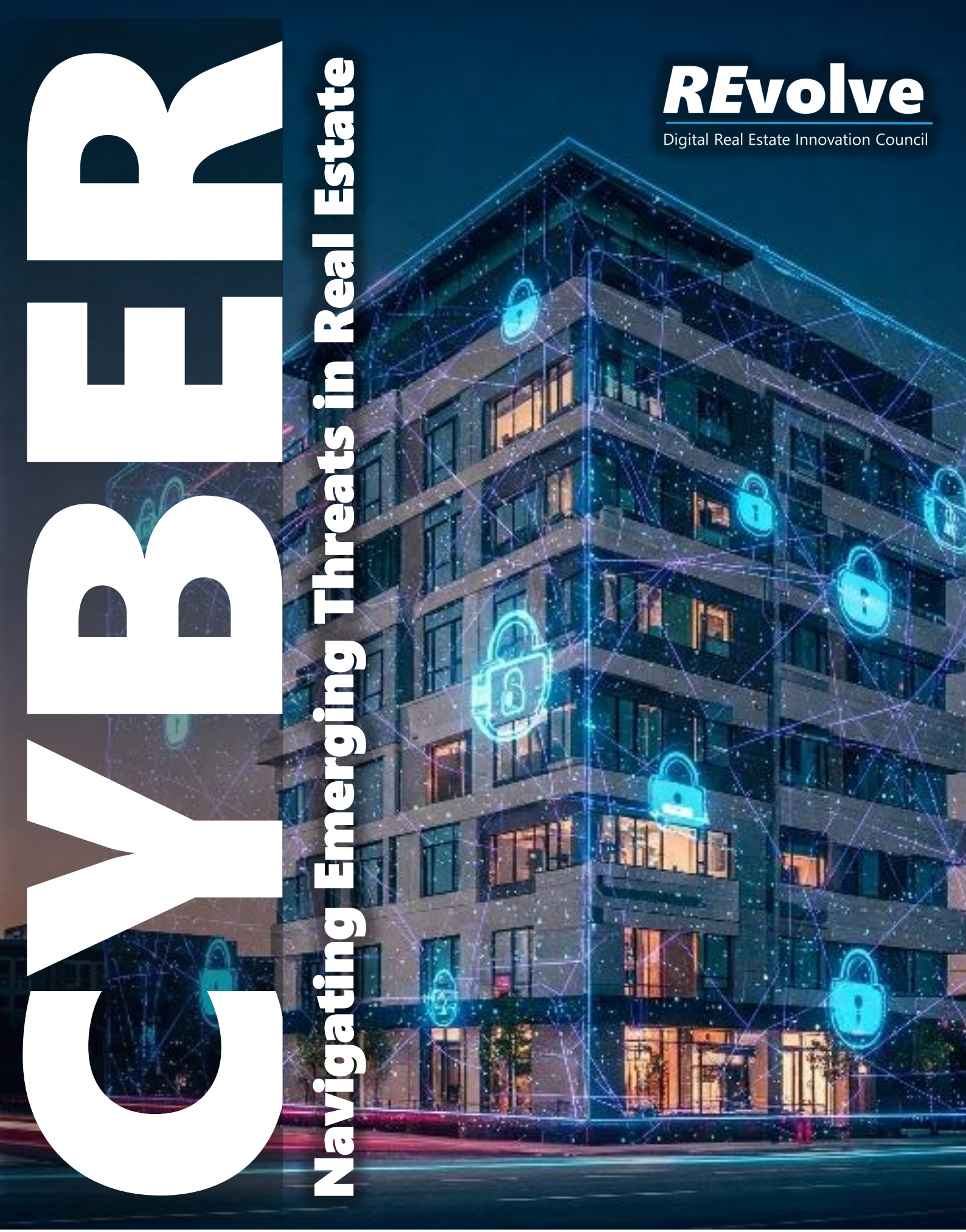
CYBER

Navigating Emerging Threats in Real Estate

REvolve

Digital Real Estate Innovation Council



Our members:

CLIFFORD CHANCE · Knight Frank · LGIM · re:sustain · smartspaces.

Information partner: INFABODE

An API Initiative: Property Insight

Index

REvolve
Digital Real Estate Innovation Council

Introduction

In an increasingly virtual world, the Real Estate sector is becoming more dependent on technology, interconnected systems, and digital networks. While this transformation enhances efficiency and user experience, it also expands the attack surface for cybercriminals. Threats are more sophisticated and convincing than ever, exploiting vulnerabilities in property management systems, financial transactions, and personal data storage.

Whilst there is patchy awareness of cyber security risks, ambiguity around responsibility remains a challenge within real estate. Many organisations operate under the assumption that cyber incidents happen to others—and if they do occur, responsibility for them lies elsewhere, leading to gaps in preparedness and response.

AI-powered solutions can offer a potential defence, but they also enable cyber criminals to produce more accurate and believable material. However, understanding where vulnerabilities lie and clarifying accountability, should help the sector better protect itself against these evolving cyber threats.

This paper explores some of the key cyber security challenges unique to the Real Estate sector and suggests how businesses could improve their cyber resilience and better prepare for the future.

Section 1

Cyber in the Real Estate sector

1.1 Definitions

Before delving into this topic, it is important to clarify some of the terms used when discussing cyber and cyber security.

According to the Cambridge Dictionary, "cyber" is "*involving, using, or relating to computers, especially the internet*" and "cyber security" is "*things that are done to protect a person, organisation, or country and their computer information against crime or attacks carried out using the internet*.[1]"

However, when assessing cyber risks, it is common for businesses to look more broadly at information security (infosec) which is "*the protection of important information against unauthorised access, disclosure, use, alteration or disruption, which might include financial, confidential, personal or sensitive data*[2]*.*"

Some of the most common cyber attacks, which most real estate businesses would see as the greatest risk, include:

- Ransomware attack - when a type of malware is used to prevent someone from accessing their device and the data stored on it, usually by encrypting their files. A criminal group will then demand a ransom in exchange for decryption[3].
- Phishing - when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make them visit a website, which may download a virus onto their computer, or steal bank details or other personal information[4].
- Data breach - any security incident in which unauthorised parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information)[5].

However, cyber incidents include a much broader range of events that disrupt business operations, such as data tampering, business email compromise, AI impersonation and third party cyber risk. It is difficult to stay ahead of these threats as the tactics used by cyber criminals evolve with advancing technology meaning that new threats are emerging all the time.

