

# achieving green, healthy & cyber secure buildings

## The Green Buildings Guide, 2024.

A guide on green & healthy buildings and achieving the right certification.

We examine the pros and cons of the most popular rating schemes and the challenges in creating buildings that are sustainable as well as healthy for occupants.

Plus, we highlight the essential role of technology in achieving these endorsements and the cyber security threats that are often unnoticed.

**oryx**  
**align**

# contents

This guide is divided into two sections: Section 1 offers advice on green & healthy building certification.

Section 2 highlights the essential role of technology in achieving environmental endorsement.

<b>Section 1 - Green &amp; Healthy Building Certification</b>	<b>3</b>
Executive Summary by Greg Richards	3
1. The market	4
2. Popular green & healthy building certifications	6
3. Which certification is right for you?	8
4. Comparing BREEAM and WELL certification	9
5. Challenges of getting BREEAM or WELL certification	10
6. How can technology help organisations achieve BREEAM certification?	11
7. How can technology help organisations achieve WELL certification?	12
8. Conclusion and recommendations	13
<b>Section 2 - Cyber Security in Green &amp; Healthy Buildings</b>	<b>14</b>
Executive Summary by Peter Schwartz	14
9. The market	15
10. Importance of cyber security in green & healthy buildings	18
11. Challenges in cyber security	20
12. Hidden information technology threats for a building	21
13. Least secure IoT devices in a building	22
14. Best practices in cyber security implementation	23
15. Conclusion and recommendations	24
<b>Research Method</b>	<b>25</b>
Survey methodology	25

## section 1: executive summary

# green & healthy building certification

Green & healthy building certification has become a benchmark for sustainable construction and property management, underscoring a commitment by organisations to environmental stewardship and occupant health.

This section outlines the considerations that construction, facilities and real estate managers or landlords should heed to achieve the right certification.

And it's important to choose the correct certification for your company or client – not all certifications are the same.

But get it right, and you'll...

**Boosts Market Value:** Certified buildings often have higher lease and sale rates, as well as being the preference of clients with environmental goals.

**Reduce Operational Costs:** Sustainable buildings can save energy and reduce maintenance costs.

**Enhance Occupant Health:** Healthy buildings improve the work environment, leading to better staff acquisition and retention (especially among younger staff).

We define commercial buildings as anywhere commercial activity is the sole function; so working from home is not included, but anything from data centres to department stores is on the list.



Greg Richards  
Account Director, OryxAlign

### Boosts Market Value:

Certified buildings often have higher lease and sale rates, as well as being the preference of clients with environmental goals.

### Reduce Operational Costs:

Sustainable buildings can save energy and reduce maintenance costs.

### Enhance Occupant Health:

Healthy buildings improve the work environment, leading to better staff acquisition and retention (especially among younger staff).

# 1. the market

Before looking at the available certifications, we wanted to understand the market better. So we commissioned research from YouGov and asked senior executives at tenant companies, “When looking for new premises, how important is it or was it for you to consider the environmental accreditation of the building?”

The results show that green buildings are important or very important for tenants (86%). For the 14% who were ‘neutral’, ‘don’t know’ or stated it was ‘very unimportant’ it possibly demonstrates;

- i. The need for better education on the benefits of a green and healthy workplace
- ii. That for smaller firms with limited budgets, there are more pressing demands on resources

The appetite for green & healthy buildings has fuelled the rapid growth of rating schemes. Among the most popular are LEED, BREEAM and WELL.

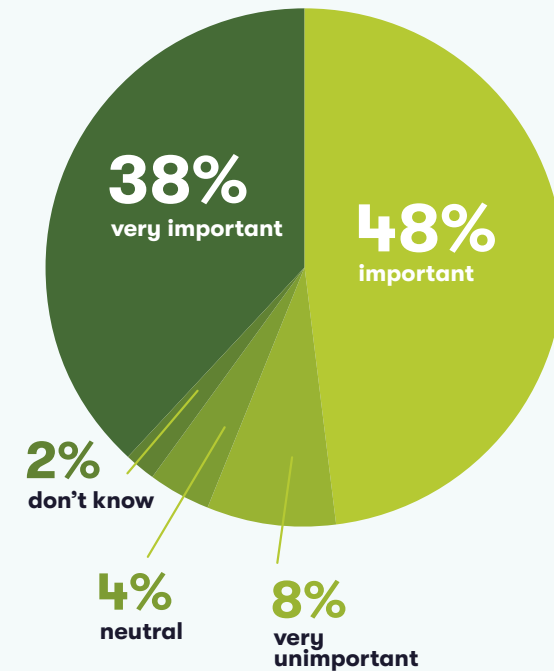
In the UK, the proportion of London office stock with some level of **BREEAM certification rose from around 6% in 2013 to 30% in 2023.** The demand for the most sustainable buildings has consistently outpaced supply, indicating a strong market preference for environmentally certified properties.

The growth of LEED (Leadership in Energy and Environmental Design) certification has been significant since its inception in 2000. **LEED certified buildings have grown from 24,393 in 2014 to 105,000 in 2023.**

The adoption of **WELL certification grew by approximately 1061% between 2017 and 2021.**

## Chart I - The tenant’s view of environmental certification

When looking for new premises, how important is it or was it for you to consider the environmental certification of the building?



Source: YouGov survey commissioned by OryxAlign, Oct 2023 n=300

**86%** of tenants consider green buildings to be important or very important



# 1. the market

continued

## Are green suppliers keeping pace with demand?

We wanted to understand if suppliers were keeping pace with such rapid growth. So we asked senior executives at construction companies, “How much experience does your company have in building or upgrading premises to WELL, BREEAM or LEED specifications?”

