \(DORA\)](#), a European regulation aimed at strengthening the digital operational resilience of the financial sector.

2.2.4 Cyber

Strictly speaking, the term 'cyber' can refer to anything related to computers, so all of the risks discussed in this paper may be considered as cyber-risks. However, more commonly it refers to the proactive risks of malicious activity or 'cyberattacks', and for the purpose of this report it is through this lens that cyber-risks will be considered. According to [IBM](#):

'A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.'

As buildings become more dependent on technology and their 'attack surface' (the number of possible points, or attack vectors, where an unauthorised user can access a system and extract data) grows, this should become an increasing priority for those responsible for managing a building.

In theory, anything that is dependent on technology to operate effectively might be the subject of an attack. Every building is unique, but some examples to be aware of are the following.

Building operation

As buildings increasingly depend on technology, those technology systems are vulnerable to being accessed and manipulated by a malevolent third party. If fire risk in a building is addressed by fire suppression systems, evacuation elevators and fire alarm systems, and these were prevented from working, the building could become significantly higher risk. Similarly, if these systems were accessed and activated, major disruption could be achieved if the alarms or sprinkler systems went off unnecessarily.

An extension of this scenario is where a building's systems are accessed and held to ransom. Organisational ransomware has become a familiar story, but if malevolent actors were to access building systems, the building itself could be held to ransom, potentially preventing doors or HVAC systems from working, triggering alarms or exploiting other operationally critical technology.

Example

In 2023 hotel chain MGM Resorts was reportedly hit by a [cyberattack](#) that shut down a number of its systems, including its room access, preventing customers from entering their hotel rooms because the digital keys malfunctioned.

Personal or corporate espionage

As mentioned above, the building itself may be targeted to prevent its effective operation, but today it is more common for a building to be attacked as a means to an end, either to gather information on a company or to attack its corporate systems.

Directly targeting up-to-date and highly sensitive systems is often challenging, but accessing them indirectly via another less-protected connected platform is often much easier.

Several building applications or smart devices can be targeted to attack an organisation's broader systems. There are a range of examples of this, with HVAC systems, smart fish tanks or even smart kettles being used to gain access to corporate information.

Buildings might not be used just for access to corporate systems, but also to monitor activity within them. For example, accessing registers of building users for personal information, intercepting documents sent to printers and gaining remote access to cameras are all methods that can be used to gain useful intelligence.

It is not just remote access that is a concern. Most office workers will be familiar with entrance signs warning of 'tailgaters' – unauthorised users walking through an otherwise restricted access door straight after someone uses their entry pass card.

However, it is now relatively easy and inexpensive to purchase devices that allow many of the commonly used access cards to be cloned (copied and then replicated later).

This means that instead of needing to follow a person through a door, just a brief exposure to their security card may be enough to allow full access to a building. Smart phone apps and wallet credentials are also vulnerable.

Another more advanced example involves a seemingly ordinary USB stick that, when plugged into a computer, can deceive the system into recognising it as a keyboard.

Once this is done, the 'keyboard' can type anything that it has been pre-programmed to type, giving the computer instructions to do anything that can be instructed from a normal keyboard. This could include forwarding emails and sharing screen grabs.

Most people would be wary of plugging in an unfamiliar USB stick, but this is not always the case. Another type of attack that is emerging is 'juice jacking', where public USB charging ports are used to steal data from or install malware onto a device.

Examples

US retailer Target was the victim of a large data breach when malware was used to steal data on around 40 million debit and credit cards. [Reports](#) revealed that the hacker's entry point was through the retailer's HVAC supplier, which highlights the vulnerability of online systems.

Meanwhile, in 2022 the FBI alerted US businesses to a rise in cyberattacks where hackers were posting USB sticks to victims that, when installed by the recipient, were able to [gain unauthorised access](#) to corporate systems and networks.

Perhaps one of the earliest, and most extreme, examples of a reported cyberattack on a building is [Stuxnet](#) – a computer worm believed to have been used to cause damage to nuclear installations in Iran.

Deepfake

Emails purporting to be from someone they are not are commonplace, and are often referred to as 'phishing' when used for the purpose of tricking someone into revealing information or taking some action.

However, as technology becomes more capable and cost-effective, it is becoming possible to achieve the same outcome in more sophisticated ways. For example, instead of sending an email impersonating an employee's manager, a phisher may now create and use a realistic voice or video message based on publicly available materials and, increasingly, even participate in real-time conversations. These are often referred to as deepfakes, and property professionals should be aware of what is possible with technology and how it can be used to trick people into taking actions that they should not.

Example

In May 2024 it was [reported](#) that an engineering consultancy firm had been 'the victim of a deepfake fraud after an employee was duped into sending HK\$200m (£20m) to criminals by an artificial intelligence-generated video call.'

An employee had been tricked into transferring the money via a hoax call from people 'posing as senior officers of the company' using fake voices and images.

Phantom cyberattack

Perhaps the easiest attack of all is the one that doesn't actually happen. If an attack is threatened, how does anyone know whether to take it seriously or not? And if it is assumed to be real, how far should an organisation go to mitigate it?

If an office property manager receives an anonymous message in the middle of winter stating that the building has been hacked into and all heating is going to be turned off, wi-fi prevented from working, lifts halted, doors stopped from opening and alarms triggered every ten minutes, what would they do? It is impossible to act confidently without having a clear view of whether the building has in fact been compromised. If this confidence is not possible, then all a malevolent actor needs to do is to be considered credible to cause significant disruption.