There have been a number of high-profile incidents of cyber attacks within the sector that have highlighted some of these lesser known methods of extracting information from an organisation. For example, the engineering firm ARUP was a victim of a deep fake fraud when an employee was tricked into transferring HK$200m (£20m) to criminals via an AI generated video call[6].

Around 7.7m cyber crimes were experienced by businesses over the past year - around half of all businesses in the UK

(National Cyber Security Centre)

[1] Cambridge dictionary
[2] IBM
[3] National Cyber Security Centre
[4] National Cyber Security Centre
[5] IBM
[6] The Guardian

1.2 Legislation and security controls

Cyber security regulations have increased in the UK over recent years due to the growing threat of cyber attacks and the need to protect personal data, businesses, and national infrastructure. This includes data privacy laws to protect how personal information is used by businesses (e.g. UK GDPR[7]), consumer and IOT security (e.g. The Product Security and Telecommunications Infrastructure Act 2022), and cyber resilience for businesses (e.g. Digital Operational Resilience Act). It is likely that this trend will continue and the government will continue to update regulation to incorporate developments such as AI.

In the Real Estate sector, there is no universally standardised best practice for infosec. However, companies generally expect a certain level of security controls within their own organisations and from their suppliers. Some of the most common include:

- **Cyber Essentials / Cyber Essentials Plus**[8] - Government-backed certification for basic cyber security controls to help keep an organisation's and its customers' data safe from cyber attacks. The National Cyber Security Centre (NCSC) recommends Cyber Essentials as the minimum standard of cyber security for all organisations.

- **ISO 27001**[9] – voluntary, international standard for information security management. Helps organisations establish and maintain an information security management system.

When considering cyber security, real estate businesses should consider following the "CIA" triad model[10]; confidentiality, integrity and availability. This is an information security model designed to protect sensitive information from data breaches and is used in the information security standard ISO 27001 and mentioned in the GDPR.

Digital Operational Resilience Act (DORA)

Aims to strengthen the IT security of financial entities such as banks, insurance companies and investment firms and make sure that the financial sector in Europe is resilient through a severe operational disruption such as a cyberattack.

Real estate companies can be indirectly affected if they provide services to financial entities.

The Product Security and Telecommunications Infrastructure Act 2022 (PSTI)

Requires manufacturers, importers, and distributors of UK consumer connected (or "smart") products to ensure such products meet a number of security requirements intended to make them more resilient against cyber attacks.

[7] ICO
[8] https://www.ncsc.gov.uk/cyberessentials/overview
[9] https://advisera.com/27001academy/what-is-iso-27001/
[10] IT Governance

CLIFFORD
CHANCE

Cybersecurity in real estate

The real estate sector is particularly exposed to cyber threats, as it holds vast amounts of data and is often reliant on core IT systems. Interruptions and downtime can be extremely costly and as buildings become 'smarter', the attack surface only grows larger.

Navigating this evolving threat landscape requires a proactive approach. What are the key steps that we are seeing clients take?

- Vendor management is a critical area of focus. Many cyber incidents can be traced back to third-party vendors and supply chains in real estate can be complex. Conducting thorough due diligence on vendors is important, but thankfully this is getting easier with increased use of automated tools. After due diligence, it is critical to bind third parties to clear contractual obligations around incident preparedness, response and remediation, clearly defining responsibilities to avoid 'finger-pointing' when vulnerabilities emerge and incidents occur.

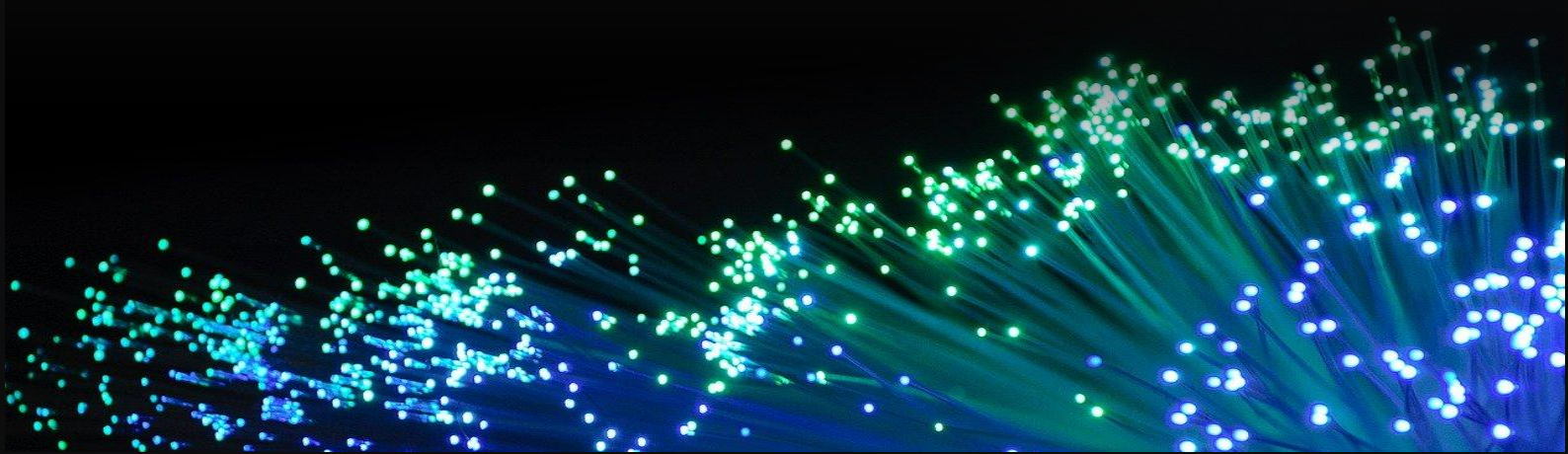
- Getting the basics right is another priority. While larger organisations generally have robust cyber defences, the same cannot always be said of smaller vendors, many of whom operate in competitive markets with tight margins and may not have the scale for cyber risk programmes. Organisations should ensure that they ask the right questions and get the right controls in place.

- AI presents both challenges and opportunities. Newer AI tools make it free, quick and easy for bad actors to write code that helps them to engage in cybercrime but emerging AI-powered solutions can also offer defence mechanisms to detect and shield against such threats. The focus on AI should not obscure that an organisation's personnel are often the weakest link; training employees to recognise phishing attempts, deepfakes, and common fraud vectors is crucial. Again, software can help staff build muscle memory for spotting cyber threats, but with competing priorities, it's an ongoing challenge to get staff to pay attention to cyber risk.

