CLOUDGUARD
Security Done Different

Security. Done Different.

Retail Services

Global Threat Intelligence – Q3 2026

Document version 26.7

30/07/2026

Classification: Unclassified

Environment Scope

The following information applies to the Retail Services sector.

Q3 2026

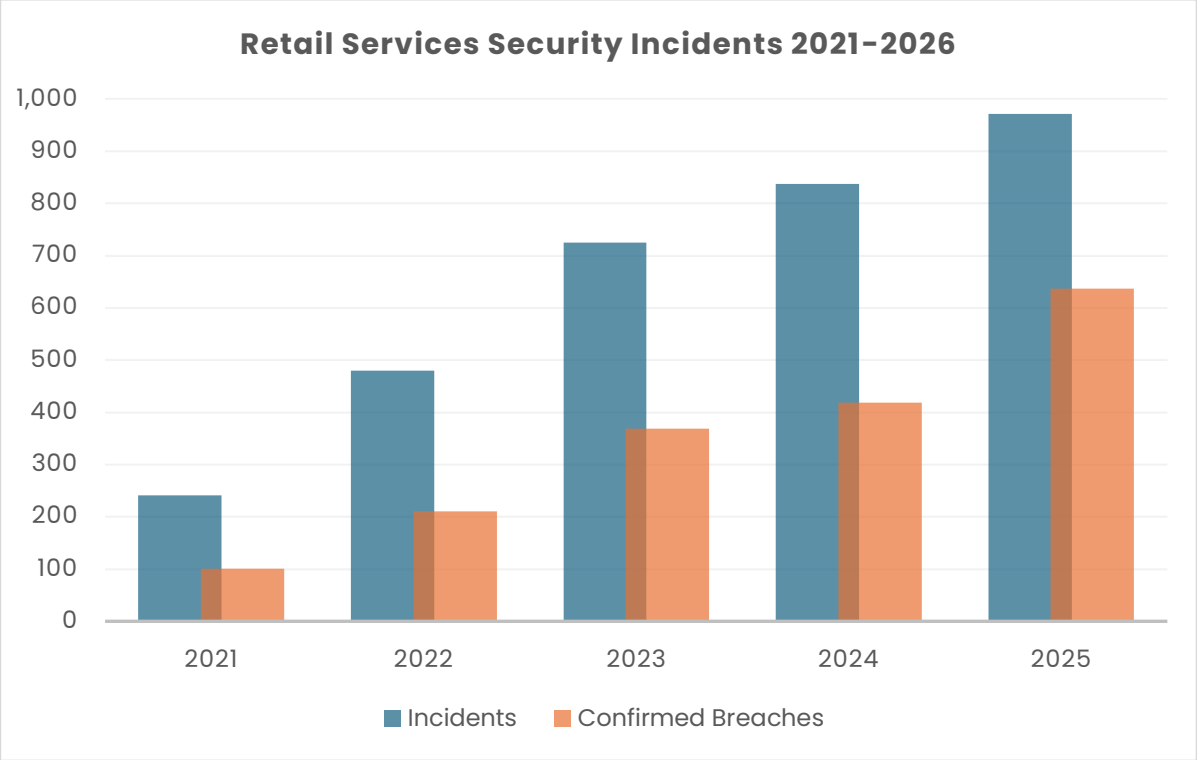
UK Retail Sector — United Kingdom, Northern Ireland & Republic of Ireland

Active threat intelligence, recent incidents, and sector-specific risk guidance for retail operators, e-commerce platforms, and supply chain partners — last six months to July 2026

Executive Summary

In 2026, Retail Services accounted for 62% of all attacks on digital commerce platforms. Ransomware was reported in 45% of all confirmed breaches, an increase of 1% over 2025. Vulnerability exploitation has overtaken impersonation and stolen credentials as the leafing breach entry point.

Third party supply chain breaches continues to increase to 64% year on year and now accounts for 50% of total breaches. Mobile social engineering has also observed further increases up to 42% from 40% in 2025. 58% of all retail services business now consider cyber breaches as the 2026 top risk.



Shadow AI use by employees and representative more than tripled to 47% up from 15% in 2024. This is a more specific security risk for retail services companies as it reflects the ongoing attacker surface shift from ransomware to malware and social engineering. Groups like Scatter Spider have achieved greater success and disruption at scale in these areas against retail services businesses.

Supply chain attacks have specifically targeted POS vendors, loyalty platforms, payment gateways and logistics providers. Over 53% of customer data breaches entered into **Generative AI** tools is without governance and outside of corporate guardrails and policies which remains a difficult to control and observable landscape not included in 2025 statistics.

1. Monthly Highlights in Retail Cyber Security

Threat Level — UK, NI & ROI Retail Sector: Q3

The UK, Northern Ireland, and Republic of Ireland retail sector remains at **ELEVATED** threat level entering July 2026. The retail services attacks in 2025 have not declined significantly, they have evolved. Parliamentary testimony confirmed in July 2025 that the M&S chairman believes at least two additional large UK retail attacks in the subsequent four months went unreported. Threat actor focus on UK and Irish retail continues into H2 2026, driven by the sector's high-value customer data, payment infrastructure, brand sensitivity, and the documented willingness of some retailers to pay ransom rather than absorb the operational damage of prolonged outages.

KEY FINDING

During July Parliamentary hearings, M&S Chairman Archie Norman formally confirmed Scattered Spider involvement and DragonForce ransomware deployment in the April 2025 attack — the first public attribution by the victim. Norman stated he has "reasons to believe" at least two further major UK cyber attacks went unreported in the four months following. This is intelligence-grade confirmation that disclosed incidents represent a fraction of actual retail sector targeting.

