modern networks

CYBER SECURITY FOR SHOPPING CENTRES

A practical guide for operators and centre management teams

NOVEMBER 2026

Prepared by
Geraint Williams
Chief Information Security Officer





TABLE OF CONTENTS

About this guide 3

Know what you are protecting 4

Put identity first 5

Stop payment and email fraud 6

Watch for retailer led social engineering 7

Protect the systems that run the site 8

Manage supplier access 10

Use the right data and service focus 11

Prepare for an incident 12

Ten priorities for centre operators 13

Next steps 14



The aim of this guide

Keep the centre running, protect shared systems and reduce the risk of trusted accounts being compromised.

Shopping centres face a different cyber security challenge from traditional retailers. Centre operators manage shared systems, services and suppliers, while individual retailers usually manage their own IT, networks and point of sale systems. This creates a unique set of risks.

This guide is for shopping centre operators, centre directors, property managers, facilities teams, security teams, finance teams and marketing teams. It explains the cyber threats most likely to affect a retail destination, from compromised email accounts and supplier access to building management systems, CCTV, car parks and public Wi-Fi.

You'll find practical advice, clear actions and key questions to help protect the centre, reduce disruption and strengthen day to day cyber resilience. The aim is simple: keep services running, protect critical systems and reduce the risk of trusted accounts being used against the business.

Know what you are protecting

A retail destination does not normally control each retailer's IT. It does control, or rely on, a wide set of shared systems and services. Start with these.

Area	What sits within scope
Building systems	Heating, ventilation, lighting, escalators and energy management.
Security systems	CCTV, recording systems and access control for plant rooms, roofs, service yards, goods lifts and control rooms.
Visitor services	Public Wi Fi, websites, mobile apps, digital voucher services, event booking and digital signs.
Parking	Payment systems, parking apps and automatic number plate recognition data.
Business data	Tenant contacts, emergency plans, supplier contracts, building plans, security schedules, newsletters, competition entries and event registrations.
Suppliers	Managing agents, facilities providers, security firms, CCTV vendors, lift and heating contractors, parking firms, digital sign vendors and marketing agencies.
Keep the boundary clear	Do not assume that a retailer's IT is part of the centre's estate. Record who owns each system, who supports it and who can access it.



Risk level: HIGH

A compromised account can cause serious disruption, even without access to retailer systems

Put identity first

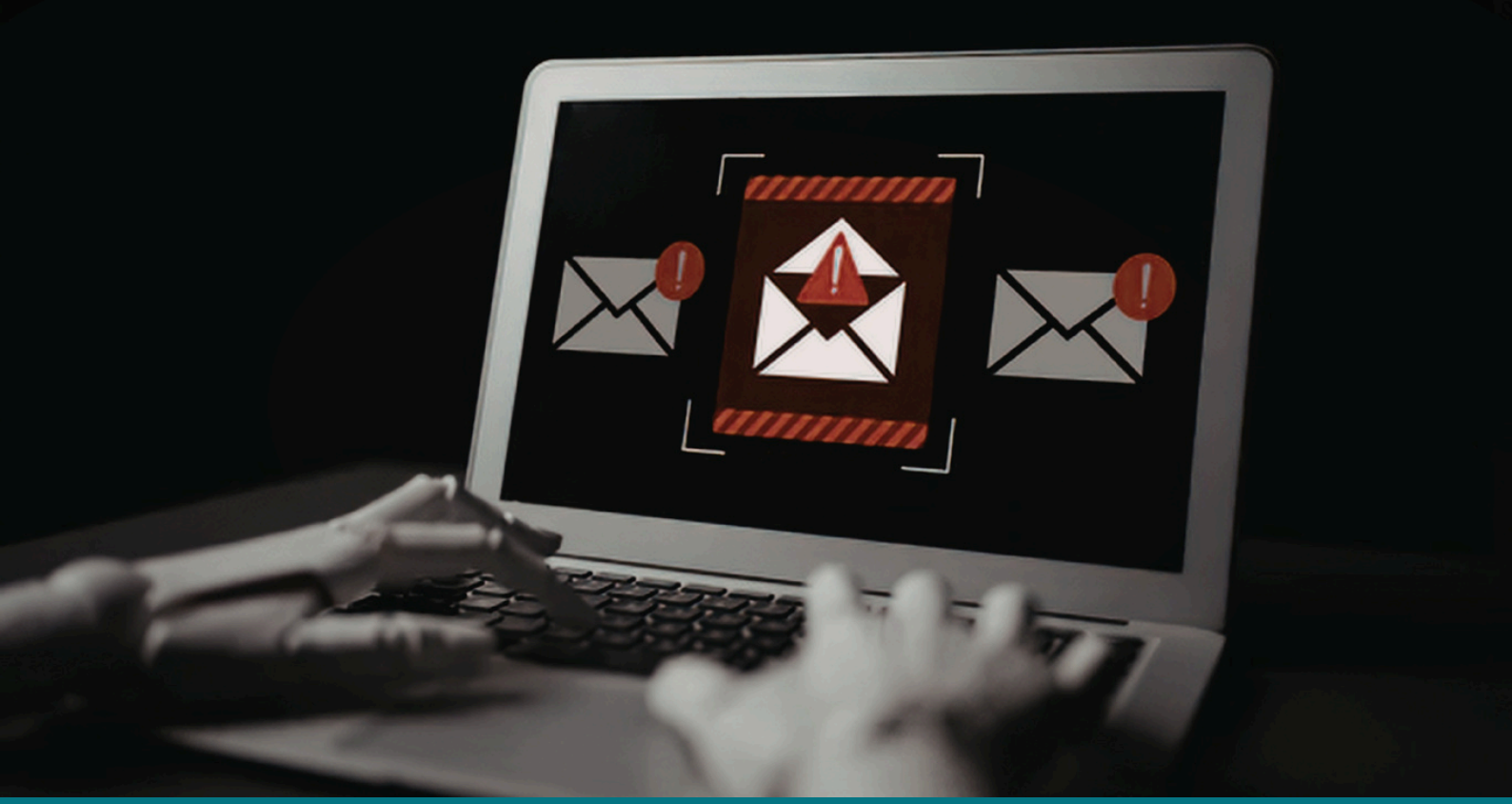
Attackers might access your systems using valid login credentials. A compromised Microsoft 365 account can expose contacts, plans, contracts, schedules and service details. It can also help an attacker pose as a trusted staff member.