- Legacy technology also poses notable risks. Decommissioning deprecated systems can improve security, but this can be complex and labour-intensive.

Above all, securing top-level buy-in is vital. The steps above require investment in time and capital and can only meaningfully succeed with support from senior team members. If further incentive were needed, emerging legislation increasingly holds senior leadership accountable for cybersecurity.

The risk landscape continuously evolves with new threats emerging regularly. Keeping abreast of these changes is vital and requires a team effort, with collaboration and communication both within and outside the organisation.



1.3 Cyber awareness and cyber readiness

As the number of cyber attacks have increased, so has the awareness of cyber risks. However, whilst some senior leaders tend to be well briefed, the wider workforce can be less knowledgeable about the potential threats to their organisation.

Only 3% of organisations are assessed as having a mature stage of cyber security readiness in 2024. But 80% of companies feel moderately to very confident in their ability to stay resilient amidst this evolving cyber security landscape.

(Cisco Cyber security Readiness survey)

The level of preparedness across the sector to anticipate, respond to and recover from a cyber threat or attack will vary with several factors, such as the size of the business, its culture, the level of buy-in from the senior management team and past exposure to cyber incidents.

Larger real estate companies tend to be better prepared than smaller companies. In most cases, they have bigger budgets and better resources focused on cyber security and some have staff dedicated to it. Larger companies also tend to be subject to stricter regulations which forces them to implement more robust

infosec controls. They can also benefit if they have high levels of cyber insurance which can include advice and guidance from the insurer and its consultants as to the appropriate cyber security measures required to defend the business. However, this is not to suggest that most large companies have appropriately considered and prepared for cyber risks, indeed on occasions, the existence of dedicated specialists or comprehensive insurance policies can lead to complacency and assumption that all risks are mitigated.

According to the latest government figures, only *22% of all UK businesses have a formal incident response plan in place for cyber incidents and only 31% of all UK businesses undertook a cyber risk assessment in 2024*[11].

But within the Real Estate sector, as the quantity and sophistication of cyber incidents have increased, many companies have been stepping up their own precautionary measures within the business.

One of the big areas of focus is vendor management. With a complex supply chain, controlling cyber risk arising from third party suppliers is a big challenge. Some companies are using tactics such as implementing additional technical due diligence on vendors, requesting regular supplier updates and making annual cyber security attestations (an official verification that the supplier is following specific standards and best practice). The availability of automated tools and risk management platforms can also help organisations to manage their third party risk. In each stage of the supply chain, it is important that companies identify who is responsible for what and document that in technical documents and contracts wherever possible.

[11] Cyber security breaches survey 2024 - GOV.UK

Another large risk area for companies is their own employees' vulnerability to cyber threats. The increased threat canvas means that companies are increasingly needing to assess how their own employees would respond to a cyber threat to assess whether additional education and training is required.

Phishing incidents are the most common threat and they are becoming more and more believable as AI is used to increase spelling accuracy, personalisation and video imaging. According to Government data, *18% of businesses tested staff for cyber awareness with exercises such as mock phishing exercises in the last 12 months*[12]. This involves simulating phishing incidents to see if staff report them as a phishing attack and then addressing any omissions with the appropriate training.

63% of medium businesses and 71% of large businesses have used security monitoring tools.

(gov.uk)

[12] Cyber security breaches survey 2024 - GOV.UK

Real estate cybersecurity, the smart choice

As real estate undergoes a digital transformation, cybersecurity is no longer optional - it's essential. Organisations within our sector are becoming more mature in their approach to cybersecurity, recognising its importance not only for their own operations but also across their entire supply chain. The reality is that cyber risks extend far beyond individual companies, affecting service providers, partners, and tenants alike.

At Smart Spaces, we understand that cybersecurity must be at the core of real estate's digital evolution. Clients, particularly those in financial services, now expect service providers to demonstrate maturity and adherence to recognised cybersecurity standards. Many won't even consider working with vendors who lack information security accreditations such as ISO 27001 or SOC 2. Cybersecurity is no longer a competitive advantage—it's a necessity.

Legacy infrastructure, reliance on third-party systems, and fragmented security measures create vulnerabilities that attackers can exploit. Many buildings still operate with outdated protocols, and the integration of multiple technologies from different vendors leads to inconsistent security practices.

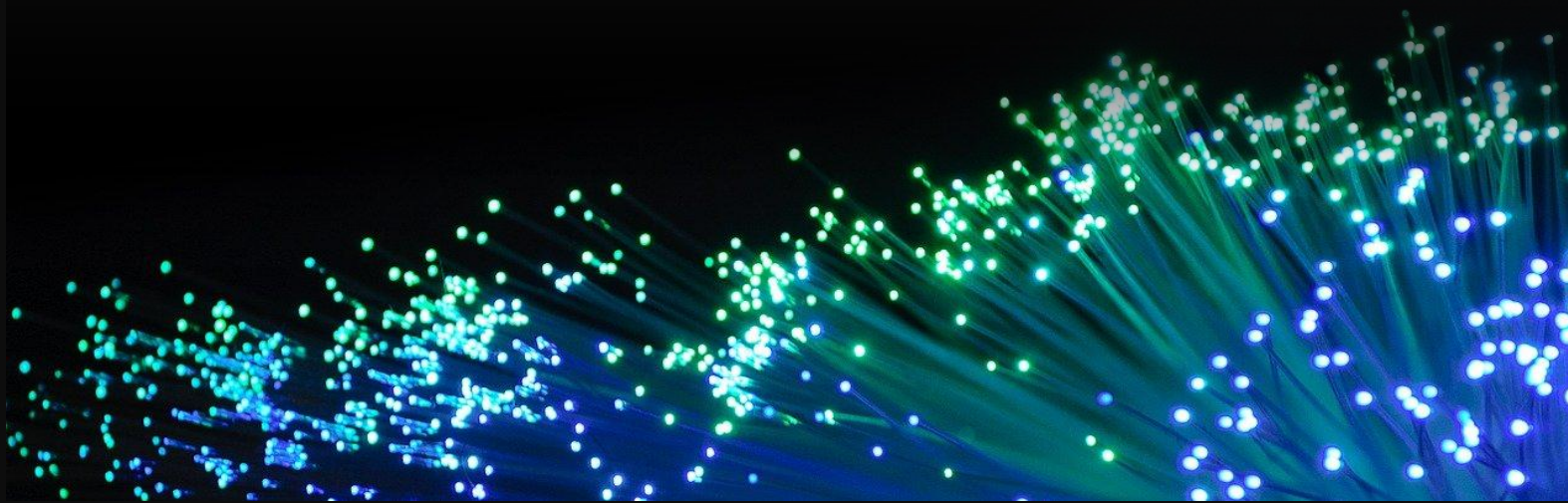
The level of cybersecurity preparedness varies significantly based on the size of an organisation and the external support available. Large firms tend to have dedicated security teams, while smaller companies often struggle with limited resources, making them more vulnerable. However, responsibility doesn't end with individual businesses. Ensuring security at every stage of the supply chain is critical at every rung.

