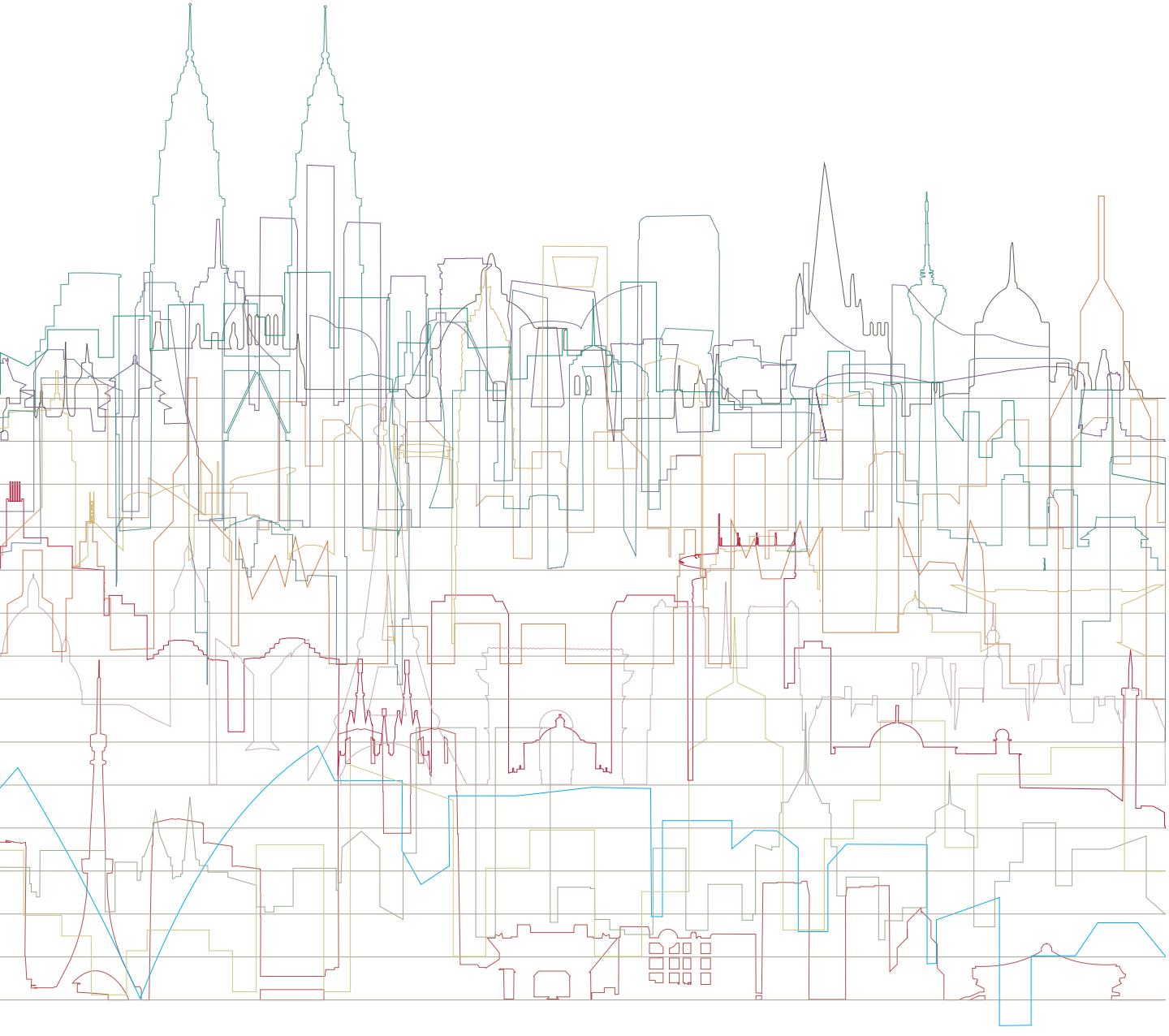
THE OXFORD METRICA REVIEW

MARKS & SPENCER (M&S) A PROFILE IN CRISIS



OXFORD METRICA

01 / 2025

What happened to Marks & Spencer (M&S)