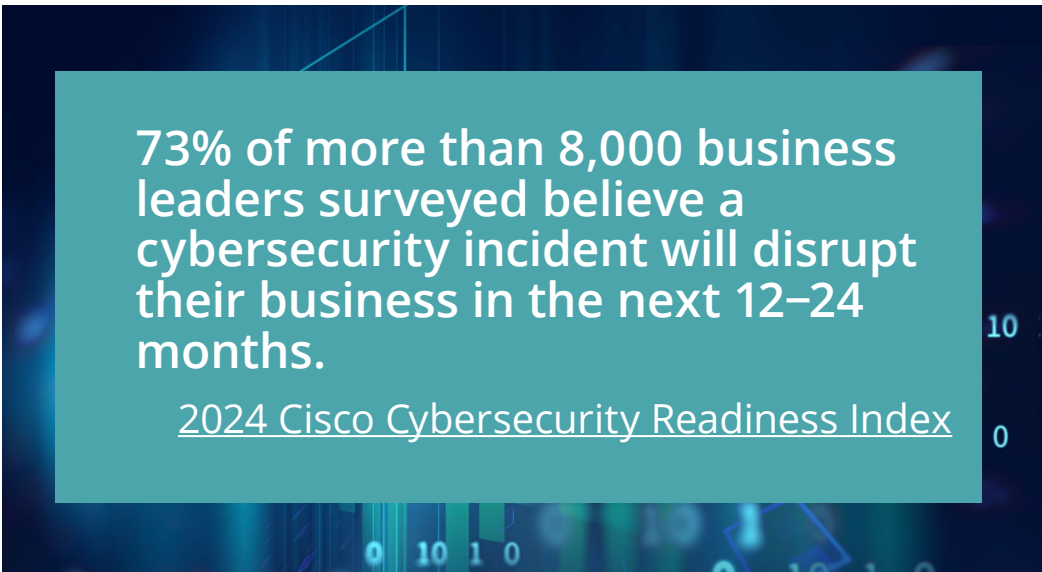
2.2.5 Networks

Typically, most of the hardware and software that is used in a building needs two things to operate: power and access to the internet, for example via fixed wire or wireless networks, including mobile networks such as 5G. At the most basic level, ensuring there is sufficient power and bandwidth available for the ever-increasing number of devices being connected to a building is essential. Not doing so can lead to buildings working ineffectively, incurring higher costs that could potentially outweigh any savings from the use of the device in the first place.

Networks need to be managed and separated, not only physically but also virtually. Core networks for essential systems like security (access control and CCTV) should be segregated from those used for providing guest wi-fi and digital signage. Even where networks are physically separated, additional steps should be taken to secure them, including physical labelling of equipment (especially if different networks are within the same physical space – even if the rack is secure), port isolation, media access control (MAC) address filtering, device tagging, virtual local networks (VLANs) and secure remote connections via virtual private networks (VPNs).

However, beyond capacity issues, both power and network access can be compromised, whether intentionally or otherwise. Utility cables may be interrupted by roadworks outside of the building itself, and a building can rapidly become unusable due to circumstances beyond the property manager's control. This requires a contingency plan, such as the provision of an alternative power source or the installation of secondary internet access.

In addition to this, both copper wire networks and 3G networks are in the process of being retired, causing buildings, or technology within buildings that are reliant on them, to cease to function. While this can typically be rectified in advance with sufficient warning, if there is insufficient tracking and awareness of which systems exist within a building, significant disruption can be caused.



73% of more than 8,000 business leaders surveyed believe a cybersecurity incident will disrupt their business in the next 12–24 months.

[2024 Cisco Cybersecurity Readiness Index](#)



3 The future

Forecasts about future processing power, connected devices and data collection all suggest a continuation of the recent exponential growth for many years to come.

While this growth is exciting and is likely to add value to the real estate sector, it also means that whatever risks buildings face today will most likely be bigger, faster and more complex tomorrow. This in turn means that the likelihood of something going wrong, the impact when it does happen and the complexity of mitigating it will all grow.

Beyond the growing availability and capability of technology, there are other trends that are likely to drive digital risks in buildings up the agenda across business, government and society as a whole.

Building flexibility

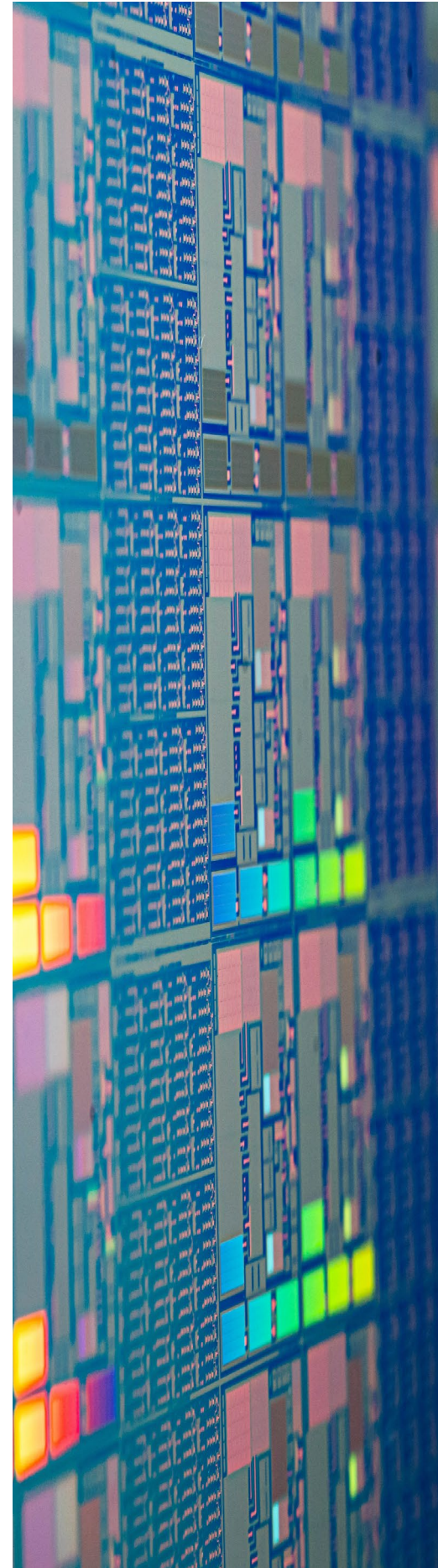
The world is changing, and buildings need to become more flexible. Much of this flexibility relies on technology, and so we can expect the adoption of technology in buildings in the coming years to grow rapidly.