As buildings become smarter, these risks will only intensify. AI, for example, will play a dual role. It will enhance security by detecting threats in real-time while also being leveraged by attackers to orchestrate sophisticated cyber threats. The stakes are high: a single breach can result in financial loss, reputational damage, and regulatory consequences.

To mitigate risks and build a secure digital ecosystem, real estate firms must take a proactive approach:

- Integrate security from the outset
- Enhance access control & authentication
- Ensure end-to-end encryption
- Enforce and maintain security accreditations
- Promote cybersecurity awareness

Cybersecurity is critical for ensuring resilient and efficient smart buildings. As threats evolve, companies must adapt - prioritising security not as a one-time investment but as an ongoing commitment. Those that integrate cybersecurity into their digital transformation strategy will lead the way in creating safer, smarter spaces. At Smart Spaces, we remain committed to driving this change, ensuring that innovation in real estate is not just intelligent, but secure.



Section 2

Real Estate specific challenges

There are several challenges with cyber security some of which are unique to the Real Estate sector. It is common for businesses to focus their attention on technology but both people and buildings also bring vulnerabilities.

Large and complex supply chains

As previously mentioned, real estate companies often have large and complex supply chains. Cyber risks can therefore originate not from the organisation itself but from its third party suppliers. This is especially problematic when the suppliers are smaller and less sophisticated and don't have the necessary security controls in place to prevent a cyber incident. Some of these suppliers might be a high reward target for malicious agents, particularly where there is lots of personal data being handled or where there are large payment transactions taking place.

This is where proactive vendor management becomes crucial to make sure vendors are using the appropriate infosec controls and that any data is being correctly managed. Without this, it is difficult to have any direct level of control if a cyber incident, such as a systems outage, should occur to the vendor. Some market standard levels of infosec have been established which can help steer companies in the right direction but there is a lack of sector specific 'best practice' in place which would help.

Half of businesses report having experienced some form of cyber security breach or attack in the last 12 months.

(DSIT)

Case study: Third party supplier risk

In 2021, PropTech firm Plentific was the victim of a cyber security attack which exposed their users to a scam. Plentific runs a platform that allows property managers to manage and source local repairs for their tenants. Scammers gained unauthorised access to the system and the email addresses of some of the residents. The scammers subsequently sent phishing emails to these tenants, posing as Plentific and requesting the transfer of digital currency to pay for repairs.

So what? *This case highlights the cyber security risks that real estate companies face not only directly but also through their supply chain or third-party partners.*

Source: *Inside Housing*

Fourth party risk

It is common to talk about third party risk from suppliers but there is also a security risk from the "fourth party": the supplier's supplier. This could be from the person fitting out the office who wrongly leaves wires and devices plugged in, or from using shared services within a building where there is no single control over the shared parties' technology or data. This is something that is often overlooked and all organisations should be including it within their risk management registers.

Buildings

Buildings, rather than the businesses using them, can be a direct target of cyber-attacks. As buildings have become smart, and the technology and networks within most buildings have increased, so have the digital risks within them. There have been a number of high profile examples of buildings being targeted, with hackers gaining access to a business through its HVAC systems, or technology failures shutting down door access systems. One major concern with cyber risk in buildings, is that it is unclear as to who takes responsibility and accountability for these incidents; is it the landlord, the occupier, the property manager or all of them? This should be a particular concern for larger property agents who manage multiple buildings and who would be expected to have an understanding of the technological risks that exist in the building.

Legacy technology in buildings

The Real Estate sector does not give sufficient consideration as to how responsible it is for cyber risks emanating from building management systems and IOT systems that are embedded into the fabric of buildings. This is particularly highlighted when an organisation moves into an office or building with legacy technology. In many cases, the technology and networks systems might be old, expired or unsupported, meaning it is very difficult for owners or property managers to have any control over cyber security for that technology or its supply chain. One concern in the sector is that this puts pressure on property managers to become technology experts when they rarely have the required skillset. With new regulation around cyber controls likely in the future, property owners and managers need to establish where responsibility lies with legacy infrastructure.

Cyber Awareness and Readiness

When ownership of a building changes, it often leads to significant shifts in supply chains and priorities. Changes in vendors and the overall operating model can alter how governance is applied from the asset owner downwards.

Previous configurations, plans, and maintenance records can either be opportunities for a thorough clean-up, adding complexity, or simply being overlooked because the solution is unknown or not considered within the new owner's broader tech ecosystem.

Regardless of the technology in use or the nature of failures, whether from cyber-attacks or service disruptions, local building teams and broader support partners must be skilled and well-practiced in handling incidents that affect critical systems. Quick and coordinated action can help prevent the spread of issues and minimise the impact for building users.

To ensure that Operational Technology (OT) remains reliable, robust, and free from vulnerabilities, building owners should take essential cyber hygiene steps as early as possible, such as conducting technology due diligence during the acquisition phase. After acquisition, a detailed system configuration inspection and the establishment of regular monitoring throughout the asset's lifecycle should be considered.

Procurement and Vendor Management

At L&G, we build strong partnerships that foster a culture of best practices and robust governance with our supply chain. We continuously monitor and validate our vendors' commitments to cybersecurity, operational resilience, and technology best practices.

