# TCS internal probe crucial as M&S cyberattack reveals third-party vulnerabilities



In the wake of a significant cyberattack that has severely impacted Marks & Spencer (M&S), the attention now shifts toward the internal investigations being conducted by Tata Consultancy Services (TCS). As M&S grapples with an estimated £300 million hit to its operating profit due to the attack, which has effectively put its online business on hold for over three weeks, stakeholders are keenly interested in uncovering the circumstances surrounding this breach. The incident, attributed to a hacking collective identified as Scattered Spider, has raised serious concerns about the vulnerabilities inherent in third-party partnerships.

The repercussions of the attack extend beyond immediate financial loss; M&S has also suffered a market capitalization decline exceeding £750 million amidst the turmoil. CEO Stuart Machin has pointed to human error involving a third-party contractor as the breach's catalyst, though he has not confirmed whether a ransom was demanded or if TCS’s systems were directly compromised. The incident reflects broader cybersecurity challenges, as M&S’s systems were breached through social engineering tactics rather than a failure within its own technical defenses. Despite having tripled its technology investments over the past three years, M&S discovered that attackers exploited human vulnerabilities to gain access, illustrating the ever-evolving nature of cyber threats.

Notably, amidst the chaos, M&S's cybersecurity efforts have drawn attention. Industry experts like Mark Hughes, CSO at The National Lottery, argue that the retailer's response has been commendable. Hughes emphasised the importance of collaborative efforts, stating that M&S worked closely with the National Cyber Security Centre (NCSC) to share insights and threat intelligence, showcasing a commitment to not only safeguarding its own operations but also contributing to broader industry defence. He remarked, “What matters is how you respond,” highlighting M&S’s integrity and urgency during this crisis.

The aftermath of the cyberattack presents a critical learning opportunity for businesses navigating the increasingly perilous landscape of cybercrime. According to the UK's Cyber Security Breaches Survey, over 40% of UK businesses encountered cyber threats in the past year, which exacerbates concerns around third-party access. Analysts underscore the necessity for companies to bolster their cybersecurity frameworks, particularly as the sophistication of threats continues to escalate. While M&S accelerates its recovery strategies, which include halting online orders until July and renewing focus on its digital initiatives, the retailer is also cognizant of the vigilance required to protect customer data. Approximately 600 systems are undergoing restoration following the breach, during which hackers accessed personal information such as names and email addresses but reportedly did not compromise financial details.

As TCS concludes its internal investigation, the scrutiny on the company is palpable. The IT services firm, a key partner for M&S since 2018, finds itself at the crux of questions regarding its security practices amidst rising cybersecurity incidents affecting retail giants in the UK. This incident not only undermines TCS’s reputation but also serves as a critical reminder for tech service providers about the imperative of robust security measures. With the National Crime Agency investigating the breach and the ongoing ramifications for M&S, the incident underscores the need for greater transparency and preparedness in the fight against cyber threats.

In conclusion, M&S’s experience serves as both a cautionary tale and a call to action for businesses across sectors to invest in more than just technology. It is an urgent reminder of the importance of fostering cybersecurity literacy at all levels of an organisation, particularly in light of the significant vulnerabilities presented by third-party interactions. As the fallout continues, M&S’s commitment to recovery and industry collaboration could provide a model for others navigating similar challenges in a landscape fraught with complexity and uncertainty.

## Reference Map:

* Paragraph 1 – [[1]](https://retailtechinnovationhub.com/home/2025/5/25/tata-consultancy-services-greenlights-internal-investigation-amid-fall-out-from-mands-cyber-attack), [[2]](https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0), [[3]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/)
* Paragraph 2 – [[2]](https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0), [[4]](https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8), [[5]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b)
* Paragraph 3 – [[1]](https://retailtechinnovationhub.com/home/2025/5/25/tata-consultancy-services-greenlights-internal-investigation-amid-fall-out-from-mands-cyber-attack), [[5]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[6]](https://www.reuters.com/business/retail-consumer/tata-consultancy-services-carries-out-internal-probe-into-ms-hack-ft-reports-2025-05-23/)
* Paragraph 4 – [[3]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/), [[4]](https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8), [[7]](https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems)
* Paragraph 5 – [[2]](https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0), [[6]](https://www.reuters.com/business/retail-consumer/tata-consultancy-services-carries-out-internal-probe-into-ms-hack-ft-reports-2025-05-23/)
* Paragraph 6 – [[4]](https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8), [[5]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[7]](https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems)
* Paragraph 7 – [[3]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/), [[5]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[6]](https://www.reuters.com/business/retail-consumer/tata-consultancy-services-carries-out-internal-probe-into-ms-hack-ft-reports-2025-05-23/)