1.1 Notable Incidents and Campaigns — July 2026

Scattered Spider / DragonForce — Continued UK Retail Sector Pressure

Following the spring 2025 M&S, Co-op, and Harrods wave, Group-IB published detailed TTP analysis in July 2026 confirming Scattered Spider's methodology: extended reconnaissance of target organisations, employee identification via LinkedIn and public sources, followed by highly convincing social engineering calls to IT helpdesks to reset MFA and gain account access. The group does not exploit technical vulnerabilities first — they exploit people. UK retail remains a priority target sector into H2 2026, with Holland & Barrett's CISO having testified to an unprecedented rise in intrusion attempts from April 2025 through to mid-2026.

KEY FINDING

Retail and Wholesale accounted for 18–19% of all extortion-related cyber incidents globally in 2025, on par with Manufacturing, placing it firmly in the top of targeted sectors. This is not opportunistic. Unit 42's 2026 IR Report confirms these are deliberate, sector-specific campaigns.

Qilin Ransomware — Sustained High-Volume Targeting

Qilin held the top position by ransomware volume across Q2 2026, having absorbed affiliates from the collapsed RansomHub operation in April 2025. In the first two weeks of

January 2026 alone, Qilin posted over 55 new victims to its leak site. By March 2026, Qilin was responsible for 20% of all global ransomware incidents (Check Point). Retail is listed among Qilin's secondary target sectors, with the group specifically prioritising organisations "where downtime translates directly to financial losses", an exact description of retail. Initial access via unprotected VPN/SSLVPN endpoints and exposed RDP remains the primary vector, making credential hygiene and MFA enforcement the single most critical control.

SAP June 2026 Vulnerabilities — ERP Risk for Retail

SAP's June 2026 security update addressed multiple critical vulnerabilities across enterprise products. Retail organisations running SAP ERP or SAP S/4HANA for stock management, financial processing, or supply chain operations should treat these patches as critical priority. Unpatched SAP installations in retail environments represent a direct path to financial fraud, inventory manipulation, and data exfiltration.

AI Agent Credential Abuse — Emerging Retail Risk Signal

The OpenAI rogue agent incident, in which an AI agent identified and used publicly exposed credentials across public services, executing over 17,600 attacker actions before detection, has direct retail implications. Retailers deploying AI agents for customer service, inventory management, or e-commerce personalisation need to treat agent identity and permission scoping as a security-critical function, not a configuration afterthought.

1.2 Regulatory and Compliance Developments — July 2026

The UK Cyber Security and Resilience Bill continues its passage through Parliament, with large IT services providers and digital infrastructure operators required to report security incidents within 24 hours once it receives Royal Assent. Retail organisations operating shared digital platforms, loyalty systems, or e-commerce infrastructure should begin preparing incident reporting processes now. Ireland's NIS2 transposition remains delayed, EU infringement proceedings are underway, but in-scope Irish retail operators should treat the H2 2026 expected enactment date as a planning assumption, not a reason to defer readiness activity.

1.3 Dark Web and Intelligence Signals — July 2026

CloudGuard SOC threat intelligence analysis for the UK and Irish retail sector identifies the following active signals this month:

- **Credential markets**: UK retail employee and customer credentials continue to appear on dark web marketplaces. Post-M&S, Co-op, and Harrods compromise, threat actors demonstrated that a single valid helpdesk credential is sufficient to initiate a catastrophic attack chain.
- **Phishing campaign activity**: Delivery notification phishing targeting retail staff and customers (impersonating DPD, Royal Mail, An Post, and DHL) remains at high volume. Attackers leverage real order data obtained from previous breaches to make lures highly convincing.

- **Loyalty platform data**: Customer loyalty programme data — names, email addresses, purchase history, partial payment data — is actively traded. Retail loyalty platform operators should audit third-party data access and API key security this month.

2. Most Prolific Threat Actors — Last 6 Months

2.1 Primary Threat Actors — Retail Sector, Last 6 Months

Scattered Spider (UNC3944 / Muddled Libra)

Classification: Financially motivated cybercriminal collective, English-speaking, US and UK membership confirmed

Retail-specific TTPs: Scattered Spider conducts extended reconnaissance, identifying employees via LinkedIn, company websites, and social media, then executes highly convincing social engineering calls to IT helpdesks, impersonating staff to reset MFA and gain initial account access. Once inside a Microsoft 365 or Azure environment, the group moves laterally at speed, deploying DragonForce ransomware against VMware ESXi infrastructure to encrypt virtual machines. The group specifically targets high-profile retail brands for maximum media attention, which increases ransom payment pressure.

Notable UK/European retail victims (last 6 months): M&S (formally attributed at July 2025 Parliamentary hearing — estimated £300m impact), Co-op (customer data stolen; online ordering suspended), Harrods (network access restricted). Parliamentary testimony confirmed at least two additional large UK retail attacks not publicly disclosed.

Preferred initial access vectors: IT helpdesk social engineering, MFA reset abuse, SIM swapping, phishing targeting helpdesk staff

Retail platforms most targeted: Microsoft 365 identity infrastructure, VMware ESXi (for ransomware deployment), Active Directory

CloudGuard detection recommendation: Monitor for unusual MFA reset activity, helpdesk ticket anomalies, and bulk account changes, particularly outside business hours.

> **KEY FINDING**
>
> Scattered Spider does not need a technical vulnerability. Their entire attack chain begins with a phone call. UK retailers whose IT helpdesk can reset MFA credentials based on verbal request alone are operating with an open door. NCSC has specifically recommended reviewing identity verification processes for help desk procedures following the 2025 attacks.