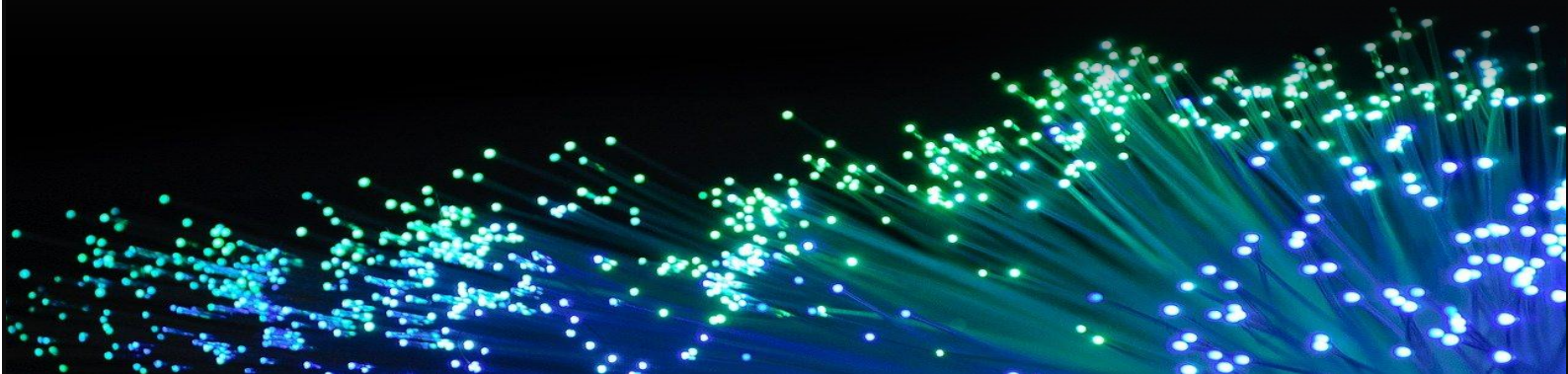
We regularly request independent penetration tests to identify and address key areas needing attention. This approach ensures good governance of our mostly cloud-based supply chain. Any identified vulnerabilities are monitored and retested until they are resolved.

Future Outlook and Emerging Opportunities

The future of cybersecurity in the real estate sector looks promising, with several emerging opportunities:

- Enhanced AI Capabilities: AI can play a crucial role in network and device discovery, as well as in recommending steps to close security gaps.
- Converged Networks: The trend towards converged networks and infrastructure-as-a-service models will enable more efficient and secure management of building systems.
- Increased Regulatory Compliance: Adherence to standards such as ISO27001 and Cyber Essentials Plus will become more prevalent, ensuring higher levels of security and resilience in the sector and especially preferred partners.

As the real estate sector continues to embrace digital transformation, cyber awareness and readiness must remain a top priority. By addressing current challenges and leveraging emerging technologies, asset owners can seek to secure and increase resilience of their assets. By staying proactive and informed, the real estate sector can not only mitigate risks but also capitalise on the opportunities presented by advancements in technology.



Cyber insurance

Real estate businesses should have adequate insurance in place to cover cyber risks within their business. The cost of cyber insurance increased in the early 2020s but the last few years has brought a moderation or even a reduction in some premiums. However, the insurance industry is still grappling with the exact scope of cyber risks meaning some organisations who experience a breach may find that their cover is not broad enough to include that specific incident, particularly as these threats keep evolving. Another grey area occurs when cyber risks occurring in a building are excluded from traditional building insurance but are not necessarily included within cyber insurance leaving a gap in cover.

Leavers

One area of vulnerability for real estate companies is 'leavers', employees leaving the business. This issue was highlighted very publicly when a disgruntled Twitter employee shut down Donald Trump's personal Twitter account for eleven minutes on his last day in the office[13]. Risks from leavers include the deletion of key information, the transfer of company data on to USB sticks which are taken away, sharing confidential information or the continued access to a building and systems after they have left. A robust 'off-boarding' process for all leavers, contract and permanent, is vital to ensure that all company owned hardware is returned, network access terminated, company passwords changed and door access removed. This action needs to be taken before the individual departs or before their end date and should be made a key priority for line managers by the HR and risk teams.

The global average cost of a data breach in 2024 was $4.88m — a 10% increase over last year and the highest total ever.

(IBM)

[13] https://www.standard.co.uk/news/world/disgruntled-twitter-employee-shuts-down-donald-trumps-personal-account-on-last-day-at-work-a3675296.html

Implications of 'cyber' on real estate companies

Cybersecurity is an increasing challenge for all industries, including real estate, as technology becomes more integral to business operations. The real estate industry, with its reliance on personal relationships and sensitive client information such as financial details, property records, and legal documents, is a prime target for cybercriminals.

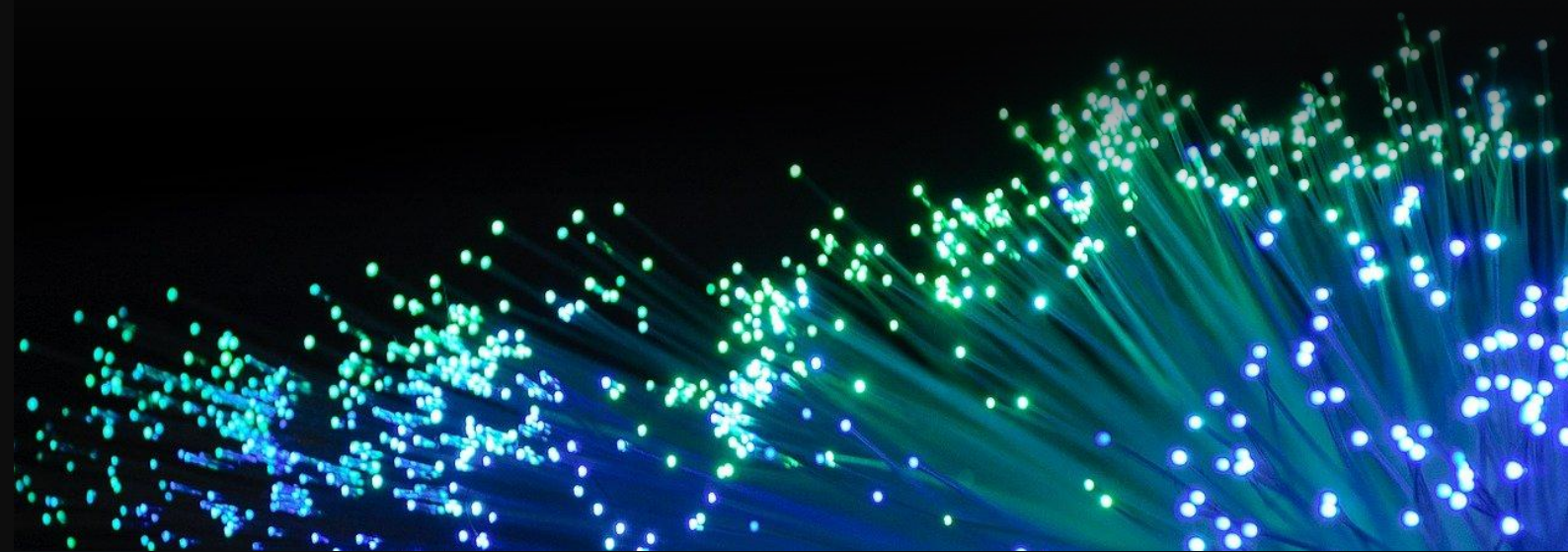
Historically, cybersecurity has been a low priority in the industry. This is partly due to the lack of regulation demanding high cybersecurity standards, but also in part because its interaction with clients has been through close personal relationships, and not technology dependent. The industry has, for some time, largely leveraged technology inside its network to support the delivery of services and management of transactions.