Customer expectations

The use of technology in most buildings is now expected, and this expectation will continue to rise. This may include using building-specific technologies, for example downloading apps, but it is likely that the focus will be more on creating frictionless customer experiences in the building that are short-lived and temporary interactions. As costs are reduced and people use more technology day to day, buildings will need to become more connected and 'smarter', embracing more and more use cases of technology – both in the building's own interpretation and also to enable occupiers' own uses.

Systems thinking

Technology enables more joined-up management of a building. For example, managing heating, ventilation, automated blinds and air quality together can provide optimum performance, with significant benefits for a building's operation compared to dealing with each in isolation. While connecting systems is positive news for performance, it increases the risks of cyberattacks spreading more widely and also of unexpected interactions between systems. As buildings become more joined-up and system-led, so too grow both the size and



likelihood of digital risks, especially where these services are delivered by different providers in each building, leading to a plethora of bespoke cross-silo configurations.

Legislation/standards

New legislation and standards are appearing related to future digital risks and the need to manage them.

– Property legislation/standards

Increasingly, data and technology are part of the built environment. The need for a 'golden thread of information', as determined in the UK for building safety, is just one example where there is a growing demand for data on buildings to be managed.

The current edition of RICS' [International Building Operation Standard \(IBOS\)](#) clearly states some of the areas of performance for which data should be collected.

– Technology legislation/standards

There are huge amounts of legislation and standards emerging that are not aimed at the property sector but that may affect it. Some examples of these are detailed in [section 4](#) of this paper.

Different jurisdictions often take different approaches to technology regulation, which means that any solutions need to be appropriately localised.

Technology to understand technology

Digital systems collect and store increasing amounts of data, but this can be of such a volume and complexity that it can be hard to make sense of it. Analysing and using data will be increasingly reliant on yet another layer of digital systems, including AI, and this will lead to a greater focus on understanding how a building is operating and the risks that it faces.

Awareness

It is now common to hear or read about phishing attacks, ransomware demands and deepfakes across media and in the workplace. Consumers, customers and staff are more aware of the risks of technology in their everyday lives and in their work, and there will be a growing expectation that companies are also aware and taking these risks seriously.

There are many reasons why in the future we can expect to see a significant focus on the digital risks within buildings.

Today the world has many competing priorities. However, building stakeholders are faced with two stark choices: ignore the digital risks in buildings until there are more high-risk examples in the market and hope that they are not the victims, or get on the front foot today when it is significantly easier and cheaper than it will be tomorrow.

3.1 The wider impacts

Beyond the direct impact of digital risks on the operation of the building or its users, there are additional considerations, including the following.

Insurance

Traditionally, a property owner has building insurance, a property professional requires professional indemnity insurance and occupiers source their own insurance policy to protect them from business interruption, occupier's liability and other risks. It is easy to assume that these insurance policies appropriately cover new risks such as those mentioned above, but that may not necessarily be the case.

According to a 2023 [Financial Times](#) article:

'Underwriters have put tougher exclusions on standard cyber policies for major state-backed cyber attacks, meaning such events will not typically be covered... Meanwhile, property insurers have sought to explicitly exclude cyber coverage from their policies covering businesses.'

New specific policies may be required to adequately address the relevant risks, and even where existing policies may provide protection, insurers are increasingly likely to require further evidence that digital risks are being considered and appropriately mitigated.

Reputation

Occupiers and end users of buildings are increasingly mobile and are more likely than ever to take action if they lose trust in the buildings or businesses they use. A corporate occupier who suffers a data breach through improperly updated building systems is likely to avoid taking space in other buildings owned or managed by the same owner/manager.

A retailer may face reduced footfall if the shopping centre in which they are located is seen as invading privacy through the improper and intrusive use of facial recognition technology. There have been many cases of this in recent years, and while there is not significant quantitative evidence yet about the financial impact, there is little doubt that an organisation's income or share price could be negatively affected.

Building value

Insufficiently managed digital risks can affect the ability of a building to operate effectively, increase operational costs, reduce income and damage brands. All of this will affect property value. In a similar way to a 'brown' discount being applied to environmentally inefficient buildings, properties that are poorly connected, with outdated and improperly maintained systems, may attract a similar 'digital discount'.

As the link between digital risks and building value becomes clearer over the coming years, it is expected that those buying, managing and selling buildings will pay increased attention to this topic.