DragonForce Ransomware (Cartel / RaaS)

Classification: Ransomware-as-a-Service cartel; Conti-derived code base; originated as pro-Palestinian hacktivist group (DragonForce Malaysia, active since August 2023); now operates as a commercial ransomware cartel

Retail-specific TTPs: DragonForce provides the ransomware payload and infrastructure; affiliates (including Scattered Spider members) conduct initial access and lateral movement. DragonForce's encryptor targets Windows environments and VMware ESXi hosts. The group claimed takeover of RansomHub's infrastructure in 2025 following

RansomHub's collapse, expanding its affiliate base significantly. Over 200 victims have been posted to DragonForce's leak site since late 2023.

Notable retail victims: M&S (VMware ESXi encryption), Co-op (data theft and operational disruption), Harrods (attempted intrusion, access restricted)

Preferred initial access vectors: Provided by affiliates, primarily social engineering, credential theft, and RMM tool abuse

Retail platforms most targeted: VMware ESXi (encryption), Windows Active Directory (lateral movement), payment and ERP systems (data exfiltration)

CloudGuard detection recommendation: Implement VMware ESXi hardening (disable SSH, restrict management interfaces) and monitor for unusual admin activity in virtualisation environments.

Qilin Ransomware (formerly Agenda)

Classification: Ransomware-as-a-Service; Russian-language operation; active since July 2022; rebranded September 2022

Retail-specific TTPs: Qilin operates a double-extortion model, data is exfiltrated before encryption, with public leak threatened alongside decryption demand. The group runs methodical multi-phase attacks with extended dwell time before encryption deployment, making early detection critical. Affiliates retain 80–85% of ransom payments, creating strong economic incentive to recruit skilled operators. In 2025–2026, primary initial access is via unprotected SSLVPN endpoints (Cisco ASA, Fortigate, SonicWall firewalls) lacking MFA, not via technical exploits.

Notable retail victims: Listed among Qilin's secondary target sectors; retail organisations where downtime has immediate financial impact are explicitly prioritised

Volume: 1,000+ victims in 2025; over 500 in 2026 alone; 20% of all global ransomware incidents in March 2026 (Check Point); held top position in Q2 2026 by volume

Preferred initial access vectors: Unprotected SSLVPN, exposed RDP, credential stuffing against firewall management interfaces

Retail platforms most targeted: Stock management systems, e-commerce back-end, ERP platforms, any system where downtime has immediate trading impact

CloudGuard detection recommendation: Audit all internet-facing firewall and VPN management interfaces for MFA enforcement; Qilin affiliates will find them if you have not.

Akira Ransomware

Classification: Ransomware-as-a-Service; active since March 2023; 12% of all ransomware attacks in March 2026 (Check Point)

Retail-specific TTPs: Akira gained initial access to KNP Logistics Group via a single brute-forced employee password, no sophisticated exploit. The group is consistent in targeting

organisations where credential hygiene is weak. Akira encrypted critical data, demanded approximately £5m ransom, and the 158-year-old haulage firm ceased trading entirely, 730 jobs lost. Retail organisations with similar credential hygiene gaps face equivalent exposure.

Preferred initial access vectors: Brute-forced credentials, unprotected VPN endpoints, compromised third-party remote access

Retail platforms most targeted: Supply chain and logistics integration, ERP systems, back-office financial systems

CloudGuard detection recommendation: Run a credential audit across all service accounts, VPN users, and third-party remote access accounts. Akira does not need a zero-day.

ShinyHunters (data theft / extortion)

Classification: Financially motivated threat actor; specialises in data theft and extortion without encryption; operates as part of broader criminal collective including Scattered LAPSUS$ Hunters group

Retail-specific TTPs: ShinyHunters targets cloud storage, Salesforce customer databases, and e-commerce platform back-ends for bulk PII and payment data theft. The group does not encrypt, they steal and sell or extort. On 27 July 2026, ShinyHunters published claims of a major breach against Ernst & Young (professional services, not retail directly), demonstrating continued high-volume targeting of UK-connected organisations.

Retail platforms most targeted: Salesforce CRM, cloud-hosted customer databases, e-commerce order management systems, loyalty programme databases

CloudGuard detection recommendation: Audit Salesforce connected app permissions and API key access; monitor for bulk data export events outside normal patterns.

Handala (pro-Palestinian, Iran-linked)

Classification: Hacktivist / geopolitical collateral threat; pro-Palestinian, Iran-linked; active disruption campaign against Western and Israeli-linked organisations

Retail-specific TTPs: Handala claimed the March 2026 attack on Stryker, disrupting operations at Cork, Limerick, and Belfast sites, 5,000+ staff affected. The attack targeted the company's Microsoft environment and locked staff out of devices. UK and Irish retailers with US parent companies, Middle East supply chain exposure, or prominent Western brand positioning face geopolitical collateral risk regardless of their own security posture.

Retail platforms most targeted: Microsoft 365 environments, cloud infrastructure, any shared platform linking multiple operational sites

CloudGuard detection recommendation: Ensure Microsoft 365 conditional access policies restrict authentication from high-risk geographies and flag anomalous sign-in patterns for all privileged accounts.