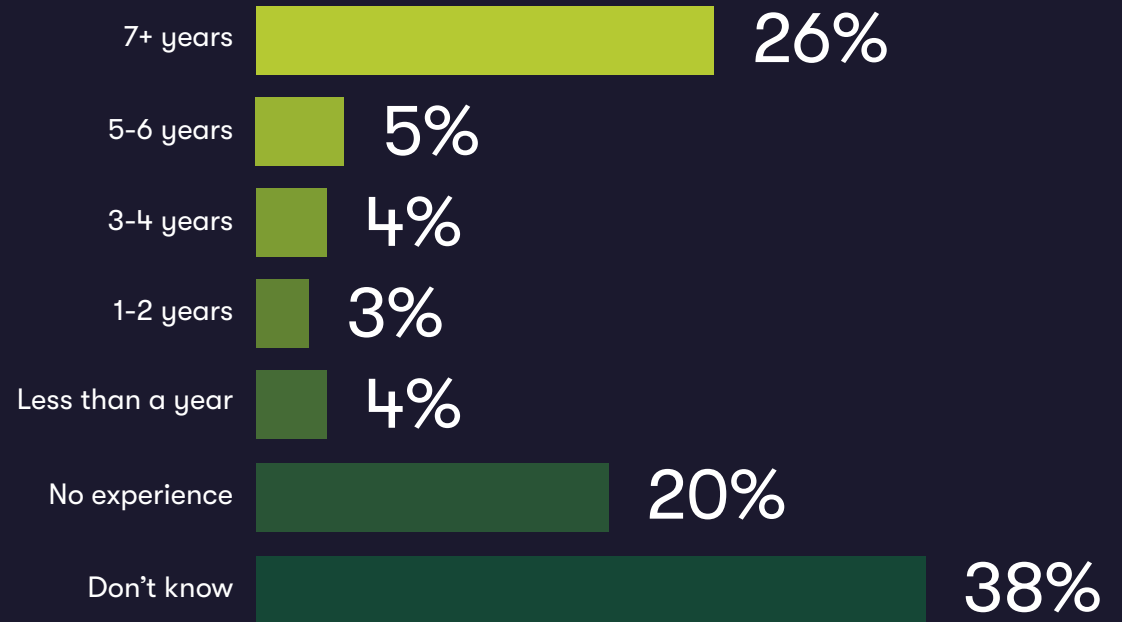
It seems there is very little middle ground in the research results. Construction companies either have a lot of experience (26%) or no experience (20%). Alarmingly, 38% don’t know.

However, given the demand for these certifications, construction companies with experience or who are on a path to gaining skills in this area are sure to do well.

Similarly, facilities management companies and executives may gain an advantage by demonstrating an understanding of the certifications and how to manage them.

## Chart II – UK construction company experience of green certification

How much experience does your company have in building or upgrading premises to WELL, BREEAM or LEED specifications?



Source: YouGov survey commissioned by OryxAlign, Oct 2023 n=300

**38%** of construction executives don't know how much experience of green certification their company has

## 2. popular green & healthy building certifications

We've briefly touched on some of the green building rating schemes available; now it's time to list and explain the major players.



### LEED (Leadership in Energy and Environmental Design)

The LEED system is a design-based rating scheme created in the USA to primarily rate the 'greenness' of buildings. It awards points for such design features as energy savings, water efficiency, indoor air quality, and reductions in CO2 emissions.



### WELL Building Standard

The WELL Building Standard is a performance-based system that uses real-time data to measure, certify, and monitor features of a building that impact human health and well-being. Established in the USA, it now has international recognition and investigates the key concepts of air, water, nourishment, light, fitness, comfort, and mind.



### BREEAM (Building Research Establishment Environmental Assessment Method)

Created in the UK by the Building Research Establishment (BRE), BREEAM is an evidence-based rating scheme primarily focused on the sustainability of existing buildings and those in construction. Areas assessed include energy, innovation, land use, materials, management, pollution, transport, waste, and water.



### Fitwel

Fitwel is a building certification system that enhances occupant health and productivity through evidence-based design and operational strategies in the built environment. It emphasises wellness and sustainability.



### NABERS UK


An adaptation of an Australian rating programme, NABERS UK helps building owners understand their building's performance versus similar buildings. It measures and rates the actual energy efficiency of offices and is currently managed in the UK by BRE.

## 2. popular green & healthy building certifications

continued

Table I shows the top 15 countries for green & healthy buildings, and the popularity of each certification in those countries.

Note the dominance of BREEAM in the UK (and how the UK's appetite for certification puts it in 2nd place globally), plus how the popularity of LEED and WELL are often connected.

 = Certification's most popular country

 = Certification's second most popular country

 = Certification's third most popular country

Note: Some countries, such as Australia, have their own rating system and, therefore, may not appear in this league table, which focuses only on LEED, BREEAM and WELL.

\* Source: LEED projects website, certified from 2000 onwards

\*\* Source: BREEAM projects website, certified assessments from 2008 onwards

\*\*\* Source: WELL projects website, certified from 2018 onwards

**Table I – Top 15 countries for LEED, BREEAM and WELL**

Country	LEED*	BREEAM**	WELL***	Total Green & Healthy Buildings
1. USA	122,206	697	26,677	149,580
2. UK	305	16,871	941	18,117
3. China	9,805	191	2,149	12,145
4. Canada	4,277	31	3,501	7,809
5. Mexico	2,058	-	2,628	4,686
6. France	247	4,026	283	4,556
7. UAE	2,066	26	2,166	4,258
8. India	3,045	-	1,004	4,049
9. Netherlands	101	3,542	209	3,852
10. Spain	1,414	2,028	319	3,761
11. Italy	1,271	659	820	2,750
12. Poland	407	1,819	235	2,461
13. Sweden	555	1,729	104	2,388
14. Brazil	1,649	3	131	1,783
15. Finland	515	1,175	51	1,741

### 3. which certification is right for you?

Consider your goals: do you want to enhance occupiers’ well-being, gain an energy efficiency rating, achieve savings, or demonstrate your green credentials to clients?

Many companies with an international portfolio and a need for consistency choose LEED as their certification. It is one of the most established certificates, with over 105,000 buildings across 90 countries.

