Business briefing

June 2025

How retailers can navigate cyber attacks

In recent weeks, a series of ransomware attacks have disrupted operations at several major UK retail businesses, including M&S, Harrods and the Co-Op. The consequences can be swift and severe: halting operations, requiring notifications; jeopardising reputation and the need to hold on to customer trust. As retailers digitise rapidly, attackers could increasingly look to exploit the resulting opportunity.

Why are retailers prime targets for cyber attacks?

Retailers are vulnerable due to a combination of operational and structural factors. Many rely heavily on technology to sustain high turnover, especially in fast-moving consumer goods. Retailers also often hold large amounts of consumer data. While this data may not always be highly sensitive, its volume and the involvement of customers across different jurisdictions can make legal requirements – such as notifying regulators after a breach challenging.

Heavy reliance on supply chains adds another layer of risk. Attackers can target weaker security defences in suppliers or vendors as an indirect potential route to the retailer's network. Managing and investigating breaches that originate in the supply chain can add a layer of complexity.

Also, whilst there is no indication of this in relation to the specific recent attacks, some retailers operate with legacy systems and tight margins, making ongoing security investments difficult.

How does an attack impact retailers?

As recent events demonstrate, the impact on retailers can be both immediate and severe. Critical systems can be encrypted – or even if intact might need to be taken offline as a precaution during the investigation. This can instantly halt turnover, causing loss of revenue, replenishment issues and, potentially, empty shelves.

Contacts

Richard Breavington
Partner
Cyber & Tech Insurance
+44 20 3060 6341 (UK)
richard.breavington@rpclegal.com

Rachel Ford
Partner
Cyber & Tech Insurance
+44 20 3060 6821 (UK)
rachel.ford@rpclegal.com

Daniel Guilfoyle
Partner
Cyber & Tech Insurance
+44 20 3060 6912 (UK)
daniel.guilfoyle@rpclegal.com

In the wake of an incident, retailers (as with all companies who suffer a breach) must comply with their legal and regulatory notifications. They also risk potential litigation from customers, employees, or third parties to the extent that the incident brings to light any breaches of regulatory or contractual duties.

On top of this, retailers rely on customer trust and credibility. The negative press tied to an attack can cause reputational damage and a decline in customer retention and acquisition.

How do attackers get into a retailer's systems?

Tactics used by attackers range from the simple to the highly sophisticated.

In M&S' case, it is understood that the hacker group, Scattered Spider, used social engineering tactics through a third-party supplier to access M&S' systems. This allegedly involved the unassuming method of claiming to be an employee to trick IT staff into changing passwords and resetting authentication processes. This highlights that even with sophisticated technical precautions in place, well meant human activity is a vector which cannot be completely guarded against.

The risk of this type of social engineering seems likely to continue. Reasons include the use of AI leading to more creative and credible scenarios such as voice mimicking, making language less of a barrier. Also, the ongoing proliferation of 'Ransomware as a Service' in which access to systems can be sold to experienced ransomware gangs by anyone who is able to leverage that access – potentially through local knowledge and experience.

How can retailers address vulnerabilities?

While even the most advanced security cannot fully prevent social engineering or supply chain risks, retailers can take proactive steps to reduce exposure. This includes investing in cybersecurity upgrades like endpoint detection, encryption, and zero-trust architectures, implementing protocols such as multi-factor authentication (MFA), incident response plans, and continuous monitoring by security operations centres (SOCs). Hiring or contracting cybersecurity and legal compliance experts is also an important consideration.

More broadly, these incidents highlight the need for robust cyber resilience governance strategies. Cyber risk is tightly linked to data governance and regulatory exposure, so the responsibility should not sit solely with IT. It should be shared among legal, compliance, operations, and leadership teams. In our experience advising on breach response, effective incident management typically involves a cross-functional team, including the CISO, Head of Legal and COO or CEO, supported by the CFO and communications leads.

Equally important is cultivating a strong security culture. Scenario-based training, including phishing simulations and incident response drills, should be considered. This should also be supported by an environment that empowers individuals to identify and report risks without hesitation.

How can we help?

The RPCCyber – App provides a one-stop-shop resource for cyber breach assistance and pre-breach preparedness. As well as information about RPC's cyber-related expertise, the app also contains guidance on prevention against common incidents and access to our ongoing cyber market insights.

RPCCyber – can be downloaded for free from the **Apple Store** or **Google Play Store**.

© 2025 Reynolds Porter Chamberlain LLP – 160943809