vorboss

An operator’s guide to secure and resilient building systems

Navigating the Cyber Security and Resilience Bill & evolving tenant expectations

Contents

"

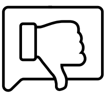
Resilience is knowing where your risks are and being able to respond quickly when something happens. You cannot eliminate every single digital threat, but you can control how quickly and effectively you respond and recover.

Robert Hatch
Chief Information Security Officer, Vorboss

Cybersecurity has crept into the leasing conversation

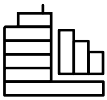
Tenants face growing pressure from customers, insurers, regulators, and investors to strengthen security and recover quickly when incidents happen.

The main factors behind this



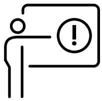
Customer trust

Even one cyberattack can damage business reputation.



Financial impact

Security breaches can cause disruption and significant financial loss.



Compliance pressure

Businesses are facing stricter regulations and insurance requirements.

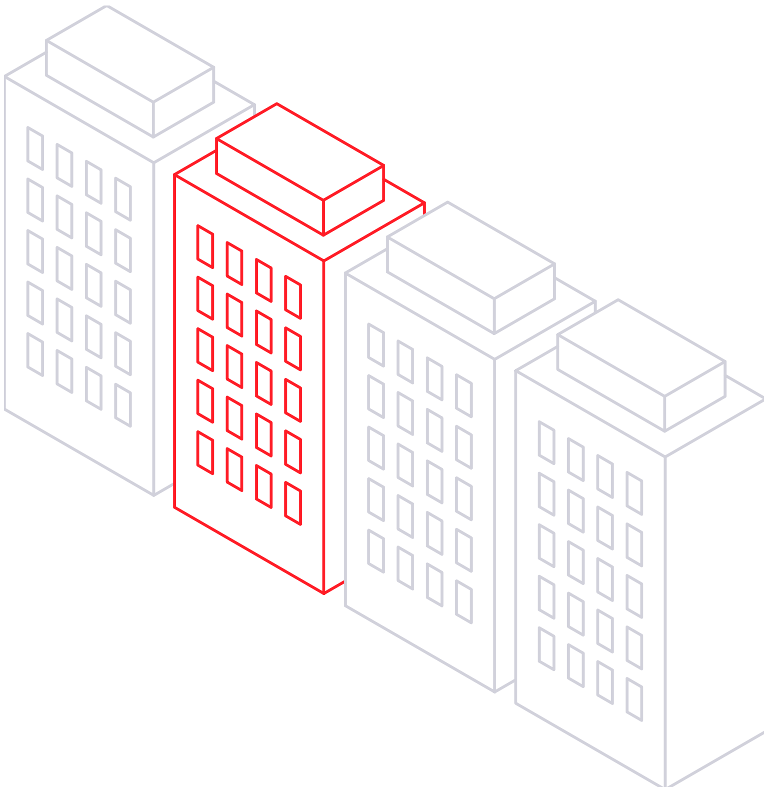
As a result:

Tenants are no longer only assessing their own cybersecurity, but also the resilience of the buildings they operate from.

> "Cybersecurity is now a board-level priority, driving demand for resilient, secure, and digitally enabled office space."

Source: Savills, Cybersecurity Spotlight (2025)

“Over 1 in 4 UK buildings have experienced a cyberattack in the last year.”



Source: RICS Facilities Management Survey (2025)

Shared building systems can create new entry points for hackers

If one system is compromised, attackers may be able to access other connected systems across the building, including tenant business operations.

WEAK SECURITY IMPACTS

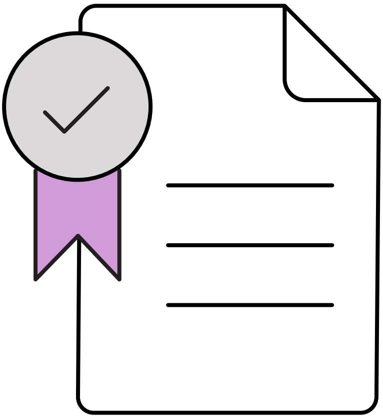
Occupancy rates

Building competitiveness

Landlord reputation

Reviewing your systems now is a simple way to stay ahead of tenant expectations.

What is the Cyber Security and Resilience Bill?



Introduced to Parliament in late 2025, the Bill expands the UK’s cyber laws, bringing more organisations and service providers under regulation.

How are landlords and operators affected?

Flex and managed workspaces

If your building runs on shared systems such as Wi-Fi, tenant apps, or digital access controls, you may now face new responsibilities under the Bill.

Shell and core buildings

If your tenants operate in regulated sectors such as finance, healthcare or energy, their new compliance and reporting obligations under the Bill may extend to their office building's digital infrastructure.

If you are affected by the new Bill, you will be required to

- Report a cyber incident within 24 hours
- Submit a detailed follow-up report within 72 hours
- Demonstrate active risk management measures
- Cooperate with regulator investigations

How do I find out if I'll be affected?
While guidance is still developing, it's best to stay ahead and speak to cybersecurity experts who can offer advice.

