# Tackling the retail sector’s unprecedented wave of cybercrime

The shopping experience has fundamentally changed, with online shopping and in-store apps that offer the latest deals and savings allowing for unique customer profiles that support truly bespoke experiences. From small local stores to global brands, the retail sector generates, manages, and stores more data than ever before, including customer information (generated online and in-store), as well as supply chain and asset tracking data.

But each data transfer point presents a channel through which bad actors can access these volumes of corporate and personal data, as well as introducing harmful software into the underlying infrastructure in order to hold it to ransom. While physical and digital security measures may already have been established, the fast pace of modern cybercrime demands a fresh, proactive approach to cyber security at corporate headquarters, store locations, warehouses, and across online channels and supply chains.

The range of threats that an effective cyber posture must account for continues to expand, and now includes account takeover, credit card fraud, phishing, web scraping, API abuses, and distributed denial of service (DDoS) attacks. Although many of these are familiar and dependable countermeasures already exist, the rise of AI has allowed them to be automated, allowing criminals (including state-sponsored bad actors) to attack at scale, impacting both profit and reputation.

All this puts a considerable strain on IT teams, who struggle implement the latest threat intelligence as it becomes available and often fail to detect ‘back doors’ to critical data until it is too late. We have seen the disastrous results of these breaches multiple times in recent months, such as the breach Marks & Spencer suffered in April 2025. The company’s share prices were significantly affected, with its losses estimated as at least £300m. The same cybercriminals would later target Jaguar Land Rover, forcing it to make multiple employees redundant as production lines were suspended.

We must also consider the reputational damage that follows breaches like this, which often proves impossible to recover from. Rigorous data protection regulations, such as the GDPR, require retailers to ensure data is collected, transferred, and stored with the utmost care, as well as to inform customers if a breach occurs. In this worst-case scenario, rebuilding customer confidence will prove challenging, as we saw when the Co-op’s offer of a £10 voucher to affected customers was widely deemed inadequate.

The cyber threat landscape never stays still for very long, with new threats emerging regularly. This evolution will only accelerate as the retail sector adopts smart technology, Cloud platforms, and SaaS applications, while cybercriminals utilise bots and automation to intensify attacks. Retailers must therefore treat cyber security with the same seriousness physical security systems and collaborate closely with technology partners to develop fully integrated systems that provide customers with complete peace of mind.