AI

The application of AI is not so much a new or discrete risk, rather an amplifier of other risks identified in this paper. The deployment of AI, for example in monitoring environmental systems, can create a 'black box' scenario where the basis for an output or action cannot be easily understood. Other considerations when it comes to AI might be whether the training model was based on proprietary data or whether datasets were ethically compiled. These should all be considered in the use of technology in buildings at all times, but with the use of AI, they can become more important, more complex and more opaque.

3.2 Identifying responsibility for digital risks

Today, there seems to be a broad acceptance of the existence of digital risks, but there is less consideration of who takes responsibility for them. Indeed, there is often an assumption that because they are relatively new risks, responsibility lies elsewhere.

There are high-profile examples from history where the real estate sector has not taken sufficient responsibility for certain issues or risks that have then gone on to have catastrophic consequences. It is important that the sector learns from this and recognises the need for accountability where risks have been identified.

A typical property management agreement would require the manager to manage the building to the standard of an experienced manager, having regard to the principles of [property agency and management](#) and relevant professional codes of conduct, e.g. the [RICS Rules of Conduct](#).

As set out in [section 4](#), professional codes already cover at least some digital risks, and these may evolve over time. In addition, a management agreement may include specific services requiring appropriate monitoring and maintenance of building systems, and it is open to the parties involved to specifically address the topic of digital risk.

However, it is important to give consideration to the potential responsibility of all the various parties involved, including owners, managers and tenants. Contracts can be outdated and may not cover new technology and its interconnectivity. It can therefore be unclear where the responsibility to maintain a secure building sits, especially when addressing the connectivity between the building infrastructure and the tenant systems.

For example, a large commercial building might have offices, hotels and restaurants as different tenants, all very different businesses with very different potential risks. If one of the restaurant's systems is hacked, by virtue of connectivity the malware could spread into the rest of the building, affecting all the other businesses.

Technically, it is likely to be the owner's responsibility. However, the malware only got in through the malpractice of one of the tenants, so liability may be unclear.

In practice, it is likely that in many buildings, digital risks are not really considered in any detail during contractual negotiations, and even when they are acknowledged, they are assumed to be the responsibility of someone else or, if all else fails, covered by an insurance policy – two assumptions that are not necessarily correct. As mentioned above, it is dangerous to assume that an insurance policy has all digital risks covered. Therefore, defining best practice and then clarifying responsibility for the digital risks is essential.

'We go to great lengths to design or curate the experiences buildings and places create for residents, tenants and visitors.

But those experiences are increasingly mediated, augmented or disrupted by digital technologies that to a significant degree end users choose for themselves – and that third parties often provide.

The challenge for placemakers and the property sector is how to incorporate this digital ecosystem into our design process and operational practices so that we harness the capability of digital to achieve the outcomes we set out to achieve.

If we don't, the outcomes are not likely to be what we expect!'

Rick Robinson

Director and Global Principal for Connected, Secure & Smart Places,
Jacobs



4 The implications for property professionals

In this new digital world, it is essential that the sector looks again at buildings, the way that they are managed and used, the role of property professionals and the standards that apply with a fresh pair of eyes.

For example, the standard of good estate management and what would be expected of an experienced manager will evolve over time, and may already include ensuring that an appropriate digital risk strategy is in place. In the absence of express agreement, there is likely to be significant disagreement as to who should take responsibility and the extent of any duty. As buildings evolve and more technology and data are used in the operation of a building, who is responsible for these new aspects?

Clarity and agreement on who is responsible for what is critical. In time, new roles will evolve or existing roles will take on new responsibilities. Perhaps an example of this may be phone systems, traditionally managed by the facilities team, today more often managed by the IT team.

[Section 4.1](#) will look at some of these themes and what RICS standards and guidance say about the responsibility of RICS members regarding digital risks in buildings. [Section 4.2](#) will then look at an example of a recent RICS Disciplinary Panel hearing, and [section 4.3](#) lists other relevant regulations.

'In the same way that telephony came over from FM to IT as it became IP-based, the transition is now happening with buildings.

We need to ensure that we are skilling up for the converged FM/IT department to provide a modern way to manage assets.'

Linda Chandler
Digital Place Expert and BRE Trustee

4.1 The RICS member's role in digital risks and property management

A starting point for understanding the role of the RICS member in managing digital risks is to explore how the topic is covered in [RICS standards and guidance](#). RICS has published standards for many years, and some, although they were published at a time when digital risks in buildings were less commonplace, are still relevant to the subject.

It can be expected that RICS standards will increasingly address digital risks directly, both when RICS is updating any existing standards and in any new ones where guidance is required. However, today there are a number of elements relating to digital risks covered by existing RICS standards.

4.1.1 Duty to manage building systems and digital infrastructure

RICS members working as property managers are responsible not only for the physical components of a building but also the digital infrastructure, which includes hardware, software and network systems. This responsibility is part of maintaining the integrity, safety and operational efficiency of the building.

- 'Many buildings now have a building management system – in effect, an IT system to operate the building. It is the property manager's responsibility to ensure the system is operating properly and is maintained regularly, not least because the system will be a key part of ensuring compliance with the regulatory obligations applying to the building.'
[Commercial property management in England and Wales](#) (2nd edition, 2011) p. 16
- 'Building operation is becoming ever more technology- and data-driven. IBOS is a data-driven framework that provides a standardised understanding of a building's operation; however, it is also important that the digital risks to the building and users are considered, and that the data collected is used in an ethical way.'
[IBOS](#) (1st edition, 2023) p. 26
- 'Responsible businesses need to understand... the most appropriate effective and efficient technologies to capture, collate, interpret, store and communicate the information they collect so that it can be used to inform responsible decision-making.'
[Responsible business: A framework for real estate management](#) (1st edition, 2021) p. 12

4.1.2 Responsibility for digital risks

The operation of a building and the well-being of its occupants extend to the digital realm, where compromised systems could lead to severe risks. RICS members should consider these risks, ensuring that they appropriately identify and manage them and that appropriate insurance cover is in place for themselves and their buildings.