However, its footprint in the UK is relatively small, and the program has been criticised for focusing on a building’s design rather than its performance. LEED uses modelling software to predict future energy use rather than being a performance tool that measures actual energy consumption.

WELL is regarded as part of the second

wave of sustainability – human health. How the built environment impacts human health is fast becoming a significant factor in the design and popularity of buildings.

One of the drawbacks of WELL certification is time. According to the USGBC\* it takes 25 days for LEED assessment but up to 6 months for WELL.

BREEAM is seen as a UK alternative to LEED. Launched in 1990, it was the world’s first sustainability assessment method for buildings. According to the World Green Building Council, a BREEAM rating

can increase rental rates by up to 24.9% compared to conventional buildings.

However, a criticism of BREEAM is its higher cost compared to LEED.

NABERS UK is limited to energy efficiency and does not include other sustainability elements, so it is less comprehensive than LEED or BREEAM.

Fitwel is a newer alternative to WELL. Although there are more categories in Fitwel, the lack of performance verification means it is viewed as less rigorous.

**Table II – Key features of the leading green & healthy certifications**

Certification	UK dominant?	Sustainability focused?	Health & well-being focused?	Measures real performance?
LEED	✗	✓	✗	✗
BREEAM	✓	✓	✗	✓
WELL	✗	✗	✓	✓
NABERS UK	✓	✓	✗	✓
Fitwel	✗	✗	✓	✗

\* US Green Building Council



## 4. comparing BREEAM and WELL certification

We believe BREEAM and WELL are appropriate for most UK-based organisations and therefore worth further investigation and comparison.

BREEAM spotlights the negative impacts of buildings on the environment, covering a wide range of sustainability issues, including energy, water use, waste, pollution, materials, ecology, and management processes.

On the other hand, WELL is a certification that emphasises human health. Created by the International WELL Building Institute (IWBI), the WELL Building Standard focuses on aspects of buildings that impact occupant wellbeing.

This includes air quality, water quality, nutrition, light, fitness, comfort, and mental health. WELL aims to create built environments that improve the occupants' nutrition,

fitness, mood, sleep patterns, productivity, and performance.

BREEAM focuses primarily on environmental sustainability, while WELL prioritises human health and wellness. These are not mutually exclusive goals, and many buildings aim to achieve BREEAM and WELL certification to ensure they are both environmentally friendly and conducive to tenant welfare.



*BREEAM focuses primarily on environmental sustainability, while WELL prioritises human health and wellness*

## 5. challenges of getting BREEAM or WELL certification

Achieving a green & healthy building certificate can seem daunting. But when it is part of a planned ESG\* initiative, the effort is worthwhile.

One of the major advantages is that in a competitive commercial building marketplace, green & healthy buildings command a premium and are increasingly desirable. Although BREEAM and WELL are focused on different aims, they share common challenges.

- i. Cost:** One of the most common challenges is the expense. Costs include the accreditation fee and any renovations, modifications, or improvements needed to meet the standards. While BREEAM certification can lead to long-term savings due to energy efficiency and other factors, there can be significant upfront investment.
- ii. Design and operational changes:** Certain design elements and operational practices may need to be altered significantly, which could disrupt ongoing activities. For instance, changes might be needed in lighting, ventilation, or the materials used in the building.
- iii. Educating stakeholders:** Communicating the benefits and importance of certification to all relevant stakeholders, including owners, tenants, and employees, can be a challenge. Everyone must understand the value of sustainable and healthy workplaces.
- iv. Data privacy:** The WELL standard monitors air quality, lighting conditions, and their impact on employee health. However, this can lead to concerns about data privacy, requiring careful management to comply with laws and regulations.
- v. Building usage and occupant behaviour:** WELL certification includes the occupants' behaviour. So, changes might be required in how space is used and in encouraging healthier behaviours, like taking breaks or using stairs.
- vi. Maintaining standards:** Once certification is achieved, maintaining the required standards is challenging to ensure the building remains compliant. Regular audits may be necessary to ensure continued adherence to the standards.
- vii. Time:** Achieving BREEAM or WELL certification can be time-consuming. It involves the assessment and the time it takes to make necessary changes to the building and compile the required documentation.
- viii. Complexity of the certification process:** The WELL certification process is detailed and complex, requiring specialist knowledge. Achieving BREEAM certification is also complex and requires a detailed understanding of the methodology. Knowing how points are scored and what documentation is required is crucial.
- ix. Sourcing materials and services:** Depending on the specific requirements of the BREEAM assessment, it may be challenging to source the necessary materials and services. For instance, finding locally sourced, sustainable building materials can be difficult in some regions.

\* ESG = Environmental, Social and Governance. A set of standards measuring an organisation's impact on society and the environment, as well as its transparency and accountability.

## 6. how can technology help organisations achieve BREEAM certification?

Technology can play a significant role in helping achieve BREEAM rating. Here are some examples:

- i. Energy efficiency:** Smart building technology can automate energy usage, reducing waste by adjusting lighting, heating, etc., based on occupancy and usage patterns. Energy management systems can provide valuable data for tracking and improving energy usage.
- ii. Water efficiency:** Smart meters and automated irrigation systems can help monitor and reduce water usage, improving water efficiency scores under BREEAM.
- iii. Smart materials:** Utilising materials with embedded technology can contribute to achieving higher scores in the Materials category. For example, self-healing concrete and phase-change materials can improve a building's durability and energy efficiency.
- iv. Monitoring and control systems:** Building management systems (BMS) can monitor and control various functions, from energy usage to air quality. These can help optimise the building's operation and add to several BREEAM categories.
- v. Waste management:** Technologies such as waste tracking software can help manage and minimise construction and operational waste, contributing to the Waste category of BREEAM.
- vi. Pollution control:** Technologies like advanced HVAC systems and air purifiers can help reduce indoor and outdoor air pollution, contributing to better scores in the Pollution category.
- vii. Transport:** Using technology to encourage low-carbon transport, such as electric vehicle charging stations, can contribute to BREEAM's Transport category.
- viii. Renewable energy technologies:** Using renewable energy technologies such as solar panels, wind turbines, or geothermal systems can reduce a building's reliance on fossil fuels.