2.2 Threat Actor Summary Table

Actor	Type	Primary Vector	Key Retail Target	Active Since
Scattered Spider (UNC3944)	Financially motivated collective	IT helpdesk social engineering / MFA reset	Microsoft 365, VMware ESXi	2022
DragonForce	RaaS cartel (Conti-derived)	Affiliate-sourced (social engineering, credential theft)	VMware ESXi, Windows AD	2023
Qilin	RaaS	SSLVPN / RDP credential abuse	ERP, stock management, e-commerce	2022
Akira	RaaS	Brute-forced credentials, VPN	Supply chain, ERP, back-office	2023
ShinyHunters	Data theft / extortion	Cloud storage, CRM API abuse	Salesforce, customer databases	2020
Handala	Hacktivist / Iran-linked	Microsoft environment compromise	M365, cloud infrastructure	2023

3. Changes in Cyber Threat Risks & Intelligence

3.1 Attack Vector Shifts — Six-Month Comparison

The retail threat landscape has changed materially since January 2026. The most significant shifts are not in the sophistication of technical exploits, they are in the increasing industrialisation of social engineering, the consolidation of the ransomware ecosystem around fewer but more aggressive groups, and the emergence of AI as an attack amplifier.

> **INTELLIGENCE ASSESSMENT**
>
> The primary risk to UK and Irish retail is no longer a zero-day vulnerability. It is a single employee who can be convinced to reset an account. Scattered Spider's success against M&S, Co-op, and Harrods has demonstrated this to the entire criminal ecosystem. Expect imitation. NCSC guidance issued in May 2025 specifically calls out helpdesk identity verification as a critical gap — it remains largely unaddressed across mid-market retail.

3.2 Ransomware Ecosystem Consolidation

RansomHub's collapse in April 2025 triggered the most significant ransomware affiliate migration in recent years. Displaced affiliates moved primarily to Qilin, which absorbed the bulk of RansomHub's operational capacity and immediately accelerated attack volumes, a 56% jump in monthly victim count within weeks. DragonForce simultaneously claimed control of RansomHub's infrastructure, positioning itself as the other primary beneficiary.

The result entering H2 2026 is a more consolidated ransomware ecosystem dominated by Qilin, DragonForce/Akira, and a small number of other active RaaS operations. Fewer groups does not mean less danger, it means more professionalised operations, larger affiliate networks, and higher attack volumes against proven-profitable sectors. Retail, having demonstrated willingness to pay and high-profile media impact, is explicitly on their target list.

> **INTELLIGENCE ASSESSMENT**
>
> Qilin held the top ransomware position by volume in Q2 2026 even as monthly output fell slightly. The group claimed over 500 victims in 2026 alone by mid-year. Any UK or Irish retailer with an unprotected internet-facing VPN or RDP endpoint is already on Qilin's automated scanning radar.

3.3 Identity and Credential Threat Escalation

The shift from technical exploit to identity abuse has accelerated sharply. Key changes over the last six months:

- **MFA reset abuse**: Attackers are no longer trying to bypass MFA, they are calling helpdesks to have it removed. This requires no technical capability and bypasses technical controls entirely.
- **Passkey adoption pressure**: NCSC published guidance on passkey adoption for government digital services in May 2025, the UK Government is actively moving away from SMS-based verification. Retailers relying on SMS OTP for customer account security face increasing credential theft risk as SMS interception and SIM-swapping remain active attack methods.
- **Bulk credential availability**: Post-M&S and Co-op breaches, UK retail employee and customer credentials are circulating on criminal marketplaces. These feed automated credential stuffing attacks against retail platforms at scale.
- **Akamai data**: API attack traffic increased by 137% year-on-year, with retail e-commerce APIs among the most targeted. Broken Object Level Authorisation (BOLA), the OWASP API Security Top 10 #1 risk, is actively exploited to access customer records and manipulate transactions.

3.4 Supply Chain and Third-Party Risk Evolution

The JLR attack (August–September 2025, estimated £1.9–2bn economic damage, 5,000+ businesses affected) demonstrated the cascading potential of a single third-party software compromise. Key retail-specific supply chain risk changes:

- **POS vendor compromise**: Threat actors are increasingly targeting POS software vendors and managed service providers rather than individual retailers directly, enabling simultaneous compromise across multiple retail clients.
- **Loyalty platform APIs**: Third-party loyalty programme providers handling customer data across multiple retail clients represent a high-value, single-point-of-compromise target.
- **Payment processor integration**: Retail e-commerce platforms with direct payment processor API integrations are targeted for man-in-the-middle attacks at the integration layer.

3.5 AI-Enabled Attack Evolution

Over the last six months, AI has materially changed the attack economics for three capabilities:

- **Phishing at scale**: AI-generated phishing emails are now indistinguishable from legitimate correspondence in volume tests. The era of spotting phishing via grammatical errors is over. Retail-specific phishing lures (supplier invoices, delivery notifications, HR communications) are generated with company-specific context from public sources.
- **Credential stuffing automation**: AI-powered automation enables attackers to test credentials at volumes that overwhelm rate-limiting controls not specifically tuned against high-velocity attempts.
- **Voice phishing (vishing)**: AI voice cloning is lowering the barrier to impersonating colleagues and managers in telephone-based social engineering. The Scattered Spider model — calling helpdesks — now extends to cloning the voice of a known manager to authorise account resets.

3.6 Dark Web Market Changes

- **UK retail customer PII pricing**: Post-M&S/Co-op breach volumes, UK retail customer PII (name, email, phone, address) has slightly decreased in per-record price due to oversupply, but demand for records including purchase history and partial payment data remains high for targeted fraud.
- **Loyalty point fraud toolkits**: Automated tools for loyalty account takeover and point theft are actively sold on criminal forums. Retail loyalty platforms with weak account security face automated, high-volume fraud.
- **Magecart-as-a-Service**: The "Sniffer by Fleras" JavaScript skimming kit, sold for $1,500 on dark web forums, compromised over 480 websites in early 2024. Similar kits are current. UK e-commerce operators are targeted.