Firms are, however, now extending the boundaries of these systems through customer facing digital channels, modernising the client experience and augmenting the personal relationship with technology. However, many of these solutions are loosely integrated with older, vulnerable platforms increasing the exposure to weaknesses that can be easily exploited by cybercriminals.

The industry is becoming more aware of the severe consequences, including financial losses, legal liabilities, and long-lasting reputational damage, of a successful cyber-attack. Clients in regulated markets are demanding better cybersecurity practices from their supply chain. Legislation like the EU's Digital Operational Resilience Act (DORA) and the UK's proposed Cyber Security and Resilience Bill have raised cybersecurity's profile at the board level, it's no longer considered simply a risk, a good security posture is required to have permission to transact. Companies that can demonstrate effective management of cyber risk will inevitably gain a competitive advantage.

Cybersecurity should no longer be viewed solely as an IT issue; it must be integral to the business culture. Every employee should be trained to recognise and act on potential risks. Leaders should engage in cyber continuity exercises to enhance incident readiness. Technology teams must prioritise eliminating technical debt and addressing internal network vulnerabilities. Security standards should be consistently applied across design, development, and operations. Furthermore, teams must be equipped with the knowledge to manage security in emerging areas like AI and embedded operational technology/industrial control systems.

As the real estate industry continues to digitise, securing client information is paramount. A proactive approach to cybersecurity—balancing technology with employee awareness—will mitigate threats and help maintain client trust. The future success of real estate firms will depend not only on the properties they sell but also on their ability to protect client information.



Sector data maturity

A key element of cyber security is understanding the risks around the collection, storage and use of data. Identifying and reporting these risks at a senior and organisation wide level is imperative. This should consider not only compliance risks but also challenges to business operations and business models. Typically, data maturity in the Real Estate sector can be low; approaches are fragmented, non-standardised and not joined up which makes it difficult to manage and adequately assess data risks.

Infosec within the procurement processes

Whilst there are some widely accepted infosec controls for businesses, there is not one standardised, best practice framework. As a result, organisations adopt their own approach when onboarding new technology, relying on in-house infosec questionnaires and their preferred consolidation platform to gather information.

In a multi-occupier building, this can create inefficiencies, as a single technology provider may need to complete multiple different infosec questionnaires for each building it supplies. Whilst it is understandable that the purchaser wants to take a thorough risk-averse approach, this process is time consuming and drives up costs, potentially leading to higher prices. The sector would benefit from a recommended best practise approach outlining what certificates or controls are needed to satisfy infosec requirements.

There is also concern amongst some in the sector that, whilst being vigilant about cyber threats is imperative, some procurement for infosec has become a tick-box exercise that might not focus on where the biggest cyber threats are. Sometimes it can be more effective to get all parties together to discuss the most likely critical risks so they can shortcut the less relevant areas.

Senior level accountability

Within the financial services industry, certain individuals may hold personal responsibility for cyber security under the Senior Managers and Certification Regime (SMCR)[14] with potential for enforcement action if duties are breached. In the Real Estate sector, senior level accountability for cyber security is often less clearly defined which could lead to real estate professionals assuming it is someone else's responsibility, which can weaken a company's overall defences.

Case study: Building access failure

Facebook experienced a global outage in 2021 and became unavailable to its users for several hours. It was reported that staff were allegedly prevented from accessing parts of their own office buildings as the door access badges stopped working as part of the outage.

So what? *This example highlights that buildings as well as businesses can be direct targets of cyber attacks.*

Source: Business Insider

[14] https://www.fca.org.uk/firms/senior-managers-certification-regime

Section 3

What needs to happen

Over half of businesses (52%) are planning to significantly upgrade their IT infrastructure in the next one to two years.

Cisco

To reduce cyber threats in the Real Estate industry, a rigorous and structured approach must be taken by all organisations and with all buildings. Due to the size, fragmentation and complexity of the sector, it is imperative that some of this is done at a consistent sector level, to avoid adding significant cost and inefficiency and potentially, inadvertently increasing risk levels. Some key recommendations include:

1. More senior level accountability for cyber security

Without clear accountability, cyber risk is often ignored or shifted elsewhere. However, assigning direct responsibility for cyber security to senior executives of real estate companies would ensure it was taken more seriously. Organisations would benefit from senior staff being accountable and for mandatory reporting of cyber security risks and incidents to an appropriate authority.

2. Top-down leadership

Not only is senior level accountability important, but so too is leadership on the topic. Many property professionals lack cyber security training, leaving businesses vulnerable to cyber attacks and data breaches. To mitigate these risks, cyber security awareness and education must be prioritised at the highest level of management and seamlessly integrated into all real estate roles.

It is essential that the senior leadership team lead by example and promote cyber security and cyber training so all employees understand their own role in protecting the company's data. Making cyber training mandatory for all employees, rather than just the IT teams, will boost cyber awareness and reduce risks. Any Chief Information Security Officers should report directly to leadership to help drive cyber strategy.

3. Standardised best-practise for vendor infosec and procurement

Technology vendors are facing an increasingly complex range of infosec due diligence requirements that make the process costly and time consuming for everyone involved. The depth of infosec due diligence should in no way be reduced, but should become more aligned and consistent to reduce inefficiency. The sector would benefit from a standardised, industry-wide approach to cyber security that establishes clear and consistent requirements for third-party vendors. This could include a minimum requirement for cyber security certifications to streamline compliance and a recommended infosec questionnaire template to reduce duplication and inefficiencies. This could also potentially lead to a centralised industry approved vendor list to establish secure procurement.

4. More cyber expertise and skills

Whilst training of staff is important, there are not enough people employed in the sector who understand the cyber threats unique to the sector and are fully equipped to tackle them. Real estate firms should be encouraged to hire more cyber security experts as well as integrating cyber skills into the broader workforce. At a sector level, industry bodies could partner with universities to introduce cyber security modules in real estate courses and include them within their own training qualifications to embed these skills at the earliest opportunity.

