BEEVER AND STRUTHERS

One Express
1 George Leigh Street
Manchester M4 5DL

The Colmore Building
20 Colmore Circus Queensway
Birmingham B4 6AT

150 Minories
London EC3N 1LS

Beever and Struthers Housing Hotwire: Fast, essential updates you can't afford to miss

Hello,

Recently, three major UK retailers including Marks & Spencer (M&S), Co-op, and Harrods were targeted in a sophisticated cyberattack attributed to the Scattered Spider group. Attackers used social engineering tactics to impersonate staff, trick IT Help Desks into resetting credentials, and bypass multi-factor authentication (MFA), ultimately gaining unauthorised access to critical systems.

Impact on Retailers:

- **Marks & Spencer (M&S):** The attack disrupted online orders and impacted store inventory, causing significant operational and financial strain. Analysts estimate potential losses of up to £200m for 2025–26, though this may be offset in part by an insurance payout. The breach triggered a £1.1bn drop in market value, hitting shares that had recently reached a nine-year high. Customer data that was accessed could possibly include names, dates of birth, contact details, order histories, and masked payment card details.

- **Co-op:** The attack caused disruptions to payment systems and led to stock shortages in stores. Data belonging to up to 20 million members was accessed, including names, email addresses, dates of birth, and contact information. No payment details or passwords were compromised.

- **Harrods:** Faced with an attempted cyberattack, the store restricted internet access at its sites as a precautionary measure. While operations continued, the incident highlighted vulnerabilities in cyber security defences.

Why It Matters for the Housing Sector:
Social housing providers, like retail organisations, manage vast amounts of personal data and depend on IT systems for core functions such as tenancy management, rent processing, maintenance, and customer engagement. A breach could expose sensitive tenant data, disrupt essential services, and erode public trust.

Recommended Security Enhancements:
These recommendations align with the National Cyber Security Centre (NCSC) guidance **(https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers)**, which stresses strong authentication, access controls, and monitoring to prevent the kinds of attacks seen in recent incidents affecting retailers.

1. **Enforce Comprehensive MFA** – Apply multi-factor authentication across all staff and systems, prioritising IT admins and contractors. Use stronger options like security keys (e.g. FIDO2-compliant devices), authenticator apps with number-matching, or device biometrics over basic SMS codes.

2. **Monitor for Suspicious Activity** – Use automated tools (e.g., Microsoft Entra ID Protection) to detect unusual logins, like access from unfamiliar locations or odd hours. Set policies to block access or trigger additional verification based on risk levels.

3. **Protect Privileged Accounts** – Audit high-level accounts (Domain, Enterprise, and Cloud Admins) regularly to ensure access is still needed, permissions are appropriate, and activity logs show legitimate use. Confirm accounts are individually assigned, not shared, and have documented justification. Use Privileged Identity Management (PIM) to enforce just-in-time access, limit use to specific tasks, and track all actions to reduce risk if an account is compromised.

4. **Strengthen Helpdesk Verification** – Update helpdesk procedures to verify identity before password resets, especially for sensitive roles. Require callbacks to verified numbers or challenge questions and never reset based on an email or a phone call alone.

5. **Detect Anomalous Logins** – Flag logins from unusual sources like VPNs or unknown IPs. Enrich logs with location and network data to spot suspicious patterns, such as logins from foreign VPNs during off-hours.

6. **Rapid Threat Intelligence Response** – Use a Security Operations Centre (SOC) with a SIEM to centralise log data, detect suspicious activity, and respond to threats in real time. Integrate threat intelligence to stay ahead of emerging attacks and quickly adjust detection rules.

7. **Educate Staff on Social Engineering** – Regularly train staff to recognise phishing, fake calls, and impersonation attempts. Use simulated phishing campaigns to build awareness and improve response.

8. **Test Incident Response Plans** – Run practice drills with cross-functional teams (e.g. IT, Housing, and Customer Services) to ensure all teams understand their roles and can detect, respond to, and recover from cyber incidents effectively.

Additionally, cyber insurance helps mitigate the impact of attacks by covering costs like data recovery, legal fees, and downtime. Many policies include expert response support, making it a key part of fast, effective recovery.

Cyber resilience matters – and we can help
Our team's here to help you stay one step ahead, with cyber audit and advisory services that cover everything from disaster recovery to incident response planning. Whether you're looking to tighten up your systems or just want to sense-check your current setup, we'll make it clear, manageable, and jargon-free.

If you would like to discuss this further, we are here to support you.

Get in touch for a no-pressure chat with our specialists today!

Narinder Sandher
Partner
E: Nsandher@beeverstruthers.co.uk
T: 03330 910411

Catherine Adulta
IT Audit Manager
E: cadulta@beeverstruthers.co.uk
T: 03330 910411

Kind regards.

Maria Hallows

Maria Hallows
Head of Social Housing