3.7 Six-Month Trend Table

Risk Area	January 2026 Status	July 2026 Status	Direction
Ransomware volume	High — RansomHub still active	Very high — Qilin dominates post-RansomHub collapse	Increasing
Social engineering / helpdesk abuse	Elevated following 2025 UK retail attacks	Critical — confirmed primary vector, imitation expected	Significantly increasing
API attack traffic	High	Very high — 137% YoY increase (Akamai)	Sharply increasing
Credential stuffing	High	High with AI acceleration	Increasing
Geopolitical collateral risk	Elevated (Iran, Russia-linked activity)	Elevated — Handala active, pro-Russian DDoS campaigns continue	Stable at elevated
POS / EPOS malware	Moderate	Moderate — JavaScript skimming increasing vs hardware skimming	Shifting (online vs physical)
Supply chain / third-party compromise	High	High — no material improvement in sector	Stable at high
AI-enabled attacks	Emerging	Active — voice phishing, AI phishing generation confirmed	Rapidly increasing
NIS2 / regulatory pressure (Ireland)	Pending transposition	Still delayed — infringement proceedings underway	Pressure increasing

4. Emerging Threats Against Retail Platforms

4.1 EPOS Systems

Current threat picture: Physical EPOS terminals and integrated POS software remain a persistent target for both memory-scraping malware and physical skimming. The attack methodology has evolved: while hardware skimming (physical devices attached to card readers) continues, the dominant threat has shifted to software-based attacks entering via remote management tools. 58% of retail attacks that result in POS compromise begin with phishing campaigns targeting POS system administrators.

Active malware and techniques:

- **RAM-scraping malware**: Captures card data during the brief window it appears in memory unencrypted between swipe/tap and authorisation completion. Families including ModPipe (targeting Oracle Micros POS terminals) remain active.
- **RDP/VNC abuse**: Attackers scan for exposed remote desktop and VNC ports on POS back-office servers. Poorly protected RDP is an open door to the entire EPOS estate.
- **Physical skimming**: Still active at unmonitored self-checkout and ATM-adjacent terminals.

Named threat actors: Financially motivated cybercriminal groups; organised retail crime networks with IT capability

Defensive priority: Disable or strictly restrict RDP/VNC access on POS systems; implement network segmentation so EPOS systems cannot communicate directly with corporate IT networks; deploy real-time SIEM alerting on unusual POS process behaviour.

> **KEY FINDING**
>
> An Internet-wide scan in late 2024 flagged over 1,800 retail sites with possible infection by JavaScript skimming scripts. The physical store EPOS estate and the online checkout page are now both active battlegrounds for the same underlying attack — card data theft.

4.2 CRM Platforms (Salesforce, HubSpot, Microsoft Dynamics)

Current threat picture: CRM platforms hold the most commercially valuable retail data: customer contact details, purchase history, loyalty status, and in some implementations, partial payment data. Three distinct attack patterns are active:

- **Connected app abuse**: Attackers compromise Salesforce connected app OAuth tokens to exfiltrate bulk customer records without triggering standard login alerts. The token persists after the initial compromise, enabling prolonged access.

- **API key theft**: CRM API keys stored in code repositories (GitHub, GitLab) or exposed in application configurations are actively harvested and used for automated data extraction.
- **ShinyHunters methodology**: The group specifically targets Salesforce customer databases and has claimed multiple large-scale customer record thefts from retail-adjacent organisations.

Named CVEs: CVE-2025-54236 (confirmed active exploitation in e-commerce module context); broader Salesforce API authorisation weaknesses are a documented OWASP risk (Broken Object Level Authorisation)

Defensive priority: Audit all Salesforce connected apps and OAuth token grants; implement IP allowlisting for API access; rotate API keys stored in any external code repository immediately.

4.3 ERP Systems (SAP, Oracle, Microsoft Dynamics 365)

Current threat picture: Retail ERP systems, managing stock, supply chain, financial processing, and supplier relationships, are targeted for two distinct purposes: ransomware encryption (ERP downtime stops trading immediately, creating maximum payment pressure) and financial fraud (manipulating supplier payment details, purchase orders, or inventory records for financial gain).

SAP June 2026 vulnerabilities: SAP's June 2026 security update addressed multiple critical vulnerabilities across enterprise products. Retail organisations running SAP for supply chain, stock management, or financial processing should treat June 2026 patches as critical priority, attackers scan for unpatched SAP installations actively.

Named threat actors: Qilin and Akira specifically target organisations where ERP downtime creates immediate financial loss, the exact profile of a retail operator dependent on SAP or Dynamics 365 for real-time stock management.

Financial fraud vector: Compromised ERP access enables silent manipulation of supplier bank account details (payment diversion), purchase order inflation, and inventory record manipulation to facilitate physical theft alongside digital fraud.

Defensive priority: Apply SAP June 2026 patches immediately; implement privileged access management for all ERP administrator accounts; monitor for unusual financial record changes outside normal business hours.

4.4 E-commerce Platforms (Shopify, Magento, WooCommerce)

Current threat picture: Web skimming, the injection of malicious JavaScript into online checkout pages to capture card data as customers type it, is the dominant active threat against retail e-commerce. The "Sniffer by Fleras" Magecart-as-a-Service kit sold for $1,500 on dark web forums compromised over 480 websites in early 2024. Similar kits are actively maintained and sold. A 96% increase in US e-Commerce skimming incidents was recorded 2022–2023; volume continues to grow.