Shared systems: biggest risks

Most risks fall into 3 main areas

1. Reliable connectivity and resilience

Reliable connectivity is now just as essential as power and water. Without it, a building simply stops functioning. Leaving it unsecured opens the entire building to major cybersecurity threats.

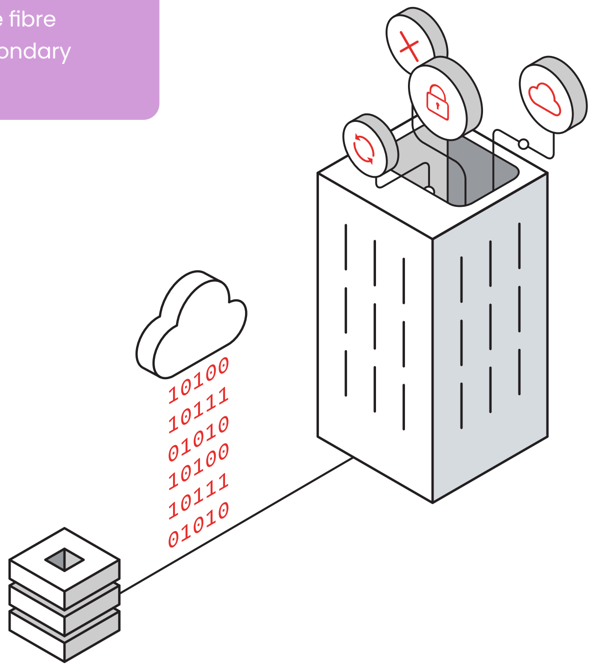
A single line = a single point of failure
Many buildings still rely on a single fibre connection with no backup or secondary route, leaving it vulnerable.

RISKS

Hardware failure
One damaged cable can take the whole building offline.

Traffic flooding
A common attack tactic where the network is flooded with fake traffic to slow it down or take it offline.

Network issue
If your building relies on one connection and there is a fault, you are vulnerable.

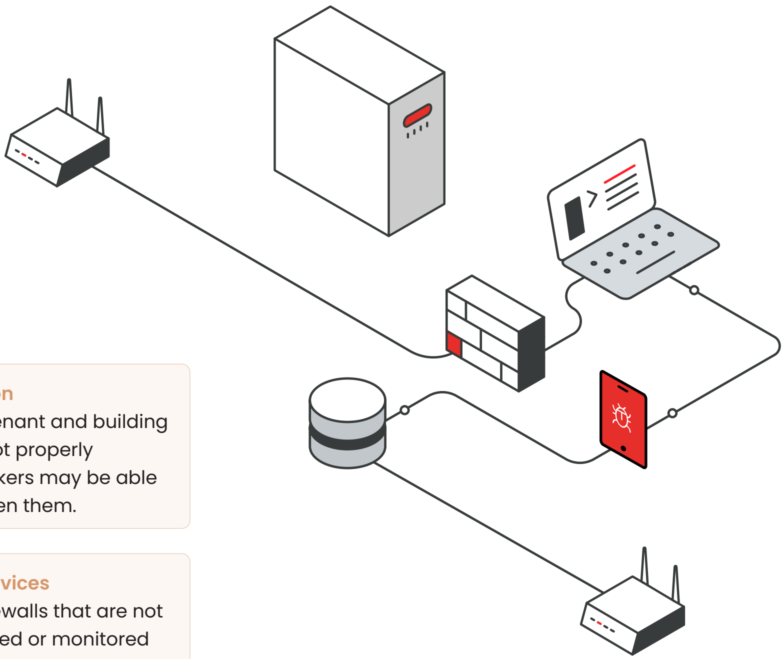


TENANT IMPACT

- × No internet access
- × Cloud systems unavailable
- × Business operations halted

2. Network management

This is where building and tenant systems most often overlap, and where hackers find a way in.



RISKS

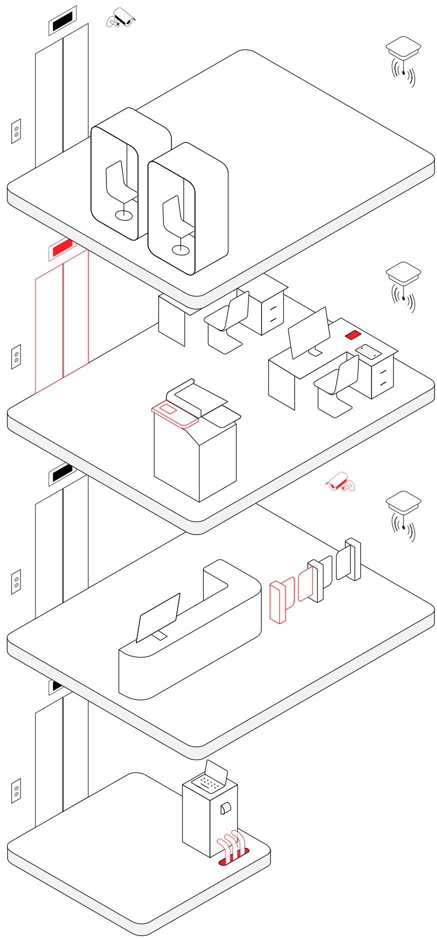
Weak separation
If guest Wi-Fi, tenant and building networks are not properly separated, hackers may be able to move between them.