5. Mandatory cyber security compliance

Currently, cyber security compliance in the sector is inconsistent. Introducing mandatory cyber security compliance for all real estate firms, modelled on the financial services sector's approach to regulations, would help elevate industry-wide security. For instance, requiring all firms to adopt frameworks such as Cyber Essentials, ISO 27001, or equivalent would establish a baseline for protection. This would require oversight from an existing industry body or the creation of a new regulator to enforce compliance. The introduction of penalties for non-compliance would also ensure firms prioritise cyber security and strengthen resilience across the sector.

Tips for cyber security best practice

- *Constantly communicate to staff about cyber security*
- *Ensure there is senior level awareness and leadership*
- *Establish a cyber security champion*
- *Educate all staff and make cyber training content engaging*
- *Take cautionary steps to protect from high risk factors e.g. banning USB sticks and promoting approved data transfer channels*
- *Proactively test staff and systems for cyber awareness*
- *Ensure you have sufficient cyber insurance cover*
- *Don't assume it is someone else's problem or responsibility.*

About REvolve

About REvolve

REvolve is an Alpha Property Insight initiative. Members of REvolve consist of leading names in the real estate sector which come together to provide unique perspectives on a particular topic. Membership of REvolve demonstrates the members' thought leadership and willingness to explore some of the most pressing challenges that the real estate sector faces in a collaborative way.

Membership does not imply agreement with or endorsement of all of the views expressed in the report. Members provide their own 'Expert View' on the topic.

Each paper is written by Alpha Property Insight and is based on both extensive desk research and a round table discussion with members.

REvolve Members

Clifford Chance

We think beyond the law and see the bigger picture.

At Clifford Chance we recognise that rapid advances in technology are raising both opportunities and challenges, significantly impacting our clients' business models, their growth strategies and even day-to-day decision making. Our clients are at the forefront of the Real Estate industry and rely on us to help them deliver the biggest and most innovative transactions, and navigate an ever changing legal and regulatory landscape. For the last 9 years, we have been ranked as the top firm for European Real Estate by Chambers and PERE has recognised us as European Law Firm of the Year (Transactions) 12 times in the last 18 years, and when combined with our pioneering technology group which comprises over 600 tech-savvy lawyers located around the world, we lead the way in guiding our clients wherever their real estate strategies taken them. We are uniquely placed in the market, acting across the real estate industry's leading players on all asset classes including office, logistics, hotel, retail, residential, data centres and new communities.

Clifford Chance is one of the world's pre-eminent law firms with significant depth and range of resources across five continents. For further information on our services, visit www.cliffordchance.com

Knight Frank

At Knight Frank, we provide innovative property solutions for our clients that add tangible value and maximise performance, across the full range of real estate services and sectors.

To us, performance is about our people and our clients working together to deliver optimised return on the real estate they touch. We do this by identifying, protecting and augmenting value at every stage of the real asset lifecycle, while considering ESG implications from the outset.

As a partnership, our decisions are made by, and for, our people, focused on the best long-term outcomes, driven by our purpose to work responsibly to enhance people's lives and environments.

LGIM Real Assets

LGIMRA is a division of Legal & General Investment Management (LGIM), one of Europe's largest institutional asset managers and a major global investor. LGIM manages £1.1 trillion[1] in assets, working with a range of global clients, including pension schemes, sovereign wealth funds, fund distributors and retail investors.

LGIM Real Assets has assets under management of £36.7 billion[2] and is one of the largest private markets investment managers in the UK. Investing in both debt and equity and across the risk/return spectrum, LGIM Real Assets actively invests in and manages assets across commercial, operational and residential property sectors, as well as infrastructure, real estate, corporate and alternative debt.

Taking a long-term view in order to future proof our investments, LGIM Real Assets continues to lead the industry in ESG performance, considering all environmental, social and governance issues at asset level as well as portfolio level.

1 Source: L&G Annual Report and Accounts, 31 December 2023. Worldwide total assets under management include LGIM AUM and other group assets not managed by LGIM. The AUM includes the value of securities and derivatives positions.

2 Source: LGIM Real Assets. AUM data as at 31 December 2023.

re:sustain

re:sustain is accelerating global real estate's decarbonisation at scale. Our Digital Twin technology remotely minimises carbon emissions and lowers energy costs, leading to substantial optimisation improvements, with reductions in consumption ranging from 22-61% over a 12-month period.

Following implementation, our Digital Twin extends its application by delivering CapEx modelling based on your specific building performance data, not generic benchmarks. This provides a real-time forecast of the measures, potential impacts, and associated costs in your journey to net zero, whilst simultaneously preserving portfolio value, meeting diverse stakeholder goals, and elevating operational performance.

Smart Spaces

Smart Spaces is the multi-accredited and award-winning smart building operating system. Its cloud-hosted Smart Building Platform powers over 75 million square ft. of commercial real estate. The world's leading real estate and occupier brands utilise Smart Spaces technology across a portfolio of alpha-class buildings in prime global locations. The software is currently in 26 countries and growing, it scales with your organisation's needs and is compatible with all major languages.

Rated to Smart Score Platinum, Smart Spaces connect your access control, lifts, HVAC, lights, IoT sensors and more, to provide integrated controls and reporting via a single pane of glass dashboard. The provision of interactive 3D modelling and a workplace app for the building community ensures a world-class smart building experience.

Smart Spaces continually invests in R&D and innovation, it is bridging the physical and digital and is the world's leading white-label smart building employee engagement app. Functionality includes live meeting room and desk booking with community, communications, smart controls, facility management tools and digital twin.

REVOLVE PARTNERS

REvolve Information Partner: Infabode

Infabode is a free research, news and insights platform for the real estate industry. Used by over 40,000+ real estate professionals Infabode is quickly becoming one of the largest online real estate communities; with content from over 1,000 partners across the globe. Infabode works with businesses to include their research, insights, blogs, news and market analysis on one platform. From

the world's most renowned researchers and institutions to smaller, more specialised consultants and bloggers, Infabode connects members with companies posting industry insights - all in one place. Totally customisable, you can search Infabode according to market sectors, region, and/or areas of interest.

Our aim at Infabode is to improve the efficiency in which key information is gathered and distributed within the real estate industry.

LGIM Expert view disclaimer

Key risks

All views expressed by LGIM as at June 2023. Past performance is not a guide to the future. The value of an investment and any income taken from it is not guaranteed and can go down as well as up, you may not get back the amount you originally invested. Assumptions, opinions and estimates are provided for illustrative purposes only. There is no guarantee that any forecasts made will come to pass.

