# Cyberattacks on M&S and Co-op expose urgent need for retail cybersecurity overhaul



The recent cyberattacks targeting Marks & Spencer (M&S) and Co-op supermarkets have sent shockwaves through the UK retail sector, exposing vulnerabilities that industry leaders can no longer ignore. Allegedly linked to the infamous DragonForce hacking group, these attacks have resulted in significant operational disruptions and a substantial loss of consumer trust.

According to reports, hackers communicated via Telegram, expressing their frustration with the Co-op's refusal to acquiesce to ransom demands. They claimed to have stolen vast amounts of sensitive customer and employee data, threatening to release this information should their financial demands not be met. Their audacious messages even likened themselves to characters from the US television series "The Blacklist," reinforcing their aim for notoriety and infamy within the cybercriminal landscape.

The cyber intrusions have had grave implications for both retailers. M&S, a stalwart of the British High Street, faced a £600 million drop in market value due to a combination of operational disruptions and the breach's fallout, including empty shelves that visibly reflected the chaos. Notably, the hackers reportedly infiltrated M&S systems as far back as February, exploiting a major vulnerability to maintain relentless access until the attack was finally detected. This suspension of operations culminated in a disaster for customers who were unable to place online orders during a critical retail period.

Crisis management teams scrambled to contain the fallout once the extent of the attack became evident. While M&S remains inhabited by the ghosts of this attack, Co-op was able to implement swift measures to mitigate damage. Leadership's decision to "pull the plug" on systems once they suspected wrongdoing likely prevented further catastrophes. Initially, Co-op had downplayed the extent of the breach, asserting that the attack had minimal impact. However, confirmation emerged that significant amounts of customer data were compromised.

Industry experts have pointed out that the encroaching threat posed by ransomware groups, including DragonForce and their alleged affiliates, underscores a growing trend of increasingly sophisticated cybercrime. Such incidents have renewed discussions about the vulnerability of large retailers, particularly those still operating with outdated IT systems—a fact that has made them prime targets for cybercriminals. With customer data becoming an attractive asset for ransom, retailers are urged to officiate robust cybersecurity measures as a means of deterrence.

The National Cyber Security Centre (NCSC) responded to the crisis with a clarion call for enhanced cybersecurity protocols across the retail sector. Their advisory highlighted the importance of vigilance and preparedness among companies in the wake of attacks of this scale. As the extent of these events unveils itself, major retailers—including Tesco, which previously reported ongoing preparations against cyber threats—find themselves on alert, understanding the potential ramifications of a single misstep.

In the aftermath of the attacks, the backlash has extended beyond immediate operational failures. Insurers are now revisiting their cyber insurance policies. Following this spate of attacks, premiums for coverage have increased significantly, with warnings that the retail sector could soon become untenable for some underwriters. The monetary losses incurred by M&S alone may run into tens of millions as it claims damages for business interruptions caused by the attacks.

As the retail landscape emerges from the shadows of these significant breaches, one thing remains clear: the lessons learned will necessitate a paradigm shift in how cybersecurity is addressed, prioritised, and implemented within this fiercely competitive sector. Without an enhanced commitment to internal security measures, retailers may find themselves caught in an ever-spiralling cycle of breaches and corporate chaos.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6, 7, 8
2. Paragraphs 5, 6, 7, 8
3. Paragraphs 1, 3, 4, 6, 7
4. Paragraphs 1, 2, 4, 6, 8
5. Paragraphs 1, 2, 3, 5, 7
6. Paragraphs 1, 3, 5, 8
7. Paragraphs 2, 6, 7, 8