It's important to note that these technologies must be carefully planned and managed, as poorly implemented technology can lead to unnecessary complexity or inefficiency. Integrating these technologies should be part of a holistic approach to sustainable building design that considers all aspects of BREEAM.

The BREEAM logo is displayed in a bold, green, sans-serif font. The word "BREEAM" is followed by a registered trademark symbol (®).

## 7. how can technology help organisations achieve WELL certification?

Similar to achieving BREEAM certification, technology plays a significant role in helping companies reach a WELL rating. Here are some ways in which technology can assist:

- i. Air quality monitoring:** Indoor air quality (IAQ) sensors can monitor levels of pollutants, temperature, humidity, and CO2. This real-time data allows for adjustments to maintain optimal air quality, which aligns with WELL's Air concept.
- ii. Water quality monitoring:** Smart sensors can monitor water quality in real-time, ensuring the water supply within the building remains healthy, safe, and clean, meeting the Water concept of the WELL standard.
- iii. Lighting:** Smart lighting systems can adjust the light intensity and colour temperature throughout the day to mimic natural daylight patterns, supporting the Circadian\* rhythm of building occupants. This aligns with the WELL Light concept.
- iv. Acoustic comfort:** Advanced sound systems can provide ambient noise control and sound masking, enhancing acoustic comfort for occupants aligning with the WELL Sound concept.
- v. Temperature and humidity control:** Smart thermostats and HVAC systems can continuously adjust the temperature and humidity levels for optimal comfort and health conditions, complying with the WELL Thermal Comfort concept.
- vi. Promoting physical activity:** Installation of technology that encourages movement, like standing desks, stair prompts, or even gamified fitness challenges, can help with the WELL Fitness concept.
- vii. Healthy eating:** Tech-enabled services like smart vending machines or app-based food delivery can provide healthier food choices to building occupants, aligning with the WELL Nourishment concept.
- viii. Mental Health:** Spaces equipped with technologies that promote relaxation and stress relief, such as biofeedback devices or virtual reality relaxation modules, can support the Mind concept of the WELL standard.

Each technology should be selected and implemented with care, ensuring that it adds value, is user-friendly, and doesn't create additional stress or complications. Furthermore, privacy and data security issues must be carefully managed, especially when dealing with technologies that gather and process personal data.

\* Circadian rhythm is the 24-hour internal clock in our brain that regulates cycles of alertness and sleepiness by responding to light changes in our environment.



## 8. conclusion and recommendations

### green & healthy building certification

#### conclusion

This guide on green and healthy building rating schemes outlines the significance and benefits of such certifications in today's commercial real estate market.

The increasing demand for environmentally sustainable and occupant-friendly buildings is clear, as evidenced by the growing prevalence of certifications like LEED, BREEAM, WELL, and NABERS UK.

These certifications boost market value, reduce operational costs, and enhance occupant health, critical in building management and design.

#### recommendations

- i. Strategic certification choice:** Companies should carefully evaluate their goals and resources before selecting a certification. For example, LEED might suit those with an international portfolio, while BREEAM could be more appropriate for UK-specific projects.
- ii. Investment in education:** Given the lack of awareness or misunderstanding about the benefits of green and healthy buildings, organisations should educate stakeholders about the advantages.
- iii. Embracing technology:** Integrating smart technologies is crucial for achieving and maintaining these certifications. Companies should invest in technologies that fulfil the criteria of certifications like BREEAM and WELL.
- iv. Skill development:** Construction and facilities management companies should focus on gaining expertise in these certification standards. Given the rapid growth of green certifications, having this expertise could provide a competitive edge.
- v. Financial planning:** Organisations should plan for the initial financial investment required for certification. The long-term benefits, like energy savings and higher lease rates, often justify the upfront costs.
- vi. Focus on both green and healthy:** While choosing certifications, companies should consider both the environmental performance of the building and the well-being of its occupants. Dual certification could be more beneficial in the long term.
- vii. Customisation according to building use:** Different buildings serve different purposes. Therefore, the choice of certification should align with the specific use and requirements of the building.
- viii. Adaptability to change:** The criteria and standards of these certifications evolve. Companies must stay informed and adapt to changes in certification requirements. For example, BREEAM is currently on version 6, WELL is on version 2, and LEED is on version 5.

By following these recommendations, companies can achieve certification and ensure their buildings are sustainable, efficient, and healthy for their occupants, thus contributing positively to the environment, society, and their ESG goals.



## section 2: executive summary

# cyber security in green & healthy buildings

The burgeoning market for green and healthy buildings, driven by increasing environmental and health consciousness, has accelerated the integration of advanced technologies for efficiency and connectivity.

This section emphasises the criticality of cyber security, particularly due to the extensive use of Internet of Things (IoT) and Operational Technology (OT).

Despite the benefits of connectivity, these devices present significant cyber risks. **The need for urgent action is underlined by an 86% increase in IoT attacks from 2021 to 2022\***. The upcoming UK PSTI Bill, enforceable from April 2024, aims to improve the security of IoT for consumers and this will inevitably impact business-grade devices eventually.

Furthermore, the guide highlights challenges like integrating legacy systems, increasing connectivity, lack of standardisation, and budget constraints. Case studies, such as the cyber-attack on Target via an HVAC system, illustrate the tangible consequences of breaches, including data theft and financial losses.

The guide recommends best practices like risk assessments, network segmentation, multi-factor authentication, regular updates, employee training, and stringent vendor management to combat these threats.



Peter Schwartz  
Senior Technology Consultant, OryxAlign

## IoT or OT?

An example of an IoT device in a building could be a smart thermostat. They are connected to the internet, allowing users to remotely control heating and cooling. They can also learn from your habits and adjust the temperature automatically for energy efficiency and comfort.

An example of an OT device might be a fire alarm control panel. It's not typically connected to the internet but is crucial for operational purposes (like detecting smoke or fire, triggering alarms and activating sprinklers). Unlike IoT devices, OT systems are often designed for specific tasks and prioritise reliability and safety over connectivity or data analysis.