- 'A professionally managed building should aim to have a documented register of the largest digital risks it faces, and the steps that can be taken to manage them.'
[IBOS](#) (1st edition, 2023) p. 26
- 'Firms **must** have appropriate cyber security in place to protect theirs and their client's data.'
[Property agency and management principles](#) (1st edition, 2024) p. 14
- '[RICS members] should be sufficiently skilled to inspect and report on all aspects of the property; this should include appropriate knowledge of building technology and pathology.'
[Planned preventative maintenance of commercial and residential property](#) (1st edition, 2022) p. 15
- 'Members and firms understand the risks and benefits of using relevant technology. Members and firms check that all data used is accurate and up to date, is kept securely, and that they have proper legal rights to use it and, where required, share it.'
[Rules of Conduct](#) (2021) p. 4
- 'Firms **must** ensure that they have adequate and appropriate indemnity cover for the work that is undertaken.'
[Property agency and management principles](#) (1st edition, 2024) p. 14

4.1.3 Data management and privacy

The collection, storage and use of data is increasingly part of building management. RICS members are responsible for ensuring data privacy, minimising the risk of breaches and managing data responsibly in line with regulations.

- 'Members and firms **must** handle personal data sensitively and process it in accordance with data protection legislation and their published privacy notice.'
[Property agency and management principles](#) (1st edition, 2024) p. 14
- 'The DO [demand organisation] should be open if data is out of date or inaccurate, agree assumptions if appropriate... and ask all bidders what additional data they require.'
[Procurement of facility management](#) (1st edition, 2020) p. 16

- 'Responsible businesses need to understand: what data and information are important to them and their stakeholders [and] how best to utilise information to support learning and improvement within the organisation, supply chain and customer base'

[Responsible business: A framework for real estate management](#) (1st edition, 2021) p. 12

In summary, RICS standards and guidance suggest that digital risks, including hardware, software, data privacy and cybersecurity, are an important part of building management.

RICS members have a responsibility to address these risks proactively. Ignoring digital risks may not only undermine building safety and operation, but also expose members to liabilities and potential breaches of RICS standards.

Providing adequate security measures, clear communication with stakeholders and appropriate insurance coverage are critical steps in fulfilling these responsibilities.

4.2 RICS regulation

Digital risks in buildings are a relatively new topic. From a regulatory perspective, each case is dealt with individually, so it is impossible to say how an RICS Disciplinary Panel would approach a case involving digital risk management. However, it may be instructive to look at a recent example of a hearing on health and safety and draw parallels with that.

In 2023, there was an [RICS Disciplinary Panel hearing](#) for a global commercial real estate company about their failure to act with due skill, care and diligence at the Mander Centre in Wolverhampton.

Tragically, this followed the death of a member of the public in 2017, which had led to an inquest at which the firm was found to have not 'identified all structures which needed to be considered, reported upon and maintained' nor 'to conduct a suitable and sufficient risk assessment', nor 'devise, implement and properly manage an effective system to ensure that all areas of the building... had been identified and were subject to routine assessment/ inspection and maintenance as required.'

The firm had been fined [£1.3m](#) for health and safety breaches and was then subject to the RICS Disciplinary Panel hearing. While the panel accepted that 'there was no deliberate wrongdoing or recklessness... The incident and its tragic consequences had arisen because of oversight/omission', it found both charges proved. In its decision on sanction, the panel went on to state, 'Ultimately, it was the responsibility of the Firm to ensure its future compliance with RICS standards'. The firm was fined a further £200,000.

In large part, the panel's findings were more about the lack of systemic identification of the risks or raising these with their client than the lack of maintenance that subsequently followed. In this case, it was felt that the property manager should have understood the risks and raised them with their client.

Modern buildings are no longer just "bricks and mortar" or "glass and steel" but should be seen as complex hardware, with interdependent physical and electrical components and a variety of operating systems.

We readily accept and demand that the phones we have in our pocket need a robust approach to cyber-security and data security, yet little thought is given to the buildings we occupy on a daily basis.

Increased automation and sophistication within buildings will bring occupiers many advantages but also create more opportunities for bad actors to exploit.

Property owners need to engage with these risks and create well-thought-out and practised policies and procedures designed to protect those who own and use buildings. Appropriate diligence needs to be carried out when acquiring properties to identify risks and put in place appropriate mitigation.

As the real estate industry increasingly embraces an operational approach to property, and brand identity becomes more important, the reputation of a building's operator is a key asset. It will only take one incident to cause significant harm to investment value.'

Matt Taylor
Partner, Clifford Chance LLP

4.3 Other relevant regulations

There are several other standards that may be relevant to the management or use of technology and data within a building but that are not always directly aimed at the property sector. However, these could still have an impact, and it is important that they are also considered.

Some examples of these are set out below, but this is not an exhaustive list.

