# Marks & Spencer faces £3m daily losses amid new cyberattack and falling share price



Marks & Spencer's ongoing battle with cyber threats illustrates the vulnerabilities that even established corporations face in an increasingly digital retail landscape. Recently, the retailer disclosed that 'some personal customer information has been taken', raising serious concerns among its loyal customer base. While it has provided some reassurance by affirming that usable card and payment details remain secure, the implications of this breach cannot be understated, especially considering the retailer’s history with cyber-related incidents.

The incident, first reported on April 21 during the Easter break, has triggered discussions about the effectiveness of Marks & Spencer's cybersecurity measures. The company's chief executive, Stuart Machin, is likely thankful for the timing of the warm and dry spring weather, which has positively affected in-store sales amidst the crisis. The change in weather appears to have provided a temporary boost, with customers eager to purchase summer clothing and outdoor essentials. Unfortunately for M&S, this respite comes juxtaposed with trade estimates indicating a loss of over £3 million in income per day due to the cyberattack, a figure some analysts suggest may be overstated as certain customers switch to in-store shopping.

Despite the loyal customer base that M&S has cultivated over decades—due in large part to its reputation for quality and innovation—the company’s share price has fallen by 12% in the past month. This decline serves as a stark reminder of the financial ramifications that can accompany data security breaches, igniting debates on corporate responsibility and accountability. As past incidents have shown, such as the technical glitches in 2015 that inadvertently exposed customer data, the necessity for robust cybersecurity frameworks has become more pressing than ever. In that case, M&S described the leakage as an internal error and unlike the current situation, assured customers that financial data was not compromised.

In a broader context, recent global events such as the pandemic and geopolitical tensions—including Russia's invasion of Ukraine—have created a complex economic environment, further complicating the challenges retailers face. The Bank of England's cautious stance on interest rates reflects the wider uncertainty in financial markets, also impacting consumer behaviour. As inflation persists, the need for sharper, more assertive financial strategies becomes increasingly evident. Economists, including the newest member of the Monetary Policy Committee, Professor Alan Taylor, have advocated for a more proactive approach to interest rate cuts, particularly amid the precarious trade conditions.

The implications of these dynamics extend even beyond M&S, to other sectors that are similarly threatened by disruptions. For instance, the film and video industries are on edge due to potential tariffs and logistical challenges, raising concerns about the viability of ongoing projects.

As Marks & Spencer navigates its current dilemma, it is poised at a crossroads. The need for accountability looms large; as it works to fortify its cybersecurity measures, the company must also reassure its customer base that it values their security as highly as their loyalty. The unfolding events will be closely watched, not only for their impact on M&S but also as part of a larger narrative concerning data integrity and the vulnerabilities faced by organisations in today's interconnected economy.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6
2. Paragraph 5
3. Paragraph 5
4. Paragraph 4
5. Paragraph 4, 6
6. Paragraph 4, 6
7. Paragraph 5

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

## Bibliography

1. <https://www.dailymail.co.uk/money/comment/article-14708699/Spring-break-M-S-Warm-weather-provides-relief-cyber-attack-debacle-drags-ALEX-BRUMMER.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.bbc.co.uk/news/technology-34656818> - In October 2015, Marks & Spencer's website experienced a technical issue that allowed customers to view each other's personal information, including names, dates of birth, and contact details. The retailer temporarily suspended the site for two hours to address the problem, assuring customers that no financial data was compromised. M&S attributed the glitch to an internal error and apologized for the inconvenience caused. The incident raised concerns about data security and the importance of robust cybersecurity measures for online retailers.
3. <https://news.sky.com/story/marks-spencer-sorry-after-website-suspended-10341582> - In October 2015, Marks & Spencer temporarily suspended its website after customers reported seeing other people's personal details upon logging in. The retailer confirmed that no financial information was exposed and attributed the issue to an internal technical problem. M&S apologized for the inconvenience and emphasized that the breach was not due to a third-party cyber attack. The incident highlighted the need for stringent data protection protocols to maintain customer trust in online shopping platforms.
4. <https://www.bbc.com/news/articles/cv22e5vx5djo> - In May 2024, Marks & Spencer's website and app experienced a technical issue that rendered them inaccessible for several hours. Customers encountered error messages and were unable to navigate the site. M&S attributed the outage to a problem with a third-party provider and apologized for the inconvenience. The incident underscored the challenges retailers face in maintaining reliable online services and the importance of effective third-party partnerships to ensure seamless customer experiences.
5. <https://www.mandspensionscheme.com/news/news/2023/04/message-from-the-trustee-capita-cyber-incident/> - In April 2023, Capita, the administrator for Marks & Spencer's pension scheme, reported a cyber incident that potentially affected members' personal data. The M&S Pension Trust communicated with members, emphasizing the importance of vigilance and providing guidance on verifying communications related to the pension scheme. The incident highlighted the broader implications of cyber threats on financial services and the necessity for organizations to implement robust security measures to protect sensitive member information.
6. <https://www.cybertecwiz.com/marks-and-spencer-pension-suffered-a-cyberattack-in-connection-with-capita/> - In April 2023, Capita, the administrator for Marks & Spencer's pension scheme, experienced a cyberattack that potentially compromised members' personal data. The M&S Pension Trust communicated with members, urging vigilance and providing guidance on verifying communications related to the pension scheme. The incident underscored the broader implications of cyber threats on financial services and the necessity for organizations to implement robust security measures to protect sensitive member information.
7. <https://www.digitalspy.com/tech/a676004/marks-and-spencer-apologises-after-website-glitch-exposes-customer-details/> - In October 2015, Marks & Spencer's website experienced a glitch that exposed customers' personal information, including names, dates of birth, and contact details. The retailer temporarily suspended the site for two hours to address the issue and apologized for the inconvenience caused. M&S clarified that no financial data was compromised and attributed the problem to an internal error. The incident highlighted the importance of robust cybersecurity measures to protect customer data in the digital age.