## Product Security and Telecommunications Infrastructure (PSTI) Bill

The PSTI Bill seeks to plug gaps in the security of IoT devices. It requires manufacturers and distributors of such devices to remove default passwords, ensure regular firmware updates and provide transparency on any vulnerabilities.

## 9. the market

The market for green and healthy buildings is rapidly expanding as organisations and individuals become more environmentally conscious and health-aware.

These buildings typically incorporate advanced technologies for energy efficiency, air quality, and sustainable resource usage.

Integrating IoT and OT is a hallmark of these buildings, making them more efficient and connected. This connectivity, while beneficial, also introduces cyber security concerns that must be addressed to protect the building and its occupants.

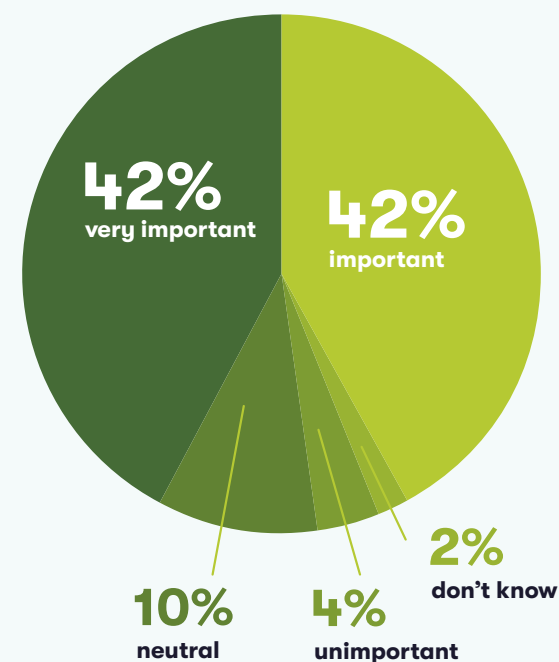
Many of these smart devices are connected to the internet to enable remote control. Anything connected to the internet is vulnerable to attack by hackers.

Traditionally, IoT had limited or no anti-virus protection and no firmware updates. The UK government has recognised this serious gap in cyber protection and introduced the Product Security and Telecommunications (PSTI) Bill, which becomes enforceable in April 2024 which will eventually improve the security of business-grade IoT.

To understand if tenants were aware of the security threat of a buildings technology, we commissioned a survey by YouGov and asked senior executives at tenant companies, “When looking for new premises, how important is it or was it for you to consider the cyber security of the building?”

### Chart III - The tenant’s view on the cyber security of a building

When looking for new premises, how important is it or was it for you to consider the cyber security of the building?



Source: YouGov survey commissioned by OryxAlign, Oct 2023 n=300

**84%** of tenants consider cyber security in buildings to be important or very important

## 9. the market

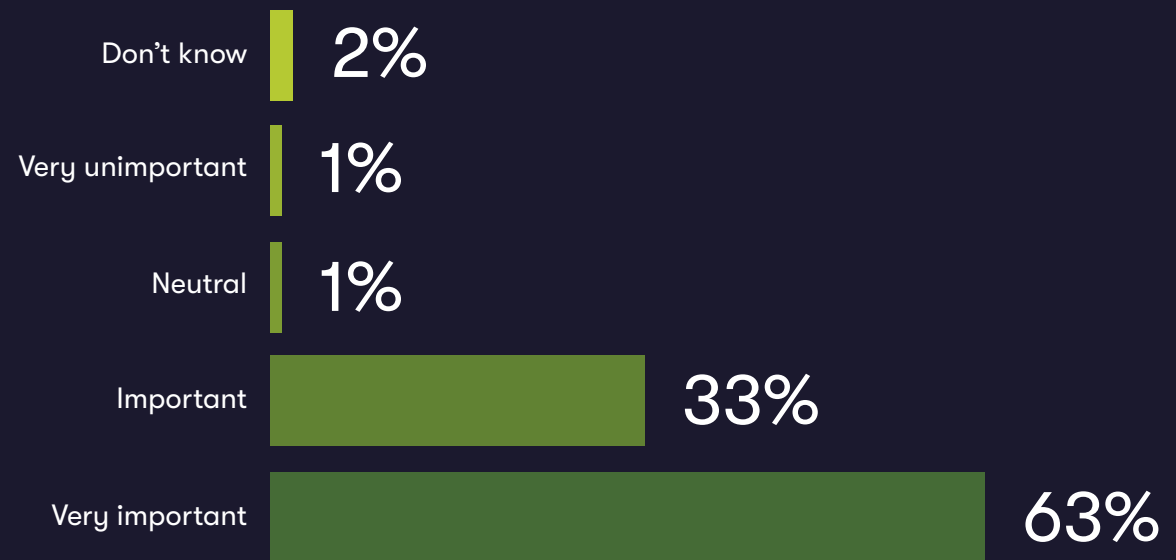
continued

Clearly, tenants seeking new premises believe the cyber protection of a building is of great importance (84%). But we also wanted to understand if the cyber security of a building's network and IoT was also a priority for those responsible for an organisation's IT infrastructure.

So we asked senior executives with IT responsibility, "When reviewing cyber security, how important do you consider the cyber security of the building network and IoT devices?" In total, 96% agreed it was either important or very important.

### Chart IV – IT decision-maker's view on the cyber security of a building

When reviewing cyber security, how important do you consider the cyber security of the building network and IoT devices?