Cybersecurity

- [ISO/IEC 27001](#): Information security management systems – ensures data protection and cybersecurity within building systems (international).
- [NIST Cybersecurity Framework](#): Framework for improving critical infrastructure cybersecurity – provides guidelines to protect building technologies from cyber-threats (USA).
- [ENISA Guideline on security measures under the EEC](#): Guidelines for smart infrastructure cybersecurity – helps secure building technologies and smart systems from cyber risks (EU).
- [CEN-CENELEC-ETSI Coordination Group ‘Smart Grids’](#): Standards for smart grid cybersecurity and data protection – relevant to buildings connected to smart grids (EU).
- [The EU Cybersecurity Act](#): Establishes cybersecurity certification for ICT products – ensures ICT products used in buildings meet security standards (EU).
- [NIS2 Directive](#): Focuses on the security of network and information systems, including building management systems (EU).
- [Cybersecurity Information Sharing Act \(CISA\)](#): Encourages sharing of cybersecurity threat information – helps building managers respond to cyber-threats effectively (USA).

ISO/IEC 27001

What: ISO/IEC 27001 is an international standard focused on information security, published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC).

Who: used by any organisation that wishes or is required to formalise and improve business processes around information security, privacy and securing its information assets.

Why: to help organisations establish and maintain an information security management system and protect three aspects of information: confidentiality, integrity and availability. The main philosophy of ISO 27001 is based on a process for managing risks: find out where the risks are and then systematically treat them, through the implementation of security controls (or safeguards).

Source: [Advisera](#)

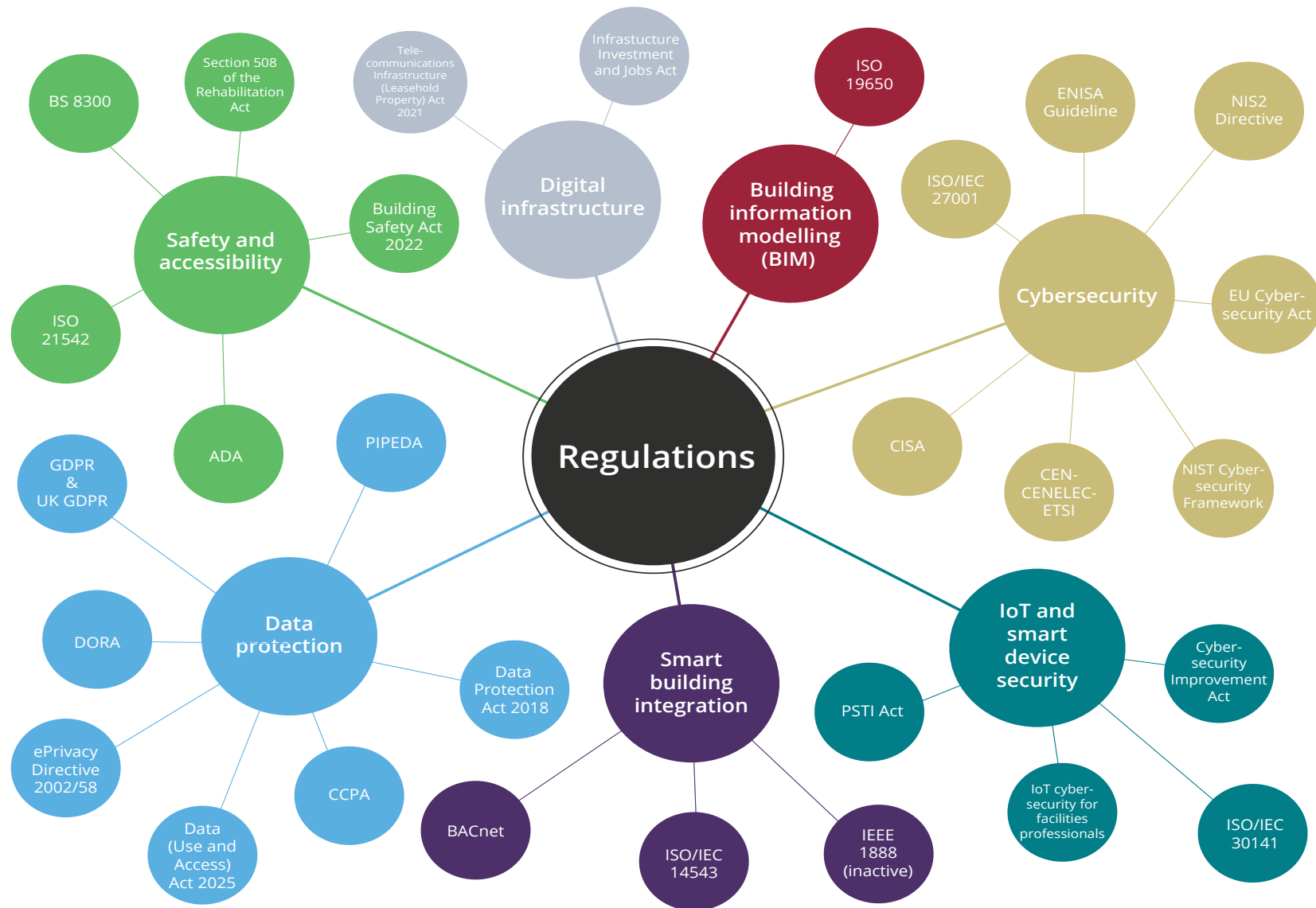


Figure 1: A visual representation of some of the standards or regulations relevant to the topic of digital risks in buildings

IoT and smart device security

- [Product Security and Telecommunications Infrastructure \(PSTI\) Act](#): Mandates security requirements for consumer connectable products, which might include smart devices in buildings, to secure them from cyber-threats (UK).
- [IoT Cybersecurity Improvement Act](#): Sets security standards for IoT devices used by the US federal government – relevant to smart devices in federal buildings (USA).
- [ISO/IEC 30141](#): IoT reference architecture – provides a framework for integrating IoT devices into buildings securely and efficiently (international).
- [IoT cybersecurity for facilities professionals in the smart built environment](#): Guidance relating to cybersecurity in smart buildings (IoT Security Foundation, UK).