M&S HAS LOST £1.3BN IN MARKET CAPITALISATION IN A SINGLE MONTH

On 21st April 2025, one of the UK's most respected retailers, Marks & Spencer (M&S), first revealed reports of a cyber-attack after customers reported payment issues and delays in receiving online orders. The National Cyber Security Centre speculated that it was an episode of ransomware, used to encrypt parts of M&S's infrastructure. Ransomware is a type of malicious software that locks or encrypts a victim's data and demands payment, usually in cryptocurrency, to restore access. The attack significantly disrupted operations, such as an indefinite suspension of its online clothing and home shopping segment, as well as deliveries, in the UK and Ireland. Moreover, the UK retailer admitted for the first time in mid-May that personal information, including customer contact details, dates of birth, household information, and online order histories, had been accessed by hackers in the breach. The group did stress however that the data included neither account passwords nor payment and card details. The hack also made for chaos in physical shops, where some food outlets struggled to maintain normal stock levels. Shoppers were met with empty shelves in some stores with signs saying: "Please bear with us while we fix some technical issues affecting product availability." At the time of writing on 23rd May, the company had not been able to take any orders through its website or app since 25th April. The hacking groups Scattered Spider and Dragonforce took responsibility for the ransomware attack. The former is known for employing advanced social engineering tactics, including phishing and multi-factor authentication (MFA) fatigue attacks. Since they first appeared in 2022, they have been linked to more than 100 targeted attacks across industries such as telecoms, finance, retail and gaming.

How management responded

Upon first revelation, M&S chief executive Stuart Machin wrote in an email to shoppers: "Over the last few days, M&S has been managing a cyber incident. To protect you and the business, it was necessary to temporarily make some small changes to our store operations...our stores remain open, and our website and app are operating as normal." Some customers, however, expressed frustration in the "disappointing" communication from the retailer. During the week of 5th May, there was a period of PR inactivity regarding the attack which led to a 7.7% fall in its share price. One such change to their operations was for M&S to indefinitely suspend its online clothing and home shopping segment, as well as deliveries, in the UK and Ireland soon after the attack was first reported. Following the breach, M&S enlisted CrowdStrike, Microsoft, and Fenix24 cybersecurity experts to help investigate and contain the incident.

Outcomes

As a result of the disruption, M&S asked about 200 agency workers at its main distribution centre to stay at home, due to a slowdown in order processing. Moreover, in certain physical stores such as Liverpool, food items were being reduced on mass owing to lower demand. However, general stock levels seemed to stabilise by mid-May. The breach, and admission that customer data had been stolen, led to widespread sentiment that shoppers may switch to other retailers. In addition to the loss in stock value (see Market reaction), there was undeniably a huge loss in perceived brand image and reputation online, and across social media. For example, between 22nd April and 16th May on X (formerly Twitter), there were over 100,000 posts related to M&S, 55% of which were negative, with only 7% positive. Moreover, based on average daily revenue, analysts have estimated that the company may have lost over £60 million in online sales as of mid-May. According to an analysis by Bank of America Global Research, the cyber-attack cost the company around £43 million a week in lost total sales. On 21st May during an announcement of their full-year results, the company warned that the disruption was likely to continue until July, expecting to wipe £300 million from its forecasted annual profit. Mr Machin blamed "human error" for the attack and also stated: "As a team, we have worked around the clock with suppliers and partners to contain the incident and stabilise operations, taking proactive measures to minimise the disruption to customers. We are focused on recovery...over the rest of the first half." Despite this, shares fell by more than 3% in early trading on the day of the announcement. M&S is also due to file a £100 million cyber claim from its insurers Allianz and Beazley. Allianz is reportedly the primary carrier on the policy and will be expected to cover the first £10 million of the claim. As a result of the operational and financial bedlam from the breach, and the respective drop in share price (highlighted below), M&S's CEO is facing a £1.1 million pay cut across a performance share plan and deferred bonus scheme.

