

Protecting Retail in Today's Threat Landscape

The retail industry knows that one-size **doesn't fit all.**



01. Retail Cyber Attacks are Rising and Spreading Fast¹

The first half of 2025 has seen a worrying increase in cyber attacks across the UK retail sector. High-profile breaches at some large UK retailers have grabbed headlines, but they represent just the visible tip of a much larger iceberg. Many more incidents likely go unreported, often due to reputational risk or incomplete attribution.

It's not just retailers themselves who are under fire. **Attackers are increasingly targeting the supply chain infrastructure that underpins retail operations**, from logistics and payment systems to third-party platforms and vendors. The downstream impact can be both severe and sustained.

In the case of one of those affected, a breach that began in April is projected to cost the business **at least £300 million in lost profits**, disrupting operations across departments and store networks².

What can make retail vulnerable is the **sheer scale and interconnectivity of its physical footprint**. Unlike many other industries, retailers operate hundreds, sometimes thousands, of digitally linked locations. This can create a dangerous dynamic; **once a breach succeeds at one node, it can cascade rapidly across the entire network**, potentially crippling operations nationwide within hours.

02. Shopping for Retail Targets: Why this Sector is Vulnerable

Retailers today face a wide range of cyber threats, including phishing campaigns, ransomware attacks, and supply chain compromises. Threat actors use malware, credential theft, and sophisticated social engineering techniques to breach defences, often with alarming success.

Yet despite being a high-value target, **cybersecurity investment in retail has historically lagged behind**. Many organisations still rely on legacy systems never designed to withstand modern threat vectors. In a sector defined by tight margins and uneven digital transformation, security hasn't always been treated as a strategic priority.

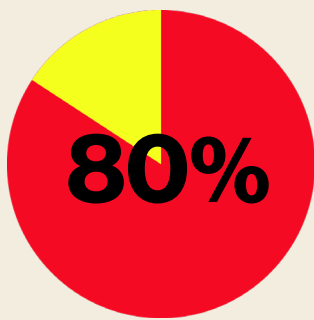
This has made retail a magnet for increasingly sophisticated attackers, including groups like **DragonForce³** and **Scattered Spider**, who target industries rich in personal and financial data. With retailers collecting and storing vast volumes of customer information, they remain a top target for cybercriminals seeking monetisable assets.

¹ Verizon, Data Breach Investigations Report, 2025

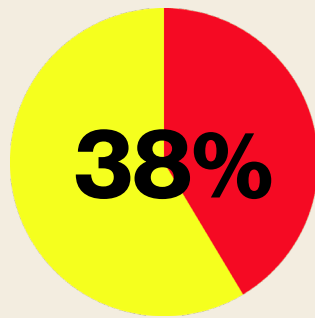
² Verizon, Data Breach Investigations Report, 2025

³ Tech Native, Navigating Cyber Threats in the Retail Sector, 2025

Recent industry research reveals the scale of the issue⁴



80% of the UK's top 50 retailers are exposed to at least one critical cyber vulnerability.



38% of the UK's top 50 retailers face risks across **all 5 major threat categories**: outdated software, vulnerable services, email security weaknesses, ransomware exposure, and certificate issues.

These are not isolated oversights. They point to a systemic fragility across the sector and a growing attack surface that threat actors increasingly see as low-hanging fruit.

Attackers are also exploiting **trusted but overlooked channels**. By embedding malicious software within systems previously considered safe, they're bypassing perimeter defences and gaining access to sensitive environments through indirect means. This reinforces the need for **robust cybersecurity practices that extend across every link of the retail supply chain**.

03. The Shifting Sophistication of Retail Attacks

Verizon's 2025 **Data Breach Investigations Report (DBIR)**, now in its 18th year, highlights the rising complexity and coordination of cyber attacks across industries and retail is no exception. While the **top three threat categories** remain consistent: **System Intrusion, Social Engineering, and Basic Web Application Attacks**, what has changed is how these threats are being deployed, and the kinds of data they now target.

In the past, retail breaches primarily centred on **payment card data**. But attackers have evolved. Their focus has shifted toward **customer credentials, loyalty accounts, and internal operational data** information that is often easier to access, more valuable, and harder to track.

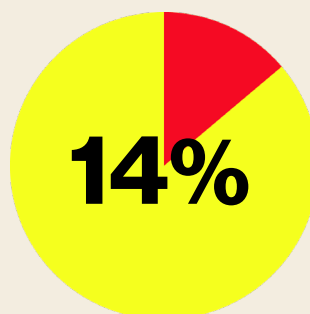
System Intrusion featured in **53% of breaches** analysed in the 2025 DBIR. Of these, **75% involved ransomware**, which continues to grow in both scale and sophistication:

- Ransomware appeared in **44% of all breaches**, up from 32% the year prior.
- This marks a **37% year-on-year increase**, even as average ransom payments have fallen.
- Robust cybersecurity is no longer a requirement - attackers are now exfiltrating data and using **extortion-style leaks** to pressure victims, making containment and reputational recovery more difficult.