Important information

This document is not a financial promotion nor a marketing communication. It has been produced by Legal & General Investment Management Limited and/or its affiliates ('Legal & General', 'we' or 'us') as thought leadership which represents our intellectual property. The information contained in this document (the 'Information') may include our views on significant governance issues which can affect listed companies and issuers of securities generally. It intentionally refrains from describing any products or services provided by any of the regulated entities within our group of companies, this is so the document can be distributed to the widest possible audience without geographic limitation. No party shall have any right of action against Legal & General in relation to the accuracy or completeness of the Information, or any other written or oral information made available in connection with this publication. No part of this or any other document or presentation provided by us shall be deemed to constitute 'proper advice' for the purposes of the Pensions Act 1995 (as amended).

Limitations:

Unless otherwise agreed by Legal & General in writing, the Information in this document (a) is for information purposes only and we are not soliciting any action based on it, and (b) is not a recommendation to buy or sell securities or pursue a particular investment strategy; and (c) is not investment, legal, regulatory or tax advice. To the fullest extent permitted by law, we exclude all representations, warranties, conditions, undertakings and all other terms of any kind, implied by statute or common law, with respect to the Information including (without limitation) any representations as to the quality, suitability, accuracy or completeness of the Information. The Information is provided 'as is' and 'as available'. To the fullest extent permitted by law, Legal & General accepts no liability to you or any other recipient of the Information for any loss, damage or cost arising from, or in connection with, any use or reliance on the Information. Without limiting the generality of the foregoing, Legal & General does not accept any liability for any indirect, special or consequential loss howsoever caused and on any theory or liability, whether in contract or tort (including negligence) or otherwise, even if Legal & General has been advised of the possibility of such loss.

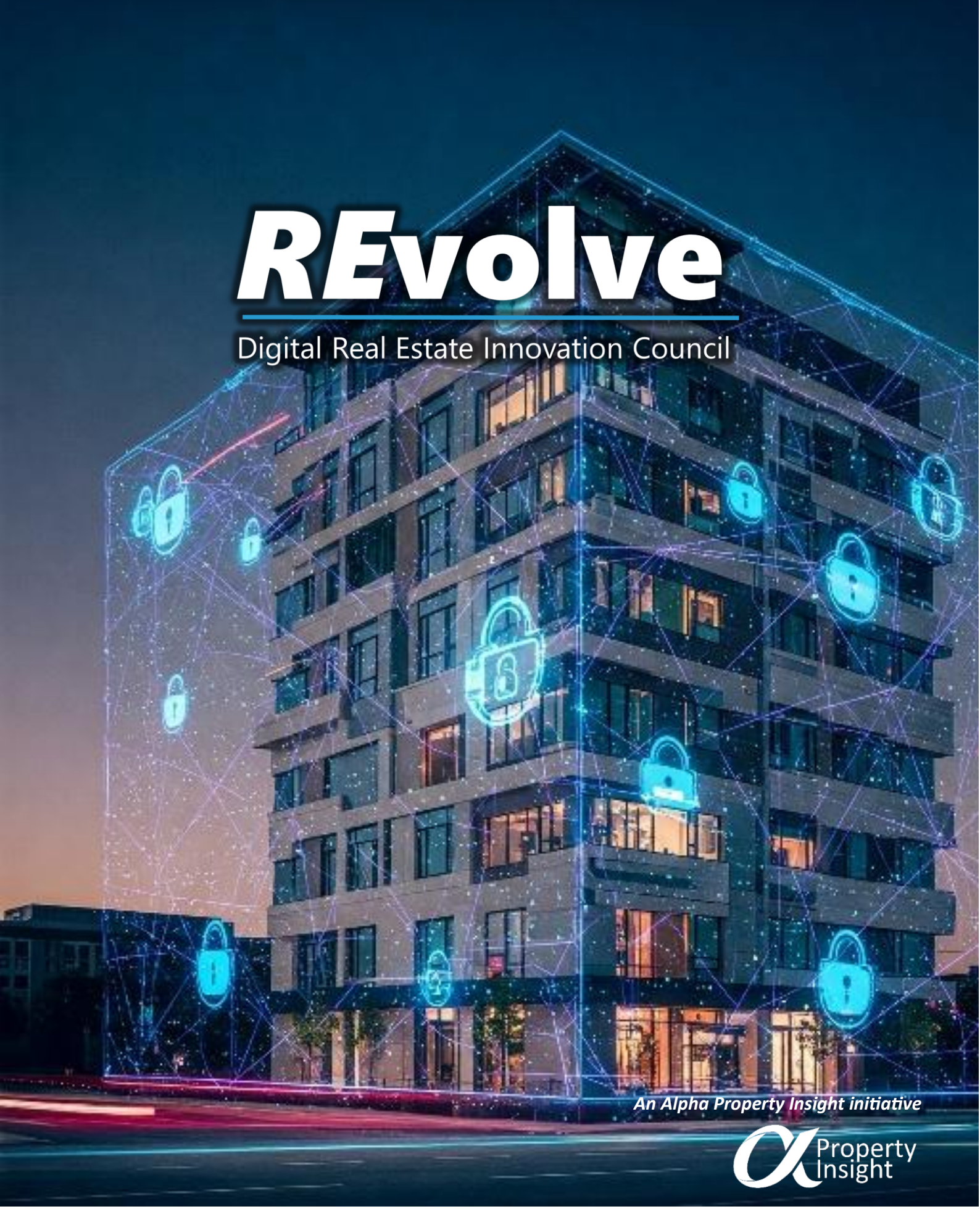
Third Party Data:

Where this document contains third party information or data ('Third Party Data'), we cannot guarantee the accuracy, completeness or reliability of such Third Party Data and accept nor responsibility or liability whatsoever in respect of such Third Party Data.

Publication, Amendments and Updates:

We are under no obligation to update or amend the Information or correct any errors in the Information following the date it was delivered to you. Legal & General reserves the right to update this document and/or the Information at any time and without notice. Although the Information contained in this document is believed to be correct as at the time of printing or publication, no

assurance can be given to you that this document is complete or accurate in the light of information that may become available after its publication. The Information may not take into account any relevant events, facts or conditions that have occurred after the publication or printing of this document.



CLIFFORD CHANCE

Knight Frank

LGIM

re:sustain
Building physics for the future

smartspaces.