Source: YouGov survey commissioned by OryxAlign, Oct 2023 n=300

**96%** of IT decision-makers agreed the cyber security of buildings was either important or very important

## 9. the market

continued

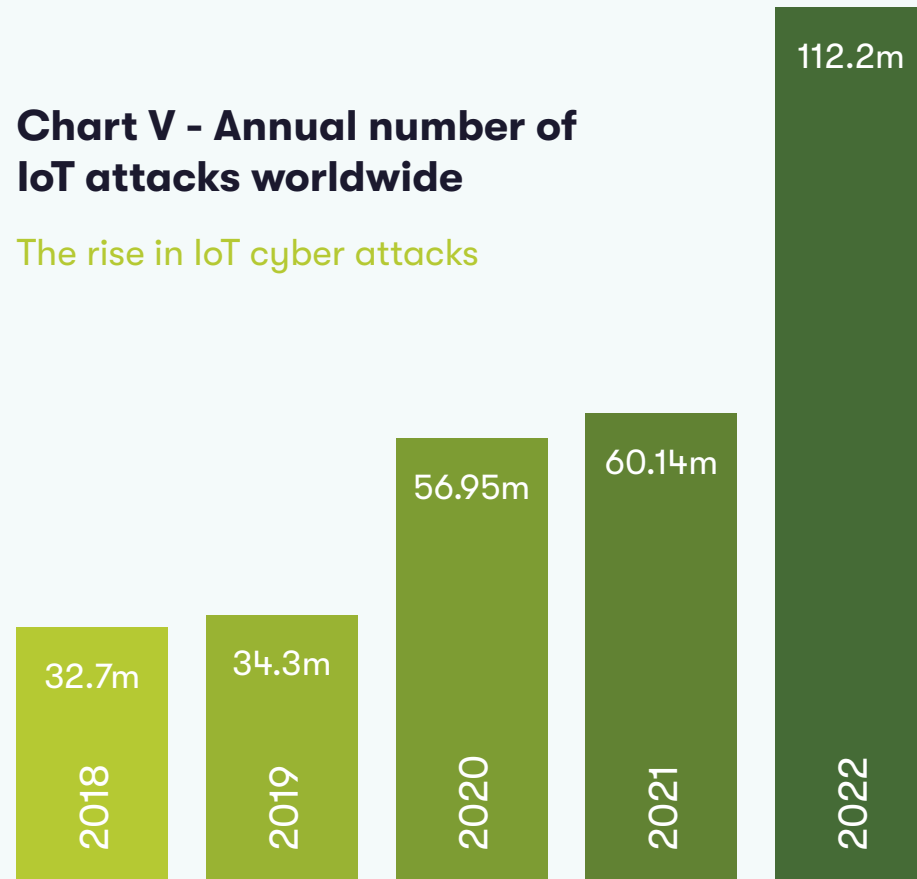
Despite significant awareness among tenants and IT decision-makers regarding the importance of building cyber security, the rise in IoT attacks has been alarming.

Attempted attacks on IoT devices used by UK government facilities and departments jumped from 38,334 in 2021 to 67,324 in 2022, a rise of 75%\*.

This aligns with global figures, which saw an 86% increase in the same years (see Chart V).

### Chart V - Annual number of IoT attacks worldwide

The rise in IoT cyber attacks



\* Source: Statista, May 2023

### Real-world IoT cyber attacks

#### Security cameras

Verkada Inc

150,000 cameras in factories, prisons and hospitals were hacked using admin account credentials and passwords found on the internet.

#### Thermometer

Vegas Casino

A thermometer in a casino aquarium was connected to the internet and enabled hackers to access the network and extract customer data.

#### Access control system

Nortek Security & Control

Failure to patch security issues enabled hackers to install malware, take control of doors and launch DoS (Denial of Service) attacks.

## 10. importance of cyber security in green & healthy buildings

Cyber security is crucial in green and healthy buildings for 3 main reasons.

- 01** Firstly, a cyber breach can lead to physical consequences, such as unauthorised access, sabotaging surveillance systems, or tampering with environmental controls (raising the temperature too high or shutting down the air conditioning until a ransom is paid).
- 02** Secondly, sensitive data collected by smart devices, like occupancy patterns and personal preferences, can be exploited if not adequately protected.
- 03** Finally, the interconnected nature of these systems means that a breach in one can potentially compromise the entire building's network. A good example is the IoT cyber attack on Target, a US-based retailer. A case study of the attack is on the next page.

### Cyber Security Roundtable - IoT and connected devices

In this video, the cyber security roundtable discusses the danger of IoT and connected devices. They're not always secure.





# 10. importance of cyber security in green & healthy buildings

continued

## Case study - Premises attacked via HVAC system

Target is a US-based retailer that was hit by one of the most damaging IoT related cyber attacks of the decade.

The attack would have been done in stages. First, gather information. A simple Google search found the heating and air conditioning was outsourced to Fazio Mechanical.

Two months before the breach, they sent phishing emails to Fazio, which should have been caught by good security software or phishing awareness training.

But Fazio was using a free version of an anti-virus that needed to be stronger, and clearly, their staff were lacking cyber awareness training because somebody clicked the dangerous email.

The phishing email contained malware that stole Fazio's passwords. Armed with the passwords, the hackers entered Target's systems via the internet-connected HVAC.

They leap-frogged from the enterprise and maintenance servers to the corporate and payment systems.

The attackers stole 11 GB of data, including customer names, contact details, and emails of up to 98 million customers — plus 40 million credit/debit cards.

What were the consequences of the cyber-attack? A 46% drop in earnings during the Christmas period, which contributed to a final cost of over \$200 million.