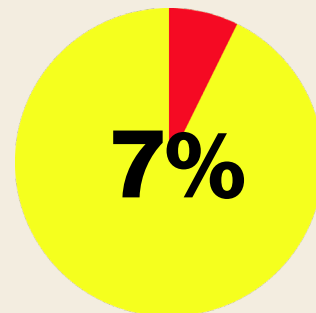
Espionage and third-party risks are on the rise

One of the most notable shifts is the **rise in espionage-motivated attacks**. In 2024⁵, these made up just 1% of breaches. This year, **they've jumped to a surprising 9%**, suggesting that some retail organisations are being targeted not only for financial reasons, but for competitive or strategic advantage.

Meanwhile, **third-party involvement was present in 30% of breaches, double** the proportion reported the previous year. Yet according to the UK's Cybersecurity Breaches Survey⁶



14% of businesses only have reviewed the risks posed by their immediate suppliers.



7% only have assessed their broader supply chain.

This gap between **risk exposure** and **risk awareness** poses a growing concern for retail organisations.

These shifts in attacker tactics, motivations, and points of entry make one thing clear: **retail cybersecurity can no longer rely on outdated assumptions or narrow threat models**. The playing field has changed, and the stakes have risen. A **robust, retail-specific cybersecurity strategy is no longer optional, it's a strategic necessity**.

⁴ Tech Native, Navigating Cyber Threats in the Retail Sector, 2025

⁵ Verizon, Data Breach Investigations Report, 2025

⁶ GOV.UK, Cyber Security Breaches Survey, 2025

04. What Can Retailers Do? Moving from Response to Readiness

Too often, cybersecurity efforts begin **after the breach**, when the damage is already done. In today's threat environment, particularly for retail that reactive approach is no longer sustainable.

Just as importantly, cybersecurity should not be viewed as a purely technical issue. It's not just about firewalls, patching, or endpoint detection. **It's organisational. It's preparational.**

Retailers need **a holistic cybersecurity strategy**, one that spans systems, people, processes, and partners. That means:

- **Training and awareness** at every level, from head office to frontline store staff
- **Proactive threat modelling and breach simulations** to pressure-test real-world response
- **Audit and modernisation of legacy systems**, with a focus on third-party and supply chain touchpoints
- **A readiness mindset** that treats cybersecurity as a business continuity function, not just an IT responsibility

In some cases, this may require a fundamental rethink of cybersecurity architecture replacing fragmented defences with integrated, intelligence-led systems designed to withstand the evolving tactics of modern attackers.

05. How Verizon Business Can Help You Now

Improving your security posture isn't about waiting for an incident to happen. It's about taking steps across the entire cybersecurity lifecycle.

Verizon's four-pronged approach covers:

- 1 Risk Management** — Benchmarking risk against DBIR threat scenarios. Building prioritised, cost-effective security plans supported by Governance, Risk and Compliance, Offensive Security, and Threat Intelligence services.
- 2 Threat Detection** — Helping customers identify, contain, and recover from advanced cyberattacks through Detection & Response, Recover Solutions, and expert Cybersecurity Consulting.

3 Trusted Connections — Secure network connections powered by global threat intelligence and advanced tools for faster detection, response, and recovery. Services protect cloud, network, and endpoints while simplifying security and reducing costs.

4 Trusted Interactions — Ensuring secure interactions for customers, employees, and partners (both human & device) across our network, from core to edge.

Practical steps you can take now

- **Security Assessments** — Identify gaps in your cybersecurity posture, uncover hidden vulnerabilities, and map your exposure to real-world threats.
- **Incident Response Planning** — Strengthen your ability to respond with robust, tested plans that can minimise confusion and downtime.
- **Breach Simulation Exercises** — Run tabletop simulations to test your teams under pressure and highlight areas for improvement.
- **Threat Intelligence** — Gain visibility into how and where your confidential data may be exposed including on the dark web.
- **Third-Party Risk Analysis** — Evaluate the security maturity of your broader supplier and partner ecosystem, and reduce points of inherited risk.

We have a deep understanding of the risks retailers face, because they are the same ones we face every day in our own retail business. With over **6,000 Verizon-owned and partner retail locations** across North America, we apply the same standards, urgency, and thinking to our own operations.

We understand that **retail cybersecurity can be different** because what's at stake isn't just data. It's your operations, your reputation, your customer trust, and the ability to stay open tomorrow.

References

1. [Verizon DBIR](#)
2. [Retail Attacks Put Cybersecurity in the Spotlight | ICAEW](#)
3. [Navigating Cyber Threats in the Retail Sector](#)
4. [Most Retailers Are Vulnerable to Cyber Attacks, Says New Report](#)
5. [Cybersecurity Breaches Survey 2025 - GOV.UK](#)