With the integration of OT and IoT systems there are more connected systems and more data points, and the risk of cyberattacks increases. If robust cybersecurity practices are not in place, cybercriminals can take advantage of the interconnectivity of these systems to access sensitive data or even gain control of building systems.

Integrating building systems networks without taking proper precautions can lead to vulnerabilities in one building system affecting all others. This could be a significant risk, as a single breach could cause widespread harm to a building's infrastructure.

Furthermore, new technology is being developed and adopted significantly faster than corresponding cybersecurity updates necessary. This lag creates vulnerabilities that can be exploited by cybercriminals, making it essential to take proactive cybersecurity measures.

These new risks can result in threats to physical and life safety as well as reputational damage. For instance, a cybercriminal gaining control of an IoT-connected kettle can easily cause a fire or power cuts, which could lead to significant damage or even loss of life.'

Sanjaya Ranasinghe
Global Director of R&D, WiredScore

Smart building integration

- [BACnet](#): Data communication protocol for building automation and control networks – ensures interoperability of smart building systems (international).
- [IEEE 1888](#) (made inactive in March 2025): Standard for ubiquitous green community control network protocol – relevant for integrating smart devices in eco-friendly buildings (international).
- [ISO/IEC 14543](#): Specifies protocols for intelligent building systems – ensures that smart building technologies can communicate effectively (international).

Data protection

- [GDPR](#): Regulation on data protection and privacy – essential for managing personal data collected by smart building systems (EU).
- [Data Protection Act 2018](#): UK legislation complementing the [UK GDPR](#) – ensures compliance with data privacy requirements in UK buildings (UK).
- [California Consumer Protection Act \(CCPA\)](#): Important for managing the privacy of occupants' data in smart buildings (USA).
- [Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#): Canadian data protection legislation – ensures responsible handling of data collected in smart buildings (Canada).
- [ePrivacy Directive 2002/58](#): Regulates data privacy in electronic communications – relevant for managing communications systems in smart buildings (EU).
- [Data \(Use and Access\) Act 2025](#): Legislation that updates and amends some aspects of UK data protection law (UK).
- [Digital Operational Resilience Act \(DORA\)](#): Regulation designed to strengthen the digital resilience of banks, insurance companies, investment firms and other financial entities (EU).

Safety and accessibility

- [Building Safety Act 2022 \(the golden thread\)](#): Requires a digital record of building information throughout its life cycle – essential for ensuring safety and compliance of smart buildings (UK).
- [Americans with Disabilities Act \(ADA\)](#): Standards for accessible design in buildings – ensures smart buildings are accessible to all users (USA).
- [BS 8300](#): Design of an accessible and inclusive built environment – ensures accessibility in smart buildings (UK).
- [ISO 21542](#): Building construction, accessibility and usability – ensures smart buildings are designed with accessibility in mind (international).
- [Section 508 of the Rehabilitation Act](#): Requires federal buildings' technology to be accessible – ensures smart systems are usable by all occupants (USA).

Digital infrastructure

- [Telecommunications Infrastructure \(Leasehold Property\) Act 2021](#): Facilitates broadband installation in buildings – critical for supporting smart building technologies (UK).
- [Infrastructure Investment and Jobs Act](#): Includes provisions for enhancing digital and cyber infrastructure in buildings – relevant for modernising and securing building technology systems (USA).

Building information modelling (BIM)

- [ISO 19650](#): Standards for organising and digitising information about buildings, including BIM – crucial for managing building information efficiently (international).



**The global average
cost of a data breach
in 2024 was \$4.88m.**

[IBM Cost of a data breach report](#)



5 Next steps

Having established the existence of growing digital risks in buildings, it is important for the sector to take steps to understand and manage these risks. Below are some suggested next steps for building stakeholders, industry bodies and governments to take.

5.1 Building stakeholders

Building stakeholders – owners, users and managers – should adopt a proactive and strategic approach to digital risk, integrating it into every aspect of building management.

Five steps to take

1 Identify, understand and plan for digital risks	Understand the technology in the building. Identify the technologies that your building relies on.
	Use data protection impact assessments (DPIAs). Evaluate how data is collected, stored and protected within building systems. A DPIA is particularly valuable when the impact of a new hardware, software or technology is being considered. Carrying out a DPIA before deployment can help to identify the risk to privacy. Guidance on how to do a DPIA is provided by the ICO .
	Adopt systems thinking. Embrace a holistic view of digital risks, considering combined systems and both direct and indirect impacts on the building and its occupiers.
	Understand compliance requirements. Stay informed about relevant laws, regulations and industry standards to ensure ongoing compliance.
	Understand the risks facing your building. From all the above, you should create a risk register identifying the likely risks, outlining planned actions and articulating responsibility for each risk. It is important to assign ownership to each risk and ensure it is dealt with at the appropriate level within the business.

2

Enhance infrastructure and implement robust security measures

Invest in building upgrades.

Allocate capital to modernise and update viable buildings with the latest technology.

Consider strategic divestment.

To minimise risk, sell or repurpose buildings where updating is not feasible.

Implement strong access controls.

Use multifactor authentication and role-based permissions to secure systems.

Maintain regular updates.

Establish processes for systematic patch management and keep all devices and software up to date.

