# Cyberattacks on M&S and Adidas expose supply chain vulnerabilities and intensify calls for retail cybersecurity reform



Recent cyberattacks on major UK retailers, particularly Marks & Spencer (M&S) and Adidas, have illuminated vulnerabilities in the retail sector, revealing how quickly such incidents can disrupt entire supply chains. The situation is particularly troubling as hackers continue to employ sophisticated methods to infiltrate corporate systems, putting consumer data and business operations at serious risk.

M&S recently confirmed that a third-party vendor was the gateway for a significant cyberattack, leading to serious operational disruptions. This incident is linked to the notorious hacking group, Scattered Spider, known for its adept use of social engineering tactics to breach corporate security. As reported, this breach has already resulted in considerable financial losses, forcing M&S to engage in an internal investigation with Tata Consultancy Services, which has been contracted for over a decade. The investigation aims to determine how the incident occurred and is expected to conclude shortly.

Adidas faced a separate cyber incident which raised alarm bells across the sector. The company reported that an unauthorised external party compromised customer data via a third-party customer service provider. Notably, although the stolen data did not include payment-related information, Adidas described the breach as a serious concern. The brand has initiated a comprehensive investigation and is taking steps to inform affected customers while liaising with appropriate authorities. In a statement, Adidas expressed regret for any distress caused, reinforcing its commitment to consumer privacy and security.

The implications of these incidents extend beyond the individual companies involved. Chris Clowes, Executive Director at SCALA, remarked that disruptions stemming from cyberattacks can rapidly ripple through a business's entire supply chain, resulting in stalled deliveries and diminished stock visibility. In a landscape already strained by geopolitical tensions and climate-related events, such vulnerabilities underscore the urgent need for enhanced cybersecurity measures across the industry.

Moreover, recent trends indicate a surge in cyberattacks targeting major UK retailers, with reports suggesting a coordinated effort by groups like Scattered Spider. This uptick highlights the pressing necessity for companies to build cyber resilience and proactively safeguard their operations, particularly when relying on third-party vendors. The ongoing investigation into the M&S breach and similar incidents prompts a reevaluation of existing cybersecurity frameworks across the retail sector.

As the retail industry faces these mounting challenges, recent events could serve as a catalyst for a broader discussion on best practices in cybersecurity, emphasizing the need for comprehensive strategies to protect not only proprietary information but also consumer trust. In an environment where trust can be easily eroded, proactive measures and robust cybersecurity protocols are no longer optional but imperative for sustaining operational integrity and customer loyalty in the digital age.

The resonance of these incidents also extends to industry gatherings, such as the upcoming Snappy Summit, where leading figures in retail will convene to discuss the evolving landscape of quick commerce. Insights from industry veterans, like Justin King, will undoubtedly touch on these pressing issues, as retailers seek guidance on navigating both innovation and security in 2025 and beyond.

## Reference Map:

* Paragraph 1 – [[1]](https://retailtechinnovationhub.com/home/2025/6/1/marks-and-spencer-and-adidas-under-attack-rtihs-rounds-up-its-most-read-articles-from-last-week), [[4]](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9)
* Paragraph 2 – [[1]](https://retailtechinnovationhub.com/home/2025/6/1/marks-and-spencer-and-adidas-under-attack-rtihs-rounds-up-its-most-read-articles-from-last-week), [[2]](https://www.ft.com/content/6d47ef31-ed80-41cf-a2bd-d0e02a280e22), [[5]](https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scatte...)
* Paragraph 3 – [[3]](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761), [[6]](https://www.helpnetsecurity.com/2025/04/29/marks-spencer-ransomware-breach-incident/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://retailtechinnovationhub.com/home/2025/6/1/marks-and-spencer-and-adidas-under-attack-rtihs-rounds-up-its-most-read-articles-from-last-week> - Please view link - unable to able to access data
2. <https://www.ft.com/content/6d47ef31-ed80-41cf-a2bd-d0e02a280e22> - This article delves into the activities of Scattered Spider, a notorious hacking group responsible for the recent cyberattack on Marks & Spencer (M&S). The group employs advanced social engineering tactics to infiltrate corporate systems, leading to significant financial losses for M&S. The piece also highlights the group's history of targeting major corporations and their collaboration with other cybercriminals, underscoring the evolving nature of cyber threats in the retail sector.
3. <https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761> - This article examines the broader implications of the M&S cyberattack, emphasizing the increasing vulnerability of businesses to cyber threats. It discusses the challenges companies face in securing their systems, especially when relying on third-party vendors. The piece also highlights the importance of building cyber resilience and the need for businesses to adopt proactive measures to mitigate potential disruptions.
4. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - This article explores the recent surge in cyberattacks targeting major UK retailers, including M&S, the Co-op, and Harrods. It discusses the potential coordinated efforts behind these attacks and the role of groups like Scattered Spider. The piece also highlights the need for businesses to take cybersecurity seriously and the potential consequences of such breaches on customer trust and operational stability.
5. <https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scatte...> - This article provides an in-depth analysis of the M&S cyberattack, linking it to the Scattered Spider hacking group. It details the methods used by the attackers, including the deployment of the DragonForce encryptor. The piece also discusses the ongoing investigation and the steps M&S is taking to address the breach and prevent future incidents.
6. <https://www.helpnetsecurity.com/2025/04/29/marks-spencer-ransomware-breach-incident/> - This article reports on the M&S cyber incident, confirming it as a ransomware attack attributed to the Scattered Spider group. It outlines the effects of the attack on M&S's operations and the company's response, including engaging external cybersecurity experts and notifying authorities. The piece also discusses the broader implications of such attacks on the retail sector.
7. <https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> - This article provides an inside look into the chaos caused by the M&S cyberattack, detailing the operational disruptions and financial losses faced by the company. It discusses the potential involvement of the Scattered Spider group and the broader impact of such cyber incidents on the retail industry. The piece also highlights the importance of robust cybersecurity measures and the need for businesses to be prepared for such threats.