modern networks

Hardware-Enabled Cyber Threats:

Risks to Retail Destinations, Commercial Multi-Tenant Buildings and Science Parks

OCTOBER 2026

Prepared by
Geraint Williams
Chief Information Security Officer



TABLE OF CONTENTS

03 EXECUTIVE SUMMARY

04 RETAIL DESTINATIONS

05 COMMERCIAL MULTI-TENANT BUILDINGS

06 SCIENCE PARKS AND INNOVATION CAMPUSES

07 COMMON CONTROL FAILURES

08 WHAT INCIDENTS MEAN & RECOMMENDED ACTIONS

09 KEY MESSAGE

10 ABOUT MODERN NETWORKS



Executive Summary

Most organisations focus their cyber security efforts on protecting networks, cloud services and user accounts. However, many significant breaches begin with physical access to a building, workstation, network cabinet, meeting room or supplier-maintained system. Our research demonstrates that attackers frequently exploit the gap between physical security and cyber security to introduce unauthorised devices, compromise trusted systems and bypass established controls. For organisations managing retail destinations, commercial office buildings and science parks, the risk is elevated because they operate shared environments with large numbers of tenants, visitors, contractors, suppliers and publicly accessible areas.

Why This Matters

Traditional cyber security assumes that systems inside a building can generally be trusted. Hardware-enabled attacks challenge this assumption.

- Examples include:
- Rogue devices connected to network infrastructure.
- Malicious USB devices inserted into corporate workstations.
- Unauthorised Wi-Fi access points.
- Hidden remote-access equipment installed by individuals posing as engineers.
- Supplier-installed devices left connected after maintenance.
- Covert recording devices placed in meeting rooms.
- Cellular gateways providing an unmonitored path out of the organisation.

In many cases, attackers do not need sophisticated technical skills if they can obtain brief physical access to equipment or secure areas.



Retail Destinations

Key Risks

Shopping centres and retail destinations have a large public footprint and significant third-party presence.

Common risk factors include:

- Public access to buildings.
- Large numbers of retailers and contractors.
- Shared communications infrastructure.
- Building management systems.
- CCTV and physical security systems.
- Payment systems and kiosks.
- Frequent maintenance activity.

Potential attack scenarios include:

- Rogue network devices connected in back-of-house locations.
- Unauthorised access points hidden within tenant areas.
- Compromise of digital signage or public Wi-Fi services.
- Malware introduced through contractor laptops or USB devices.
- Manipulation of building management, lighting or environmental systems.
- Physical access used to collect tenant or visitor information.

For retail estates, a compromise affecting central infrastructure can potentially impact multiple retailers simultaneously, creating a significant **"shared blast radius" event**.

Business Impact

- Service disruption across multiple tenants.
- Reputational damage to the destination.
- Financial losses and incident-response costs.
- Data protection implications.
- Tenant dissatisfaction and contractual disputes.

Commercial Multi-Tenant Buildings

Key Risks

Office buildings typically house multiple organisations, often sharing:

- Network rooms.
- Communications circuits.
- Building management systems.
- Access-control systems.
- CCTV platforms.
- Reception and facilities services.

This creates a unique challenge where security controls are owned by multiple parties.

Potential threats include:

- Attackers impersonating engineers or maintenance personnel.
- Unauthorised devices installed in risers or telecommunications rooms.
- Shared infrastructure becoming a pathway between tenants.
- Rogue cellular devices bypassing network security controls.
- Vulnerable supplier remote-access appliances.
- Monitoring equipment connected without authorisation.

The greatest risk frequently comes from uncertainty regarding ownership and visibility. Organisations may know their own assets but have limited visibility of devices installed by landlords, facilities providers or service contractors.

Business Impact

- Multiple organisations affected by a single incident.
- Exposure of confidential corporate information.
- Service interruption to critical business operations.
- Regulatory scrutiny.
- Increased recovery and remediation costs.





Science Parks and Innovation Campuses

Key Risks

Science parks often contain organisations operating:

- Research and development environments.
- Intellectual property repositories.
- Laboratory equipment.
- Operational technology.
- Industrial control systems.
- Specialist instrumentation.

These environments are attractive targets because the value lies not only in data but also in intellectual property, research outcomes and innovation.

Potential attack scenarios include:

- Unauthorised equipment connected within laboratories.
- Vendor maintenance devices left attached to scientific systems.
- Malware introduced through removable media.
- Compromise of specialist instrumentation.
- Theft of research and development information.
- Covert recording within high-value meeting or project rooms.

Because laboratories frequently require supplier support and specialist maintenance, legitimate access is often more difficult to distinguish from malicious activity.

Business Impact

- Intellectual property loss.
- Competitive disadvantage.
- Research delays.
- Loss of trust from partners and investors.
- Contractual and regulatory consequences.

Common Control Failures

Analysis of real-world incidents identifies four recurring weaknesses:

1. Contractor and supplier access was not independently verified.
2. Equipment could be connected without approval or monitoring.
3. Sensitive systems and locations were insufficiently supervised.
4. Physical security, facilities management and cyber security operated independently rather than as a coordinated control framework.