Continuous monitoring.

Deploy real-time monitoring tools to detect and respond to threats promptly.

3

Invest in employee training and awareness programmes

Provide cybersecurity training.

Educate all relevant employees on best practices and emerging threats.

Implement awareness initiatives.

Foster a culture of security awareness throughout the organisation.

Conduct an incident response exercise.

Carry out a desk-based 'what if?' exercise and prepare staff to act effectively during a security breach through regular simulations.

4

Integrate digital risk management with corporate governance

Align with corporate risk strategies.

Ensure digital risk management is part of the overall corporate risk framework.

Report to leadership.

Keep the board informed about digital risks and mitigation efforts for strategic oversight.

Encourage a security-first culture.

Encourage all levels of the organisation to prioritise cybersecurity in their roles.

5

Manage third-party risks and prepare for incidents

Establish supply chain security requirements.

Set strict cybersecurity criteria for all third-party service providers.

Conduct regular assessments.

Evaluate the security practices of suppliers and limit their access to critical systems.

Consider insurance.

Review and obtain effective insurance coverage to mitigate the impacts from digital risks such as cyber-threats and data breaches.

5.2 Industry bodies

In such a large but fragmented sector, industry bodies have a vital role to play in ensuring that the digital risks in buildings are recognised and appropriately managed to ensure the safe and effective operation of all buildings.

Five steps to take

1

Develop and promote cybersecurity standards and guidelines

Set clear standards.

Establish industry-wide guidelines on the management of digital risks and potential pitfalls of inadequate measures.

Clarify the implications of existing standards and laws.

Clarify how responsibilities under existing laws, legislation and standards are evolving as buildings evolve and become more digital. Even where standards themselves do not change, the way they are interpreted may, and industry bodies need to support the sector to understand and embrace this in a consistent way.

2

Raise awareness and enhance skills

Support skills development.

Offer training programmes and resources to build the necessary skills within the industry to manage and mitigate digital risks effectively.

Provide case studies.

Share success stories and practical examples on repurposing existing buildings and implementing risk mitigation measures.

3

Support accurate valuations and strategic decision-making

Ensure accurate valuations.

Advocate for valuation practices that accurately reflect the changing nature of occupier demand influenced by digital risks and the potential impact of digital risks on income and intangible value.

Guide investors.

Carry out research on the impact of digital risks on building value and the valuation process.

4

Promote collaboration and knowledge exchange

Facilitate collaboration.

Encourage collaboration among industry stakeholders to invest in research, explore innovative solutions and diagnose prevalent digital risks.

Disseminate information.

Actively share findings, resources and tools that can help organisations within the industry enhance their cybersecurity stance.

Consider digital risks in existing content.

Build the topic of digital risks into existing content such as conferences, workshops, journals and training, to ensure that professionals are aware of the digital risks in buildings and their responsibilities.

5

Support the sector with non-built environment standards

Represent the sector with standard-setting bodies and legislators outside the built environment.

There are a growing number of standards and laws regarding the use of data and technology that are not aimed at the built environment but are relevant for it. It is important for industry bodies to engage with these new standard-setting bodies to represent the built environment's perspective and use case.

Raise awareness and understanding.

Make sure that companies in the built environment are aware of standards and legislation that impact them from outside the sector and, where appropriate, provide standard interpretations of them within a building context.

5.3 Governments

Governments play a critical role in managing the digital risks associated with modern buildings, especially as it becomes a more obviously essential part of a nation's critical infrastructure. As buildings become more connected and technology-driven, it is essential for governmental bodies to establish effective frameworks that safeguard assets, promote sustainability and provide regulatory certainty for all stakeholders involved.

Five steps to take

1

Engage with the built environment

Proactively engage with the built environment.

The built environment is such a substantial but highly fragmented sector that there is a temptation for governments to engage around point solutions or small silos. This needs to continue, but in the same way that the sector needs to implement systems thinking, so too do governments need to adopt a holistic approach to the built environment.

2

Provide long-term clarity

Ensure regulatory certainty.

Release clear and consistent regulations well ahead of enforcement dates to give investors and industry stakeholders ample time to comply and adjust their strategies.

Encourage adoption.

Encourage the repurposing and upgrading of existing buildings through tax incentives, especially when carried out in an environmentally sustainable manner.

3

Mandate minimum cybersecurity standards for buildings

Set mandatory security requirements.

Impose minimum standards for the management of digital risks within buildings.

Integrate cybersecurity into building regulations.

Update building regulations to include digital safety provisions as part of standard compliance requirements.

4

Enable data exchange

Facilitate data exchange.

Address industry concerns about data sharing between landlords and tenants to promote transparency and efficiency, and enable an improved approach to digital risks. A more robust approach to data sharing within management agreements should be encouraged.

5

Enhance awareness and skills

Provide sector-specific guidance.

Offer tailored guidance and resources to help unregulated industries adopt best practices in cybersecurity.

Enhance national skills.

Build the skills needed to address digital risks into education and training, both in schools for future generations and in the workplace to upskill today's workers.

Delivering confidence

We are RICS. As a member-led chartered professional body working in the public interest, we uphold the highest technical and ethical standards.

We inspire professionalism, advance knowledge and support our members across global markets to make an effective contribution for the benefit of society. We independently regulate our members in the management of land, real estate, construction and infrastructure. Our work with others supports their professional practice and pioneers a natural and built environment that is sustainable, resilient and inclusive for all.

General enquiries
contactrics@rics.org

Candidate support
candidatesupport@rics.org



rics.org