More details are in this article **'Personal data of 98 million customers were stolen via heating controls. How?'**



# 11. challenges in cyber security

Cyber security in buildings involves several challenges:

- i. Legacy and Modern Systems:** Many buildings mix old and new technologies. Integrating legacy systems with modern security solutions can be complex and sometimes creates vulnerabilities.
- ii. Increasing Connectivity:** The rise of the IoT and smart building technologies means more devices are connected to the Internet, increasing the attack surface for cybercriminals.
- iii. Lack of Standardisation:** Standardised protocols and security measures are lacking across different building systems and devices. This inconsistency makes it harder to implement comprehensive security strategies.
- iv. Skill Shortage:** There is often a shortage of professionals with the necessary building management and cyber security skills. This gap can lead to inadequate security.
- v. Data Privacy Concerns:** Buildings that collect and store personal data must ensure compliance with data protection laws like the GDPR in the EU and UK. Ensuring privacy while maintaining functionality can be challenging.
- vi. Regular Updates and Maintenance:** Cyber security is not a one-time solution but requires ongoing updates and maintenance to protect against evolving threats. Ensuring all systems are regularly updated can be a logistical challenge.
- vii. Budget Constraints:** Implementing and maintaining robust cyber security measures can be expensive, and sometimes, building owners or managers might not allocate sufficient budget.
- viii. Awareness and Training:** There needs to be increased awareness among building managers and users about the importance of cyber security. Training staff and occupants to recognise and avoid potential threats is crucial.
- ix. Regulatory Compliance:** Maintaining and complying with evolving cyber security regulations and standards can be challenging, especially for organisations with limited resources.

*“IoT devices pose a significant risk because of the number of devices. Although we call them smart devices, they’re closer to dumb devices like microwaves or washing machines, carrying out a single, specific task.”*

*“While most legacy sites initially air-gapped their networks, this security may have eroded over time as people added devices to the network. Walking into that site today, you may see cables running from switches to firewalls, compromising the air gap. The IoT device now has internet access, is plugged into the network, and the IT team is unaware of it.”*

**Martin Wegrostek,**  
Cyber Security Manager, OryxAlign.

## 12. hidden information technology threats for a building

The growing integration of IT in building management systems (BMS) and smart technologies has increased vulnerability to cyber threats. Besides the obvious threats of unsecured IoT devices and outdated software/hardware, here are some of the hidden IT threats for a building:

- i. **Lack of Encryption:** Data transmitted between devices and systems within the building should be encrypted to prevent unauthorised access. If this data is not encrypted, malicious actors can intercept and exploit it.
- ii. **Insider Threats:** Not all threats come from outside the organisation. Sometimes, a disgruntled employee, contractor, or anyone with authorised access can misuse their access to compromise systems or data.
- iii. **Phishing Attacks:** Phishing attacks target individuals through emails or messages that appear to be from a reputable source. They trick recipients into providing sensitive data like usernames and passwords, which can lead to unauthorised access to building systems.
- iv. **Lack of Security Training:** Employees can inadvertently expose the building to various IT threats without proper awareness and training. They might engage in risky behaviours like clicking on suspicious links or using weak passwords.
- v. **Physical Security Breaches:** Physical access to IT infrastructure like servers and network devices can lead to significant security risks. Unauthorised access to these systems can lead to data theft or sabotage.
- vi. **Lack of Incident Response Plan:** If there's no plan in place to respond to a security breach, the breach's impact could be significantly worse. An incident response plan helps to ensure that breaches are detected promptly and handled appropriately to minimise their impact.



To mitigate these threats, it's essential to have a comprehensive cyber security strategy in place. This could include keeping software and systems up to date, encrypting data, securing smart devices, providing regular security training for staff, and developing a robust incident response plan.

## 13. Least secure IoT and OT devices in a building

Certain devices are more vulnerable to security issues, primarily due to their widespread use, inherent complexities, or lack of robust security features. These include:

- i. Security Cameras:** IoT security cameras can be vulnerable to hacking, allowing unauthorised access to live feeds or stored videos. This risk is heightened if the cameras use default passwords or outdated firmware.
- ii. Smart Thermostats:** These devices, if compromised, can provide insights into occupancy patterns and can be manipulated to disrupt comfort or energy management systems.
- iii. Access Control Systems:** While offering convenience, these systems can be susceptible to attacks, potentially allowing unauthorised access if not securely implemented and maintained.
- iv. HVAC Systems:** HVAC systems connected to the internet without adequate security can be entry points for hackers to access broader building management systems.
- v. Lighting Systems:** Smart lighting systems controlled by IoT are often overlooked in security planning but can be exploited to access networked environments.
- vi. Smart Elevators:** If connected to the internet for monitoring or control, these can be vulnerable, especially if they interface with other building systems.
- vii. Building Maintenance Systems:** Systems that monitor building maintenance can be hacked to gain insights into building operations or as an entry point into more critical systems.
- viii. Networked Printers and other Office Devices:** Often the least secured devices, these can provide an easy backdoor into a building's network.
- ix. Smart Appliances:** Coffee Makers, Refrigerators, etc., are often overlooked in cyber security planning; these devices can be vulnerable points in a network.

The security of these devices depends heavily on factors like the use of strong, unique passwords, regular software updates, network segmentation (keeping critical systems on separate networks), and the use of encryption for data transmission.



## 14. best practices in cyber security implementation

The **NIST (National Institute of Standards and Technology)** framework and the **CIS (Center for Internet Security)** framework are prominent guidelines for cyber security management, sharing several common features while serving slightly different purposes.

Both frameworks provide structured approaches to managing cyber security risk. Each framework is designed to be flexible and scalable, making them applicable to organisations of different sizes and sectors.

Central to both is the concept of risk management. NIST and CIS both advocate for continuous monitoring and improvement of cyber security practices. Both frameworks encourage active engagement with all stakeholders.

While the NIST Framework is often recognised for its comprehensive approach to overall cyber security risk management, the CIS Controls are lauded for their specific, actionable steps for securing IT systems.

Key elements to highlight are listed on the right, but comprehensively following either framework will guide organisations towards a robust cyber security posture.