Who might be targeted?

- Centre management
- Facilities management
- Security
- Finance
- Marketing
- Property management
- External contractors

Actions for centre management teams

- Use multi-factor authentication for staff and contractor accounts.
- Review who can access shared mailboxes, files and admin portals.
- Remove access when a person changes role or leaves.
- Keep privileged accounts separate from day-to-day accounts.
- Check unexpected sign in or account change alerts.



Simple rule
Always verify requests for money, data or access using a second method of contact. A familiar name is NOT proof of identity.

Stop payment and email fraud

Business email compromise can look like a normal request from a colleague or supplier. The message may ask for money to be transferred, access to IT systems or request a task is done urgently.

Common examples

- A fake invoice from a cleaning contractor.
- New bank details notification that appears to come from an existing supplier.
- An urgent payment request that appears to come from a centre director or managing agent.
- A false emergency maintenance request.

Checks that should happen every time

1. Treat a new bank account, payment route or urgent payment as a separate check.
2. Use a known phone number or contact record to confirm a request. Do not rely on the details in the request.
3. Ask a second authorised person to approve sensitive changes.
4. Keep a record of the check and the approval.
5. Report the message if the sender's account may be compromised.



Risk level: HIGH

A retailer account can become a route into centre processes, systems or restricted areas.

Watch for retailer led social engineering

A retailer can be compromised even when the centre is not. The attacker may then use the retailer's email or store manager account to contact centre staff. Retailers are trusted contacts, so the request might not look suspicious.

Requests that should ALWAYS be treated with caution

- Access to a plant room, comms cabinet or other restricted area.
- Security footage, access control, ID cards, building plans or contractor details.
- Changes to online directories or centre website details.
- Access to digital advertising systems.

How to respond

1. Pause the request, even if it sounds urgent.
2. Check the person's identity and store through a contact route already held by the centre.
3. Confirm that the request fits the person's role.
4. Use the normal approval route for access, data or system changes.
5. Tell security or IT if the account may have been compromised.

Protect the systems that run the site

System	Risk	Why it matters
Building management systems	Very high	Loss of heating, ventilation, lighting, escalators or energy controls can disrupt the building and raise safety concerns.
Access control	Very high	These systems protect plant rooms, roofs, service yards, goods lifts and control rooms.
CCTV	High	Threats include stolen credentials, unauthorised access, recorder compromise, ransomware and privacy breaches.
Parking and number plate recognition	High	An incident can cause outages, lost income, complaints, data exposure or fraudulent payments.
Public Wi Fi	High	Threats include rogue access points, credential theft, intercepted data and misuse of the service.
Digital signs and public displays	Medium to high	An attacker may post offensive content, scam QR codes, political messages or false emergency notices.

