


The M&S cyber attack: Lessons for UK retailers

27 May 2025  Conor Moran

In light of the recent cyber attack on Marks & Spencer (M&S), UK retailers have been presented with a stark reminder of the significant legal and operational risks posed by cyber attacks.

In addition to the M&S incident, the retail sector has also witnessed Co-Operative being forced to shut down part of its own IT systems after a hacking attempt (30 April 2025), and Harrod's experiencing system outages due to a cyber attack (1 May 2025). These incidents highlight the critical considerations across cybersecurity and data protection that all retailers must address to protect their business operations and their customers.

The M&S cyber attack

M&S first revealed it was dealing with a "*cyber incident*" on 21 April 2025 after customers reported payment issues and delays receiving online orders over the Easter weekend. This resulted in M&S experiencing significant disruption to its services, including some inability to accept contactless payments, the suspension of online orders in the UK and Ireland, and 'click and collect' service interruptions. This also led to empty shelves in some M&S stores, M&S having to ask around 200 agency staff to stay home, and remote employees being locked out of accessing IT systems.

Cybersecurity considerations

Containment, response, and recovery are key pillars of cybersecurity. The M&S incident emphasises the pressing need for all companies to proactively implement comprehensive cybersecurity frameworks to ensure preparedness for any and all cyber threats.

The NCSC published a recent blog post on these recent attacks on the retail sector. Some of the key recommendations made by the NCSC are to:

- Ensure multi-factor authentication is deployed across all systems;
- Enhance monitoring against unauthorised account misuse;
- Review how your business helpdesk manages the resetting of passwords; and
- Ensure your IT team can identify logins from atypical sources, such as rogue VPNs.

Another crucial detail emphasised in response to these incidents is the importance of retailers detecting threat actors who are using an employee's legitimate access. All retailers should use these incidents to focus the minds on putting in place:

- detailed incident response plans and improved disaster recovery capability,
- conducting penetration testing on their IT systems,
- monitoring and reviewing security controls, and
- ensure all staff are appropriately trained to ensure awareness of cyber risks.

Prevention and resilience should be the primary focus on all retailers in light of these cyber attacks. Retailers should also ensure that suppliers and third-party service providers adhere to similar cybersecurity standards (as noted in further detail below).

Data breach response and regulatory obligations

In order to comply with UK GDPR and the Data Protection Act 2018, M&S and any other similarly affected retailers have specific obligations where a cyber attack results in a personal data breach.

- An organisation must **report a personal data breach to the Information Commissioner's Office** (ICO) without delay, and in any event within 72 hours of becoming aware of the breach if it is likely to result in a risk to the rights and freedoms of individuals.
- Additionally, if the breach is likely to result in a **high risk to individuals' rights and freedoms, those individuals must be informed** without undue delay.
- Where a significant cyber incident occurs, organisations **may also need to report this to the NCSC**.

Article 32 of UK GDPR requires organisations to **process personal data securely** by means of "*appropriate technical and organisational measures*". This means all retailers must ensure the ongoing confidentiality, integrity, availability, and resilience of their IT systems and services, both to prevent breaches and to respond effectively if any breaches occur.

For retailers, this means proactively putting in place **robust data breach detection, investigation, and reporting procedures** in order to ensure the business can quickly and accurately assess the nature of any cyber attack in a narrow timeframe to meet the reporting obligations to the ICO.

All staff should be trained on personal data breaches, and appropriate internal policies and procedures must be implemented to address the risks of cyber crime. Given cyber attacks may include ransomware and data theft, the risk to personal data of individuals can be significant.

We strongly recommend that our clients carry out **simulated exercise** where they go through the stages of a cyber attack and their response with their legal, cyber/ IT and other key decision makers to prepare their response to a real attack. Whilst it is not uncommon for cybersecurity teams to conduct these exercises, we find that they are often carried out in silos with the legal and compliance teams not properly involved.

Supply chain liability and third-party risk management

Any cyber attacks may also affect contractual arrangements with other third parties, and cause a retailer to breach the provisions of contracts with such third parties. This could therefore trigger breach of contract claims from third parties if service levels or data security obligations are not met. Whilst understandably many companies focus on the risks of regulatory enforcement action, cyber attacks can also create potential contractual liability for an organisation that has failed to implement appropriate technical and security measures which has led to a **breach of contract**. For many retailers, the risk of being sued or losing key customer/ supplier contracts could actually be more significant than the threat of regulatory action. However, in our experience, this risk is often overlooked.

A further related consideration for retailers in light of the M&S cyber attack is the importance of managing third-party risks in retail supply chains. Retailers remain responsible for compliance with UK GDPR and the Data Protection Act 2018, even when outsourcing functions to third parties.

Therefore all UK retailers should conduct thorough **due diligence on suppliers' security practices**, include clear cybersecurity obligations and indemnity clauses in contracts, and ensuring the monitoring of third-party access to its systems.

'When dealing with sophisticated organisations, we often find them unable to map data flows involving key customers and suppliers and other core processing activities. This makes it difficult to argue that their processing is risk based, proportionate and complies with other data protection requirements. So, the risk of regulatory enforcement action or high-value claims is significantly increased if something goes wrong. **Data mapping** underpins many other aspects of an effective data governance strategy.

For example, it plays an important role in the implementation of robust compliance frameworks that support the implementation of generative AI solutions and other new technologies. It is important that retailers approach this exercise in a joined-up manner that is not over-engineered and can be applied pragmatically across the business.

Key takeaways for retailers

In light of the M&S attack, and the other recent retail cyber attacks, retailers should prioritise the following key steps:

1. Review and update incident response plans and disaster recovery plans, ensuring clear roles and responsibilities are defined.
2. Enhance data protection and cybersecurity measures, including regular security assessments, staff training, and implementation of appropriate technical safeguards.

- 3. Prepare for consumer law obligations during service disruptions.
- 4. Implement robust backup solutions to support rapid recovery and business continuity.
- 5. Review and strengthen contractual arrangements with suppliers and third parties to manage contractual liabilities in the event of a cyber attack.
- 6. Consider cyber insurance that covers both operational disruption and potential regulatory fines resulting from cyber incidents.

Map and continue to monitor core data processing activity, this underpins robust data protection and cybersecurity measures, and supports other strategic goals, including the implementation of AI and other tech solutions.

Conclusion

The M&S cyber attack serves as an urgent reminder for retailers that cybersecurity is not merely a critical IT issue, but a significant legal and business risk. As cyber threats continue to evolve in sophistication and frequency, retailers must ensure they implement appropriate preventative measures to ensure resilience and business continuity, while meeting obligations to customers and regulators.

Next steps

If you would like to arrange a simulated cyber attack with our lawyers and professional [cybersecurity](#) experts; conduct a data mapping exercise that can be aligned with your AI governance programme and other strategic data governance goals or learn more about any of the other topics in this exercise, please get in touch to arrange a free initial call.

< Previous

[Retail Law Roundup: May 2025](#)

Next >

[Consumer protection: Investigation, fines and other measures which the CMA can take](#)

Contents

Retail Law Roundup: May 2025	→
The M&S cyber attack: Lessons for UK retailers	→
Consumer protection: Investigation, fines and other measures which the CMA can take	→
Consumer protection: Unfair commercial practices	→
Consumer protection: Drip pricing	→
Consumer protection: Fake reviews	→
Consumer protection: Vulnerable consumers	→

Contact

Francis Katamba

Partner

francis.katamba@brownejacobson.com

+44 (0)330 045 2725

Related expertise

Commercial contracts for retail

Cyber liability and data security insurance

Data protection for retail

Digital and sourcing