- i. Risk Assessment:** Begin with a comprehensive assessment of potential vulnerabilities in the cyber security infrastructure of the building.
- ii. Device Hardening:** Configure security settings of all devices to the manufacturer's guidelines. Close off any unused features, connectivity, and make sure all software/firmware is up to date.
- iii. Endpoint Detection and Response (EDR):** Implement EDR on all operating systems to assist with the detection and isolation of a breach should one occur.
- iv. Segmentation:** Isolate critical systems from non-critical ones. For instance, ensure the HVAC controls are not on the critical system network (e.g. the same network as employee workstations). Connectivity in the critical system network should be regularly reviewed and only allow what is crucial to its operation. Limit wireless access to critical networks.
- v. Multi-Factor Authentication (MFA):** Implement MFA where possible, ensuring unauthorised users cannot gain access even if passwords are compromised.
- vi. Centralised audit logging:** Ensure all devices send their audit log to a central system for analysis and monitoring. This supports detection and remediation in the event of a breach.
- vii. Regular Updates:** Ensure all software, firmware, and hardware are regularly updated to defend against known vulnerabilities.
- viii. Employee Training:** Organise consistent training for staff to educate them about the potential risks and appropriate preventive measures.
- ix. Incident Response Plan:** Have a clear, established protocol for responding to breaches or threats, which can aid in mitigating potential damages and restoring normal operations more swiftly.
- x. Vendor Management:** Ensure that third-party vendors, often involved in building management systems, adhere to stringent security standards.



# 15. conclusion and recommendations

## cyber security in green & healthy buildings

### conclusion

The integration of IoT and OT devices in green and healthy buildings has introduced significant cyber security challenges. With the alarming increase in IoT attacks, the need for robust cyber security measures is imperative.

The case study and challenges highlighted in this report underscore the tangible risks associated with cyber threats, including data theft, financial losses, and operational disruptions.

### recommendations

#### Construction Managers

**Implement security from the start:** Incorporate cyber security considerations into the design and planning stages of new buildings. This includes choosing secure IoT and OT devices and designing network architectures that allow for effective air-gapping and monitoring.

#### Collaborate with cyber security experts:

Engage with cyber security professionals to ensure the latest standards and best practice are followed. In a competitive market, this can win you new business.

#### Facilities Managers

**Regular system audits and updates:** Regularly update all IoT and OT systems to patch vulnerabilities. Conduct routine security audits to identify and address potential weaknesses.

**Employee training:** Train staff on cyber security best practices and ensure they know the dangers associated with IoT devices.

#### Commercial Real Estate Managers

**Risk assessment and compliance:** Meet with Facilities and IT Managers to discuss risk assessments. Inform clients of any vulnerabilities in their building and the impact on occupancy.

**Promote the benefits:** Ensure existing and potential tenants understand how green & healthy buildings can help attract top talent and contribute to their environmental goals.

#### Landlords

**Invest in secure infrastructure:** Allocate resources towards upgrading legacy systems and investing in secure IoT solutions.

**Inform tenants:** Keep tenants informed about the green credentials and security features of the building. Update them on any changes.

Addressing the cyber security challenges in green & healthy buildings is not just a technological issue but also a collaborative effort involving various stakeholders. By adhering to best practices and staying informed about emerging threats and regulations, all parties can contribute to a safer, more secure built environment.

## research method

This year's green, healthy & secure buildings guide is divided into two sections and so was our research.

### Section 1 - Green & Healthy Building Certification

We aimed to understand the popularity of green building certifications and whether suppliers were keeping pace with demand.

We commissioned YouGov, the UK's leading online market research and opinion polling group, and asked tenants about the popularity of green certifications. We then surveyed construction companies about their experience in achieving those certifications.

We also conducted online research into the popularity of the dominant rating systems across the globe.

### Section 2 - Cyber Security in Green & Healthy Buildings

Our overall objective was to understand whether tenants prioritised cyber security when seeking new premises, and whether senior management with IT responsibility considered the cyber security of their business premises.

Again, we commissioned YouGov to ask tenants if they did or have considered the cyber security of a building when seeking new premises. We also surveyed IT decision-makers about the importance of building cyber security, especially concerning IoT and smart devices.

We also conducted online research into the rise of IoT attacks across the globe.

## Survey methodology

### RESPONDENTS

300 total respondents

### COLLECTION METHOD

An online questionnaire conducted by YouGov

### GEOGRAPHY

United Kingdom

### SENIOR DECISION-MAKERS

Respondents are employed in executive or senior roles at tenant organisations, construction companies or IT departments.

### COMPANY SIZE

1 to 99	1%
100 to 249	22%
250 to 499	12%
500 to 999	20%
1000 or more	44%

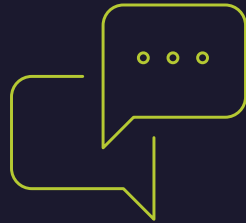
### SECTORS

Manufacturing	5%
Construction	36%
Financial services	8%
IT & telecoms	13%
Medical & health services	7%
Education	7%
Other	24%

### FIELD SURVEY DATES

04.10.23 - 16.10.23

for some good advice on  
green, healthy & cyber secure buildings,  
you can



book a 45-minute  
consultation



or ask a question,  
[hello@oryxalign.com](mailto:hello@oryxalign.com)

OryxAlign brings people and technology in parallel to drive better, faster outcomes.  
By listening closely, adjusting along the way and delivering to the highest standards, we  
create true alignment between your ambitions and the technology you need to reach them.



OryxAlign  
Bury House  
31 Bury Street  
London EC3A 5AR

**T:** +44 (0)207 605 7890

**E:** [hello@oryxalign.com](mailto:hello@oryxalign.com)

**W:** [www.oryxalign.com](http://www.oryxalign.com)



© 2023 Oryx Align Ltd

This document is copyright-protected. All rights reserved. Any unauthorised reproduction or use is strictly prohibited, unless we grant such reproduction or use in writing. Unless specified, all intellectual property rights regarding this document and its contents are the exclusive property of Oryx Align Ltd. Uncontrolled when printed.

First published January 2024

#### No Warranties and Limitation of Liability

Information provided via this tool is provided 'as is' without warranty of any kind, either expressed or implied, including fitness for a particular purpose and non-infringement. Oryx Align Ltd does not make any warranties or representations as to the accuracy or completeness of this tool, and assumes no liability or responsibility for any errors or omissions in its content. Your use of this tool is at your own risk, and Oryx Align Ltd is not liable to you or any other person for any indirect, direct, special, incidental or consequential damages arising from your access or use of this tool. E&OE.



If printed, please recycle the paper.