Lessons learned

1. M&S should have realised early on that as one of the leaders in the retail industry, it needed to actively lead the fightback against the hackers, given that the faith in the entire retail system is being destroyed and its vulnerability exposed, with similar attacks at both the Co-op and Harrods.

2. PR activity and continual communication regarding developments of the situation are crucial, especially when customers' personal data has been stolen.

MARKS & SPENCER (M&S)

3. The company (and other retailers) needs to invest more in ensuring IT systems are secure, modern, and robust.

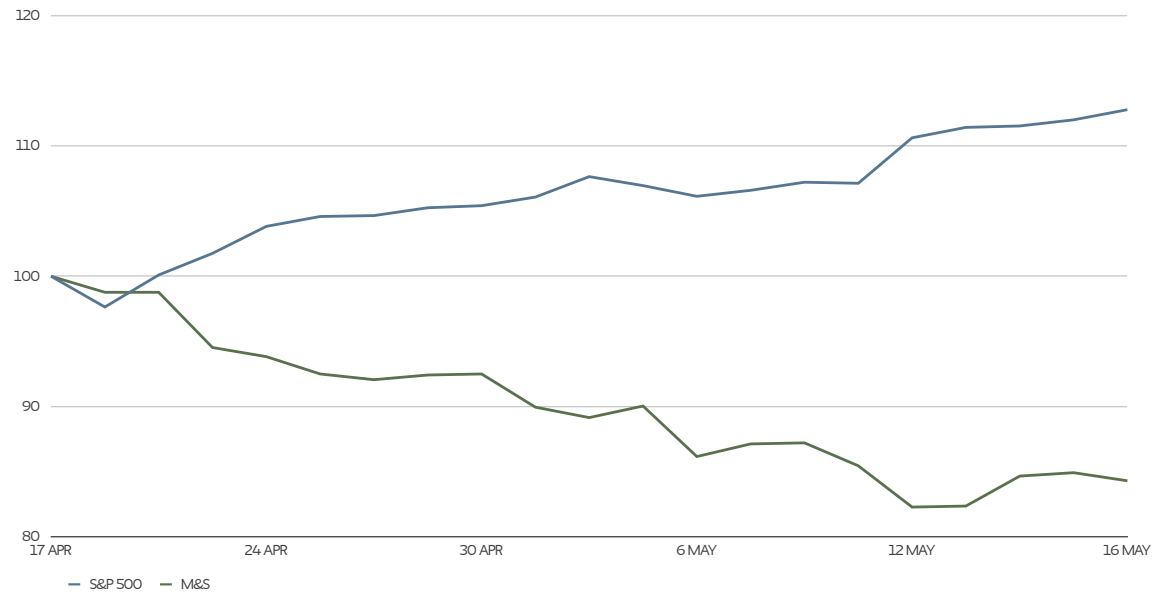
4. Ensure cash can still be accepted in the case of an emergency, such as a cyber-attack, and that staff can operate working tills.

5. A collaborative effort within the retail industry is needed to ensure that retailers don't give in to blackmail by hackers, either to keep attacks covered up or to restore operations. Admitting IT systems are not secure does indeed carry reputational risk, however, the reputational damage of paying a bribe would be far larger.

Market reaction

As shown in Figure 1 below, the attack damaged investor confidence, with M&S shares falling over 16% in a month from the initial breach, on 21st April, to mid-May, wiping around £1.3 billion off their market value. Their relative equity performance versus the S&P 500 was around 29% weaker over the same period.

FIGURE 1. Marks & Spencer (2025) (Index 17 April 2025 = 100)



OXFORD
METRICA

Oxford Metrica is a strategic advisory firm, offering informed counsel to boards. Our advisory services are anchored on evidence-based research in risk and financial performance. Our work includes statistical analysis and index construction for banks and insurers, risk and performance analytics for asset managers, due diligence support in mergers and highly customised services for corporate boards.

Dr Rory Knight is Chairman of Oxford Metrica. He is a member of the John Templeton Foundation where he chaired investments. Formerly he was Dean of Templeton College, Oxford and before that the Vize Direktor at the Schweizerische Nationalbank (SNB), the Swiss Central Bank. He has served on numerous boards.

oxfordmetrica.com