Selected Verified Physical Cyber Security Incidents

Incident	Sector	Attack Method	Physical Element	Business Impact	Status
Barclays Swiss Cottage (2013)	Banking	Remote workstation compromise	Criminal posed as engineer and installed network-connected KVM with 3G connectivity	Approximately £1.25m fraudulently transferred	Confirmed
Barclays Lewisham (2013)	Banking	Remote workstation compromise	Similar KVM-based attack using physical access	Approximately £90,000 stolen	Confirmed
Santander Surrey Quays (2013)	Banking	Attempted KVM installation	Individual posing as maintenance engineer	Attack disrupted before loss occurred	Confirmed attempted attack
Sumitomo Mitsui London (2004)	Financial Services	Credential theft	Insider-assisted physical access enabled installation of keylogging software	Attempted theft of £229m	Confirmed
Port of Antwerp (2011-2013)	Logistics & Ports	Keylogging and system compromise	Criminals physically entered offices and installed keyloggers	Used to facilitate narcotics smuggling operations	Confirmed by Europol
Antwerp & Rotterdam Port Operations (2020-2021)	Logistics & Ports	Malware introduced via USB	Bribed employee inserted malware-bearing USB device	Container management information compromised	Confirmed through court reporting
Stuxnet (discovered 2010)	Industrial Control Systems	Malware introduced into isolated environments	Believed to have propagated through removable media	Physical disruption of uranium enrichment systems	Confirmed incident, initial introduction route uncertain
ATM Jackpotting Campaigns (2013 onwards)	Financial Services	ATM malware installation	Criminals gained physical cabinet access and replaced or modified drives	Significant global financial losses	Confirmed pattern
Rogue Raspberry Pi on ICS Network (reported 2025)	Manufacturing	Unauthorised network access path	Supplier device left connected to operational network	Created unmanaged access route into ICS environment	Confirmed exposure, malicious intent not established
OpenAI Meeting Room Device (2026)	Technology	Alleged audio surveillance	Recording device hidden behind meeting room television	Potential exposure of sensitive discussions	Alleged, legal proceedings ongoing at time of publication

What These Incidents Mean for Property Owners

Although the incidents occurred in different industries, they repeatedly demonstrate the same four themes:

Common Failure	Relevance to Property Environments
Unverified contractors or engineers	Common within retail destinations, office buildings and science parks where third parties regularly require site access.
Unauthorised equipment connected to networks	Rogue devices can be hidden in comms rooms, plant rooms, risers, cabinets and tenant spaces.
Poor visibility of connected assets	Organisations frequently cannot identify every device connected to shared infrastructure.
Separation of cyber and physical security functions	Facilities, security, IT and cyber teams often manage risks independently despite sharing responsibility.

Recommended Actions

Property owners, landlords and managing agents should implement the following controls across their estates:

Governance

- Treat physical assets and connected devices as part of the cyber perimeter.
- Define clear accountability between cyber, facilities, physical security and suppliers.
- Maintain an inventory of authorised connected devices.

Access Management

- Independently verify all engineers and contractors.
- Use approved work orders and visitor management processes.
- Escort contractors in sensitive locations.

Technology Controls

- Maintain continuous asset discovery.
- Detect unknown wired, wireless and cellular devices.
- Restrict removable media and unauthorised USB devices.
- Segregate building systems from tenant networks.

Assurance

- Inspect network rooms, plant rooms and critical infrastructure regularly.
- Audit supplier-installed equipment.
- Reconcile physical assets with network-connected devices.
- Include hardware-enabled attacks within incident-response exercises.



Key Message

Every major physical cyber incident started with a trusted individual, a trusted location, or trusted equipment being used in an unexpected way. The greatest risk is often not sophisticated hacking, but the ability to introduce a device, gain unsupervised access, or exploit a gap between physical and cyber security controls.

Many organisations have invested heavily in cyber security technologies but still maintain an implicit trust model around physical access, suppliers and connected equipment.

Organisations should ask a simple question:

Can we identify every device connected across our estate, explain why it is present, confirm who authorised it and rapidly detect when something new appears?

If the answer is not consistently "yes", there remains a material gap between the organisation's physical and digital security boundaries. This gap is particularly significant in retail destinations, commercial multi-tenant properties and science parks where large numbers of visitors, contractors, suppliers and tenants interact with shared infrastructure every day.

Can you account for every connected device across your estate?

If you cannot identify what each device is, why it is there and who authorised it, your physical and digital security boundaries may already contain hidden gaps.

Arrange a physical cyber security assessment to uncover unauthorised devices, access weaknesses and supplier-related risks before they become an incident.

Contact Modern Networks Today to Book a Security Assessment

01462 426500 | sales@modern-networks.co.uk I www.modern-networks.co.uk

About Modern Networks

Modern Networks is a leading provider of managed IT services to the UK commercial property sector and an independent Internet Service Provider specialising in connected buildings. We provide IT, connectivity and telecoms services to more than 2,600 commercial properties, including shopping centres, retail parks, and business and science parks. Our expertise spans managed IT, networks, connectivity and cyber security, giving us a practical understanding of the increasingly connected technology environments that property owners and managing agents need to secure.

- **2,600+** properties. One trusted technology partner.
- **100+** shopping & retail destinations connected and supported.
- **47** science & innovation parks supported.
    - **700+** tenant organisations relying on our services.



Modern Networks Ltd, 18 Knowl Piece, Wilbury Way, Hitchin, Hertfordshire SG4 0TY
01462 426500 | sales@modern-networks.co.uk I www.modern-networks.co.uk