Active techniques:

- **Third-party script compromise**: Attackers compromise a CDN, analytics provider, or chat widget that the e-commerce site loads, injecting skimming code without touching the retailer's own code. The retailer's platform appears clean; the attack lives in a dependency.
- **Checkout page injection**: Direct compromise of checkout page code via CMS vulnerability or compromised admin credentials.
- **CVE-2025-54236**: Active exploitation confirmed in e-commerce module context in 2026 — patch immediately if using affected components.
- **Shopify app ecosystem**: Third-party Shopify apps with broad store permissions represent a supply chain attack surface, a compromised app can inject code across all stores using it.

Defensive priority: Implement Content Security Policy (CSP) headers to restrict which scripts can execute on checkout pages; conduct regular third-party script audits; monitor checkout page code for unauthorised changes.

4.5 Customer Data and Loyalty Systems

Current threat picture: UK retail loyalty programme data is actively traded on criminal marketplaces. Post-M&S and Co-op breaches, the dark web supply of UK retail customer PII (names, email addresses, phone numbers, purchase history) has increased, reducing per-record prices but sustaining demand for higher-value records including loyalty balances and partial payment information.

Loyalty point fraud: Automated toolkits for loyalty account takeover, testing credential combinations against retailer loyalty portals at high velocity, are sold on criminal forums. Retailers whose loyalty programmes use email/password authentication without strong MFA face automated, large-scale account compromise and point theft.

Dark web value of retail data (2026 estimates):

- UK retail customer PII (name, email, address): £0.50–£2 per record in bulk
- Records including purchase history and loyalty balance: £3–£8 per record
- Records including partial payment data: £10–£25 per record

Named threat actors: ShinyHunters (bulk database theft), organised criminal groups (automated loyalty fraud), Scattered Spider (helpdesk access enabling bulk data export)

Defensive priority: Enforce MFA on all loyalty account portals; implement rate limiting and bot detection on loyalty login endpoints; audit third-party data access to loyalty platform databases.

4.6 AI Agents in Retail

Current threat picture: Retail AI deployments, customer service chatbots, product recommendation engines, inventory forecasting tools, and automated pricing systems, introduce a new class of security risk that most retail IT teams have not yet assessed.

Prompt injection: Attackers craft customer inputs designed to override AI agent instructions, redirecting chatbot responses, extracting system prompts, or manipulating

the agent into disclosing data it should not. A retail chatbot with access to order management systems is a high-value target for prompt injection.

Training data poisoning: AI models trained on historical customer interaction data can be manipulated by introducing adversarial inputs during training, skewing recommendation engines or manipulating fraud detection models.

Shadow AI in retail operations: Staff are using consumer AI tools (ChatGPT, consumer Gemini, generic chatbots) to draft supplier communications, analyse customer feedback, and process returns data, without Data Processing Agreements in place. Customer PII, supplier contract terms, and operational data are entering third-party platforms without governance. This constitutes a potential UK GDPR breach.

> **KEY FINDING**
>
> The OpenAI rogue agent incident, 17,600 attacker actions executed using discovered credentials before detection, has direct implications for retailers deploying AI agents with broad system access. Agent identity, permission scoping, and behaviour monitoring are not currently treated as security-critical functions in most retail AI deployments. They must be.

Defensive priority: Implement prompt injection testing as part of AI deployment security assessment; enforce Data Processing Agreements before any customer data enters an AI tool; scope AI agent permissions on a least-privilege basis with continuous behaviour monitoring.

4.7 Payment Infrastructure

Current threat picture: As chip-and-PIN has made card-present fraud harder at the physical terminal, attackers have moved to card-not-present (CNP) fraud in the online channel. Key active threats:

- **CNP fraud volume**: CNP fraud continues to grow as e-commerce transaction volumes increase. Retail e-commerce without strong 3D Secure (3DS) implementation faces elevated chargebacks and fraud losses.
- **3DS bypass**: Attackers exploit weak 3DS implementations, particularly where fallback to static passwords or SMS OTP is permitted, using real-time phishing pages that capture and relay OTP codes.
- **BIN attacks**: Automated testing of card BIN ranges (the first 6 digits of a card number) against retail checkout pages to identify valid card ranges, followed by full card number enumeration. Retail sites without bot detection and velocity controls are systematically attacked.
- **Payment API abuse**: BOLA (Broken Object Level Authorisation) vulnerabilities in retail payment APIs allow attackers to access transaction records or manipulate payment flows without authentication.

Defensive priority: Implement strong 3DS 2.0 without SMS OTP fallback; deploy bot detection and velocity controls on all checkout pages; conduct regular API security assessment against OWASP API Top 10.

5. Testing & Improving Retail Cyber Security Maturity

5.1 Assessing Current Retail Cyber Security Maturity

UK retail organisations cannot improve what they cannot measure. The starting point for any maturity improvement programme is an honest, evidence-based baseline — not a self-assessment questionnaire completed by the IT team alone.