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14728533/Cyber-attack-hackers-op-Marks-Spencers-Blacklist-show.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/190803d9-e646-4a58-8cd2-9a627cf40bb1> - Following significant cyber attacks on major UK retailers like Marks & Spencer (M&S), Harrods, and the Co-op, insurers are increasing cyber insurance premiums by up to 10%. This shift is prompting insurers to reassess cyber risk in the retail sector, which had previously seen declining rates. Experts warn of intensified cybersecurity scrutiny and potential insurer withdrawal from the retail market. M&S may claim tens of millions of pounds for business interruption, after losing over £40 million in online sales during a system outage. The Co-op confirmed a data breach affecting numerous customers. The sector's vulnerability is attributed to large amounts of consumer data and outdated IT systems. Tesco acknowledged ongoing cyber threat preparedness in its annual report, citing crisis simulations involving ransomware. Insurance might cover not only ransomware payments but also costs associated with crisis response. However, insurers face challenges if attackers are linked to sanctioned entities. The UK’s cybersecurity agency has also issued warnings about attackers impersonating IT help desks in sophisticated social engineering scams. Brokers urge businesses to secure cyber insurance now before premiums rise further.
3. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - Several major UK retailers, including Marks & Spencer (M&S), the Co-op, and Harrods, have recently been targeted by cyber attacks, highlighting the increasing vulnerability of the retail sector. M&S has faced significant operational disruptions and a £600 million drop in value due to these attacks. Investigations are ongoing, and experts suspect a common supplier or technology could link the incidents. Cybersecurity professionals suggest a potentially coordinated effort, possibly involving the group Scattered Spider, known for manipulating individuals to gain system access. The National Cyber Security Centre has expressed concern, urging businesses to treat cybersecurity seriously. Retailers are attractive targets due to their vast customer data, real-time operations, and reliance on legacy systems. Although some customer data was accessed, sensitive financial information reportedly remains secure. Cybersecurity apathy, especially among large UK retailers, has been noted in recent industry research. Experts warn that even without paying ransoms, attackers could profit by selling stolen data. The incidents serve as a stark reminder of the growing sophistication and impact of cybercrime on the retail landscape, with recovery potentially taking months.
4. <https://www.bleepingcomputer.com/news/security/marks-and-spencer-breach-linked-to-scattered-spider-ransomware-attack/> - Ongoing outages at British retail giant Marks & Spencer (M&S) are caused by a ransomware attack believed to be conducted by threat actors known as 'Scattered Spider'. M&S confirmed it suffered a cyberattack that caused widespread disruption, including to its contactless payment system and online ordering. The threat actors are believed to have first breached M&S as early as February, when they reportedly stole the Windows domain's NTDS.dit file. Using these credentials, the threat actors laterally spread throughout the Windows domain, while stealing data from network devices and servers. Sources told BleepingComputer that the threat actors ultimately deployed the DragonForce encryptor to VMware ESXi hosts on April 24th to encrypt virtual machines. M&S has not commented on the cyber incident.
5. <https://www.infosecurity-magazine.com/news/dragonforce-goup-ms-coop-harrods/> - Anonymous individuals identifying as members of the DragonForce cybercriminal syndicate have claimed responsibility for cyber-attacks on Marks & Spencer, Co-op, and Harrods. They contacted several media outlets, including the BBC and Bloomberg, with evidence that they had infiltrated the three UK retailers' IT networks and stolen large amounts of customer and employee data. Notably, they told BBC News that the Co-op breach was more extensive than Co-op had previously admitted. DragonForce originated as a pro-Palestine hacktivist group allegedly based in Malaysia (under the name DragonForce Malaysia) that has been active since August 2023. It is understood to be behind a number of notable cyber-attacks in the Asia-Pacific region and the US. The group is believed to have shifted goals and expanded to ransomware operations. Scattered Spider, tracked as Octo Tempest by Microsoft and UNC3944 by Google Cloud, is a financially motivated threat group active since May 2022. Primarily native English speakers, likely including some teenagers based in the UK or the US, Scattered Spider members are affiliated with the cybercriminal collective ‘The Com.’ The group is associated with the 2023 hacks of Caesars Entertainment and MGM Resorts International. The hacks against M&S, Co-op, and Harrods were consistent with Scattered Spider targeting, which typically consists of waves of attacking prominent brands in specific sectors to get media attention before shifting to other targets.
6. <https://cybernews.com/news/marks-spencer-ransomware-scattered-spider-attack/> - Weeks-long payment outages disrupting operations at British retail giant Marks & Spencer (M&S) are now being blamed on Scattered Spider, the same ransomware group said to be responsible for the 2023 hack of the MGM Grand in Las Vegas. New information has surfaced linking the infamous Scattered Spider ransomware group to the devastating 'cyber incident' causing chaos for the London-based retailer since Easter weekend. Apparently, the threat actors have been freely lurking inside M&S systems since February after gaining access to a main database file for Active Directory Services containing 'password hashes for Windows accounts.' After infiltrating the system, Scattered Spider was then said to have encrypted M&S servers using a ransomware variant from DragonForce, another threat actor selling its 'white label' services to fellow Ransomware-as-a-Service (RaaS) affiliates. DragonForce, a ransomware group that has been stepping up its operations since establishing itself in August 2023, developed its customizable variant utilizing both LockBit3.0 and ContiV3. The group is believed to have shifted goals and expanded to ransomware operations. Scattered Spider, tracked as Octo Tempest by Microsoft and UNC3944 by Google Cloud, is a financially motivated threat group active since May 2022. Primarily native English speakers, likely including some teenagers based in the UK or the US, Scattered Spider members are affiliated with the cybercriminal collective ‘The Com.’ The group is associated with the 2023 hacks of Caesars Entertainment and MGM Resorts International. The hacks against M&S, Co-op, and Harrods were consistent with Scattered Spider targeting, which typically consists of waves of attacking prominent brands in specific sectors to get media attention before shifting to other targets.
7. <https://www.bleepingcomputer.com/news/security/uk-shares-security-tips-after-major-retail-cyberattacks/> - Following three high-profile cyberattacks impacting major UK retailers, the country's National Cyber Security Centre (NCSC) has published guidance that all companies are advised to follow to strengthen their cybersecurity defenses. The cybersecurity breaches that prompted NCSC's alert are the recent hacks at Marks & Spencer, Co-op, and Harrods, all multi-million British retailers. The attacks started with M&S, which suffered a DragonForce ransomware attack that utilized tactics associated with Scattered Spider. The attack disrupted online orders, contactless payments, and the company's Click & Collect service. Last week, Co-op reported another cyber incident, restricting VPN access as a precaution. While initially implying they fended off the breach, Co-op confirmed on Friday that 'significant' amounts of customer data were stolen in the attack. On May 1, Harrods confirmed that threat actors tried to breach its network, prompting restrictions on internet access—suggesting an active response, though no breach was confirmed. All three breaches were claimed by the DragonForce operation, with BleepingComputer learning that the threat actors utilized the same social engineering attack to breach both M&S and Co-op. While ransomware was deployed at M&S, Co-op was able to detect and stop the attack before the encryptors could be deployed. NCSC's security advisory comes shortly after the agency warned that these attacks should be taken as a 'wake-up call' by all large businesses in the country, as they could be the next target in the hackers' crosshairs.