Unmanaged devices
Routers and firewalls that are not regularly updated or monitored can become entry points for hackers.

TENANT IMPACT

- ✕ No internet or cloud access
- ✕ Data put at risk
- ✕ Business operations disrupted

3. Building technology



RISKS

Building access and security
Lifts and digital doors can be bypassed or shut down if not properly secured.

Heating and cooling systems
Often managed by third parties and rarely reviewed, these systems can give hackers a way in.

Smart amenities
POS systems, EV chargers, smart screens and even coffee machines all connect to the internet and, if not secured, can create a route into other systems.

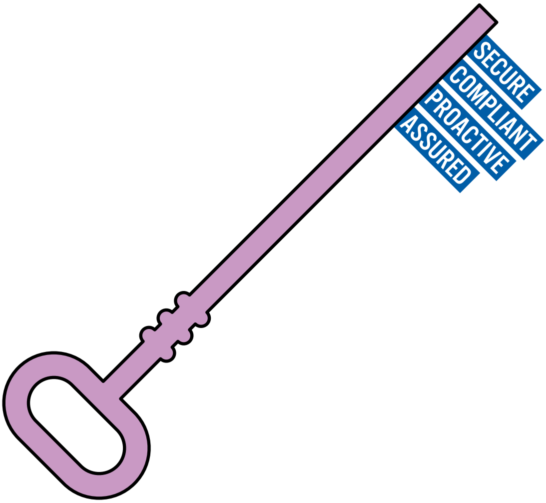
!

This may sound like a lot, but the right cybersecurity partner can help manage it for you.

TENANT IMPACT

- × Physical and digital security at risk
- × Workspace inaccessible
- × Data breach

The modern operator: how your role has shifted



A secure and resilient digital setup is now a non-negotiable for businesses choosing a workspace

Cybersecurity is now part of property management

As an operator, you're expected to understand how your building's systems are connected, protected and managed.

	BEFORE	NOW
Responsibility	Physical safety	Physical and digital resilience
Regulation	Not clearly defined / grey area	Clear rules set
Maximum penalty	Limited accountability	£17m or 4% of global turnover*

*Penalty applies specifically to those affected by the Cyber Security and Resilience Bill.

Digital resilience is a long-term asset value strategy

The definition of a great building has expanded beyond location and interior design. Today, tenants also expect reliable connectivity, secure systems and confidence that the building can keep running when issues arise.

Remain competitive

Recover from disruption quickly

Attract higher-quality tenants

Even if the new Bill doesn't apply to you, understanding risks and planning for incidents is a crucial part of protecting long-term asset value.

"

Regular reviews and good IT hygiene are some of the simplest ways to reduce risk. The most common cyberattacks start with everyday oversights. Forgotten accounts, outdated systems and unsecured networks all create opportunities for attackers.

Nathan Robins
Head of Cybersecurity, Vorboss

5 ways to make building systems more resilient

Whether you're preparing for an audit or looking to strengthen tenant confidence, these are the five areas to cover.

1. Resilient connectivity

- **Backup fibre connections**
  Add a second fibre connection to keep your building connected if the first has an issue.
- **DDoS protection**
  Invest in a solution that filters harmful traffic before it reaches your network. (It's more cost effective than you think.)

2. Keep track of systems

- Maintain a list of connected devices
- Apply updates and regularly review passwords
- Clearly define responsibilities
- Review management agreements

3. Separate networks

- Keep building technology separate from guest and public Wi-Fi
- Use firewalls to control access between different networks
- Isolate older devices

4. Monitor access

- Use multi-factor authentication for logins
- Restrict remote access to trusted users only
- Monitor and report login attempts and unusual activity

5. Know your suppliers

- Keep a list of vendors and the systems they can access
- Review supplier security standards regularly
- Remove supplier access when no longer needed
- Understand who is responsible for upgrades

!

Operators that can demonstrate secure systems and respond quickly to issues will attract higher-quality tenants.

Preparing for tenant questions

Here's what tenants want to know

1

How do you keep systems secure?

To demonstrate this, be ready to explain how regularly software is updated, how networks are separated and what protections are used to prevent unauthorised access or disruption.

2

Who is responsible for cybersecurity in the building?

Tenants want to know who is responsible for managing cybersecurity and responding if something goes wrong.

3

What happens if there is a problem?

No system is perfect and tenants understand that. What matters to them is how quickly issues are spotted, managed and communicated.

!

You do not need to become a cybersecurity expert overnight. The right partner can help manage these risks for you.

Recognised frameworks and standards

Building certifications

SmartScore

WiredScore

These are now commonly expected in modern commercial buildings.

Security standards

ISO 27001

CYBER ESSENTIALS CERTIFIED PLUS

Tenants are increasingly asking landlords about these during leasing conversations and security reviews.

UK cyber legislation

Cyber Security and Resilience Bill

NIS Regulations

It's important to understand how these may apply to your building and tenants.

If you'd like to better understand the risks around your building, get advice on the Bill or improve your cybersecurity, our experts can help.

One provider. Everything connected.