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

## Bibliography

1. <https://retailtechinnovationhub.com/home/2025/5/25/tata-consultancy-services-greenlights-internal-investigation-amid-fall-out-from-mands-cyber-attack> - Please view link - unable to able to access data
2. <https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0> - Tata Consultancy Services (TCS) is conducting an internal investigation to determine if it was the entry point for a major cyberattack on Marks and Spencer (M&S) that compromised customer data and crippled the retailer's online clothing business for over three weeks. The attack caused an estimated £300 million hit to M&S's operating profit and resulted in a market capitalization loss of over £750 million. While M&S CEO Stuart Machin attributed the breach to human error involving a third-party contractor’s staff, he did not disclose whether a ransom was paid or if TCS—which has been M&S’s primary technology partner since 2018—was directly involved. Both TCS and M&S have refrained from official comments. The UK police have launched an investigation, and TCS expects to conclude its probe by the end of the month. The incident has cast a shadow over TCS’s reputation amidst a broader increase in cybercrime affecting UK retailers and India's tech industry. TCS, also partnered with UK retailer Co-op, confirmed its services were not linked to a separate cyberattack on that company. The event highlights growing cybersecurity challenges faced by global IT service providers.
3. <https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/> - Marks & Spencer (M&S) disclosed that a recent cyberattack on its systems was carried out through a third-party contractor, bypassing its own digital defenses via social engineering tactics. CEO Stuart Machin revealed that despite increasing tech investment threefold over the past three years, the attackers exploited human vulnerabilities, gaining access through the contractor rather than a technical weakness. Although M&S has an IT contract with Tata Consulting Services (TCS), Machin did not confirm if TCS was the specific target. The breach was discovered over Easter weekend (April 19-20), and M&S promptly involved cybersecurity experts and authorities. The company halted online sales, anticipating full service restoration by July. The UK’s National Crime Agency is investigating a group of young English-speaking hackers believed to be responsible. So far, around 600 systems have been scanned and are being restored. M&S has not commented on any ransom demands due to law enforcement advice. The retailer, with annual sales of nearly £14 billion ($19 billion), emphasized the importance of vigilance against increasingly sophisticated cyber threats.
4. <https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8> - British retailer Marks & Spencer (M&S) has estimated the cost of a recent cyberattack at approximately £300 million ($400 million). The attack, described as highly sophisticated and targeted, began around the Easter weekend and has significantly disrupted operations, particularly online sales of food, home, and beauty products. The disruption is expected to continue until July. The suspension of online shopping and the need for manual processes in stores have led to reduced food availability, increased waste, and higher logistics costs, adversely affecting profits. CEO Stuart Machin emphasized the company's focus on system recovery and declined to provide details about the attackers. M&S also revealed that hackers accessed customer personal data, including names, emails, addresses, and birth dates. The cyberattack is part of a broader wave affecting other British retailers, including Harrod’s and Co-op.
5. <https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b> - A recent cyber attack on Marks & Spencer (M&S) is projected to cost the company £300 million, or about 30% of its previous year's operating profit. This incident underscores the rising threat of cybercrime, which more than 40% of UK businesses have encountered in the past year, according to the UK government's Cyber Security Breaches Survey. While retail headlines dominate, other sectors are even more exposed. For tech companies, however, such breaches are creating business opportunities as organizations invest heavily in cybersecurity—global spending on anti-hacking software is seeing double-digit annual growth and is projected to reach $300 billion by 2028. The evolving nature of cyber threats complicates the defensive landscape. Malware has declined to 20% of attacks, while "vishing" has surged, and generative AI presents both risks and defensive potential. M&S had already doubled its cybersecurity spending since 2021 and is now accelerating its digital initiatives. Experts suggest that corporate boards need better cyber literacy, especially considering vulnerabilities caused by third-party access, which contributed to the M&S breach. Online sales at M&S will remain impaired for weeks, severely impacting its integrated retail strategy and reputation. The attack serves as a wake-up call for executives to enhance their cybersecurity frameworks.
6. <https://www.reuters.com/business/retail-consumer/tata-consultancy-services-carries-out-internal-probe-into-ms-hack-ft-reports-2025-05-23/> - Tata Consultancy Services (TCS), an Indian IT firm, is conducting an internal investigation to assess whether it served as the entry point for a cyberattack on British retailer Marks and Spencer (M&S), according to a report by the Financial Times. TCS, which has been providing services to M&S for over ten years, aims to complete the probe by the end of May. The cyberattack, disclosed by M&S in April, led to significant disruptions in operations and compromised customer data. The financial impact is estimated at around £300 million ($404.9 million) in lost operating profit, with further online service disruptions expected until July. Neither M&S nor TCS has commented on the situation, and Reuters has not independently verified the report.
7. <https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems> - Following a cyberattack on Marks & Spencer (M&S) over Easter weekend, the retailer’s online services have been disrupted since 25 April 2025. M&S has announced that customers will not be able to place online orders until at least July, although they can browse and place items in their baskets. The company estimates a £300 million hit to its 2025/26 operating profits and has been losing approximately £40 million in sales weekly due to the attack. Some customer data, including names, contact information, and order history, was stolen, but no payment or password details were compromised. M&S has contacted affected customers and is urging vigilance against phishing attempts. The cyberattack, reportedly carried out by a group called DragonForce, involved ransomware. The company has suspended its Sparks loyalty offers and is focusing on business recovery, assuring that its long-term growth plans remain unchanged. While M&S shares have dropped 4.9% year-to-date, analysts remain optimistic, highlighting robust performance in its food sector and suggesting potential for long-term investor gains once stability returns. Compensation has been offered to impacted customers in some cases.