Control access to critical systems: points to review

- Named owner for each system.
- Current list of users, administrators and suppliers.
- Remote access routes and support accounts.
- Password and multi-factor authentication settings where the system supports them.
- Backups, recovery steps and supplier contacts.
- Network links between building, business and public services.
- Logs and alerts that staff or suppliers' review.





Focus on access

Know exactly what access each supplier has. Keep a record of their accounts, remote access tools, keys, access cards and permissions.

Manage supplier access

Suppliers often have access to your systems, network or restricted areas. If a supplier is compromised, your centre could be at risk.

Questions to ask each supplier

- What systems and sites can you access?
- Which staff or subcontractors can use that access?
- Do you use named accounts and multi-factor authentication?
- How do you tell us when access is no longer needed?
- How will you tell us about a suspected incident?
- Who do we call outside normal hours?
- How will service continue if your systems are unavailable?



Use the right data and service focus

Most retail cyber risks focus on retailer systems such as tills, loyalty schemes and online stores. Centre operators should focus on the systems and services they manage.

Give more attention to

- The centre website, visitor apps and customer portal.
- Digital vouchers, parking apps, event tickets and booking services.
- Newsletter lists, competition entries, event registrations and customer service records.
- Visitor analytics and parking account data.
- Gift card and centre run payment services, where used.

Keep tenant POS systems in the right place

Retailers usually operate their own point of sale systems. Do not include tenant POS systems in the centre asset list unless the operator owns or supports them. Centre run gift cards, parking payments, event tickets and booking services do belong in scope.



Keep incident plan exercises practical

Use real contact lists, approval processes and supplier details. Record any gaps in your plan and assign someone to fix them.

Prepare for an incident

Make sure your incident plan works if email, phones, building systems or suppliers are unavailable or compromised. Test it with the teams that run the centre, not just IT.

Your incident exercise should cover

- Who leads the response.
- How staff report suspicious email, account or system change.
- How to contact key people if Microsoft 365 is unavailable.
- How facilities, security, finance, marketing and property teams work together.
- Who has the authority and ability to shut down or isolate a system during an incident.
- How suppliers join the response.
- How staff record decisions, actions and evidence.
- How information is shared with retailers and visitors.
- Which events may need review for privacy, law enforcement or regulatory reporting.

Useful test scenarios

- A finance account sends new bank details.
- A retailer account asks for access to a plant room.
- A supplier's remote account is used without approval.
- CCTV or access control is unavailable.
- Digital signage shows false content.
- Parking or number plate recognition services stop working.

Ten priorities for centre operators

No.	Priority	Level
1	Identity and multi-factor authentication	Critical
2	Business email compromise and impersonation	Critical
3	Third party risk management	Critical
4	Building and smart system security	Critical
5	Access control security	Critical
6	CCTV security and privacy	High
7	Public Wi-Fi security	High
8	Parking and number plate recognition security	High
9	Incident response exercises	High
10	Retailer social engineering awareness	High

A simple 30-day review

- Confirm the owner and supplier for every shared system.
- Check multi-factor authentication and administrator access.
- Review bank details and urgent payment checks.
- List supplier remote access and physical access.
- Confirm the route for retailer requests involving access, data or system changes.
- Check that response contacts work outside Microsoft 365.
- Book one incident exercise for the centre management team, facilities, security and finance.

Questions for the next management meeting

- Which shared service would cause the most disruption if it stopped working today?
- Which supplier has the broadest remote or physical access?
- Can we verify a payment or access request without using email?
- Do we know who can change digital signs, directory listings and visitor information?
- Can we contact retailers and suppliers if our main systems are not working?
- When did the centre teams last practice a cyber incident together?



Take the next step

Every shopping centre has a unique mix of systems, suppliers and operational risks. A cyber security review can help identify vulnerabilities across building systems, access control, CCTV, public Wi-Fi, supplier access and critical business services before they become incidents. This guide highlights the importance of understanding shared systems, strengthening access controls and testing incident response arrangements.

How we can help

Contact Modern Networks for a comprehensive cyber security assessment of your site. Our experts can identify risks, assess critical systems, review supplier and remote access arrangements, and recommend practical remedial actions to help protect your operations, visitors and reputation. A proactive assessment today could prevent costly disruption tomorrow.

T: 01462 426500 | E: sales@modern-networks.co.uk | W: www.modern-networks.co.uk