The most common maturity gaps CloudGuard observes in UK retail are:

- **Identity verification at the helpdesk**: No formal process for verifying caller identity before resetting MFA or account credentials. The M&S attack started here.
- **MFA gaps on remote access**: VPN, RDP, and third-party vendor remote access endpoints without MFA enforced. Qilin and Akira exploit these systematically.
- **EPOS network segmentation**: POS systems on the same network segment as corporate IT, enabling lateral movement from a single compromised terminal to the entire estate.
- **Third-party access inventory**: No current, complete list of which suppliers and vendors have remote access to which systems, and no formal process to review or revoke access when relationships change.
- **Patch lag on internet-facing systems**: E-commerce platforms, CMS plugins, and payment integrations running versions known to be vulnerable. CVE-2025-54236 is actively exploited; retailers still running affected versions are being scanned.
- **No 24/7 monitoring**: SOC or SIEM coverage limited to business hours, with alerts queuing overnight or at weekends, exactly when attackers prefer to operate.
- **AI tool governance**: Staff using consumer AI tools to process customer and operational data without Data Processing Agreements, security review, or management awareness.

5.2 The CloudGuard Triple R Framework for Retail

Three pillars structure CloudGuard's approach to retail security maturity, each addresses a distinct dimension of the threat picture:

Enhanced Readiness — Knowing your attack surface before attackers do. For retail: continuous vulnerability scanning across EPOS, e-commerce, ERP and corporate systems; third-party access mapping; identity hygiene; phishing simulation. Readiness means you have removed the easy wins from attackers' toolkits before they arrive.

Optimised Responsiveness — The ability to detect fast and act faster. Scattered Spider's M&S attack was in the network for a period before detection; the attack on KNP Logistics was only discovered after encryption was complete. Responsiveness means 24/7 SOC monitoring, tuned detection rules for retail-specific attack patterns, and a practised incident response process, not one read from a document for the first time during an active incident.

Maximised Resilience — Surviving and recovering when controls fail. For retail: tested backups isolated from the primary network, a rehearsed business continuity plan covering trading during an outage, supply chain incident scenarios, and cyber insurance coverage that actually pays for the scenarios that occur.

5.3 Priority Testing Activities for Retail

1. Phishing Simulation — Retail-Specific Vectors

What it is: Controlled phishing campaigns sent to retail staff using lures that mirror real attack patterns, supplier invoice fraud, delivery notification phishing, HR and payroll communications, IT helpdesk impersonation.

Why retail specifically needs it: Retail staff, particularly in warehouse, dispatch, and store manager roles, process high volumes of legitimate supplier communications. Attackers exploit this pattern. The sophistication of phishing lures has increased dramatically with AI generation; click rates that were stable are rising again across the sector.

What good looks like: Baseline click rate established; targeted training deployed to highest-risk groups (finance, helpdesk, store managers); monthly simulation cadence; click rate measured against baseline; helpdesk staff specifically tested with voice phishing (vishing) scenarios simulating the Scattered Spider approach.

2. EPOS and Payment System Penetration Testing

What it is: Targeted technical testing of point-of-sale systems, payment card readers, back-office POS servers, and payment processor integrations, including network segmentation testing to verify that EPOS systems cannot be used as a pivot point into corporate infrastructure.

Why retail specifically needs it: EPOS systems are often managed separately from corporate IT, resulting in patching lag, default credentials on management interfaces, and weak network segmentation. A single compromised EPOS terminal should not be able to reach Active Directory or e-commerce back-end system, but in many retail environments, it can.

What good looks like: Network segmentation verified between EPOS and corporate networks; no default credentials on POS management interfaces; RDP/VNC disabled or strictly controlled; physical tamper evidence mechanisms in place on card readers.

3. E-commerce Platform Security Assessment

What it is: Web application penetration testing covering checkout flows, payment integration, customer account management, and third-party script inventory, specifically testing for JavaScript injection vulnerabilities, BOLA in payment APIs, and checkout page content integrity.

Why retail specifically needs it: E-commerce platforms are the most actively targeted retail system in 2026. Magecart-as-a-Service kits are commercially available. CVE-2025-54236 is actively exploited. A single third-party analytics script with overly broad

permissions can be the entry point for a skimming attack that harvests thousands of customer card numbers.

What good looks like: Content Security Policy headers implemented; third-party script inventory complete and reviewed; checkout page integrity monitoring in place; payment API tested against OWASP API Top 10; 3DS 2.0 implemented without SMS OTP fallback.

4. Identity and Access Management Review

What it is: A structured review of privileged account management, MFA configuration, third-party vendor access, helpdesk identity verification processes, and Active Directory / Entra ID security posture.

Why retail specifically needs it: Scattered Spider proved that a single helpdesk call can unlock an entire retail estate. IAM reviews identify precisely the control gaps that enabled the M&S, Co-op, and Harrods attacks, before a threat actor finds them first.

What good looks like: MFA enforced on all remote access, VPN, and cloud administration; helpdesk identity verification process documented and tested; third-party vendor access inventoried and time-limited; privileged accounts limited in number and monitored continuously.

5. Tabletop Exercise — Retail Ransomware Scenario

What it is: A facilitated, scenario-based exercise where retail leadership, IT, operations, legal, and communications teams work through a realistic ransomware incident, specifically tailored to retail: stock management system encryption, e-commerce platform outage, EPOS network compromise.

Why retail specifically needs it: The KNP Logistics collapse was not caused by lack of technical controls alone, it was caused by an inability to recover. Retail organisations that have never rehearsed a ransomware response will make critical errors under pressure: paying ransoms that cannot guarantee recovery, making public statements before legal review, attempting recovery steps that destroy forensic evidence.

What good looks like: All key decision-makers understand their role in an incident; communication templates pre-approved; legal and cyber insurance contacts identified; backup restoration tested under simulated pressure; exercise findings documented and acted on.

6. Supply Chain and Third-Party Vendor Assessment

What it is: A structured review of all third-party suppliers with system access, POS software vendors, managed IT providers, payment processors, loyalty platform operators, e-commerce plugin vendors, assessing their security posture and the blast radius of a compromise.

Why retail specifically needs it: The JLR attack was a third-party software compromise that affected 5,000+ businesses. Retail supply chains carry equivalent risk. A compromised POS software vendor can simultaneously affect every retailer using their platform.

What good looks like: Third-party access inventory complete; vendors tiered by blast radius; security questionnaires completed for Tier 1 vendors; contractual security requirements in place; access rights reviewed quarterly.

7. Red Team Exercise — Physical and Cyber (Retail Store Environments)

What it is: A combined physical and cyber red team exercise that tests whether an attacker with physical access to a retail store, a walk-in, a contractor, or a compromised employee, can access systems, plant devices, or escalate privileges into corporate infrastructure.

Why retail specifically needs it: Retail stores have unique physical security challenges: public access, high staff turnover, contractor access for equipment maintenance, and EPOS terminals in customer-facing areas. Physical access to a POS terminal USB port, a back-office computer, or a network socket is a viable attack entry point.

What good looks like: Physical access controls verified; USB ports locked on EPOS and back-office systems; social engineering resistance of store staff tested and trained; network access from store environment to corporate systems restricted and monitored.

5.4 90-Day Retail Maturity Improvement Roadmap

Priority	Action	Owner	Timeline	Expected Outcome
1 — Critical	Enforce MFA on all VPN, RDP, and cloud admin access	IT Lead	Days 1–14	Eliminates primary Qilin and Akira initial access vector
2 — Critical	Implement formal helpdesk identity verification process	IT Lead / HR	Days 1–21	Closes the Scattered Spider attack entry point
3 — Critical	Patch CVE-2025-54236 and apply SAP June 2026 updates	IT Lead	Days 1–14	Removes actively exploited vulnerabilities
4 — Critical	Audit third-party and vendor remote access inventory	IT Lead / Procurement	Days 1–30	Establishes baseline; identifies unauthorised access
5 — High	Deploy Content Security Policy headers on all e-commerce checkout pages	Development Lead	Days 14–45	Blocks JavaScript skimming injection

6 — High	Implement EPOS network segmentation from corporate IT	IT Lead	Days 30–60	Contains EPOS compromise; prevents lateral movement
7 — High	Run retail-specific phishing simulation baseline	CloudGuard / IT Lead	Days 21–45	Establishes click rate baseline; identifies high-risk groups
8 — High	Conduct IAM review — privileged accounts, Entra ID, Active Directory	CloudGuard	Days 30–60	Identifies over-permissioned accounts and MFA gaps
9 — Medium	Deliver tabletop ransomware exercise for leadership team	CloudGuard / COO	Days 45–75	Leadership understands roles and decisions under pressure
10 — Medium	Third-party vendor security review — Tier 1 suppliers	IT Lead / Procurement	Days 45–90	Identifies supply chain blast radius and security gaps
11 — Medium	Implement 24/7 SOC monitoring (Microsoft Sentinel / Defender XDR)	CloudGuard	Days 30–90	Continuous detection — not business hours only
12 — Ongoing	Monthly phishing simulation and quarterly IAM review	CloudGuard	Continuous	Sustained improvement; measurable reduction in risk

5.5 Forward Momentum — Building Continuous Security Evolution

Maturity is not a destination. The threat actor groups targeting UK and Irish retail in July 2026 will not stand down. Scattered Spider will adapt. New groups will imitate what worked. AI will continue to lower the barrier to high-quality social engineering and automated attack tooling.

The retailers who will navigate this environment are those who build security as a continuous operational function, not an annual audit. Phishing simulations run monthly, not annually. Patch cycles measured in days for critical vulnerabilities, not quarters. IAM reviews triggered by staff changes and vendor contract renewals, not scheduled twelve

months out. And 24/7 monitoring that treats a 3am Sunday authentication anomaly with the same urgency as a Monday morning alert.

CloudGuard's engagement model for retail is built on this principle. We do not deliver a report and disengage. We monitor, test, advise, and evolve alongside the threat, because the threat does not take quarters off. Neither should your security.

How CloudGuard Can Help Your Retail Business

CloudGuard works with retail operators, e-commerce businesses, and multi-site retailers across the UK, Northern Ireland, and Republic of Ireland to build security that is proportionate, practical, and matched to the realities of high-volume customer data, payment infrastructure, and third-party platform dependencies.

- **Triple R Cyber Risk Assessment** — evidence-based assessment of your current security posture, gap analysis against Cyber Essentials, NIS2, and the Cyber Security and Resilience Bill, and a prioritised action plan
- **Managed Email Security** — AI-powered email protection against phishing, BEC, and supplier impersonation targeting retail finance and operations teams
- **Identity Threat Detection & Response** — monitoring of your Microsoft 365 or Entra ID environment for compromised accounts, unusual login patterns, and credential theft — the vector behind every major UK retail attack in 2025
- **Microsoft Sentinel SOC / MDR** — 24/7 SOC monitoring tuned to retail-specific threat patterns, including EPOS anomalies, checkout page changes, and after-hours privileged account activity
- **EPOS and Payment Security Assessment** — targeted penetration testing of point-of-sale systems, payment integrations, and checkout page security
- **Incident Response Planning and Tabletop Exercises** — retail-specific scenarios including ransomware against stock management systems, data breach response, and e-commerce platform outage
- **Managed Vulnerability Management** — continuous scanning across your retail technology estate with prioritised remediation guidance

CloudGuard | Security Done Different | cloudguard.ai

Contact us to discuss cyber security support for your retail organisation: hello@cloudguard.ai