# Cyber attack on M&S highlights risks of remote working amid rising UK retail breaches



M&S has faced significant financial repercussions following a targeted cyber-attack, which is believed to have been perpetrated by a group known as 'Scattered Spider'. This attack has resulted in millions in lost sales, a near 7 per cent decline in share prices, and the freezing of over 230 job hires. The incident occurred earlier this week, leading to empty shelves, frustrated customers, and discontent among shareholders.

As the investigation is underway, the Co-op has also been affected, shutting down part of its IT system after discovering an attempted hack. In another incident, Harrods was targeted by online attackers shortly after the M&S breach, indicating a troubling trend of cyber threats against high-profile retailers. The Daily Mail reports that, according to the National Cyber Security Centre (NCSC), a staggering 76 per cent of UK businesses reported experiencing attempted cyber attacks in the past year.

Experts suggest that a notable shift in work culture, particularly due to the ongoing prevalence of remote and hybrid working, has heightened these risks. A report from Forbes indicates that 27 per cent of British workers currently engage in hybrid work, with 13 per cent working remotely full-time. This new working environment has posed increased vulnerabilities to organisations, including M&S, which shut off remote access to some IT systems to mitigate further risks associated with the cyber-attack.

The at-home working environment often lacks the rigorous IT security measures found in traditional office settings. Employees might use outdated software and are frequently distracted, leading to diminished vigilance against cyber threats. With employees working on personal devices and networks in more vulnerable conditions, hackers can exploit these weaknesses. The malware used in such attacks often gains entry through seemingly innocuous emails, deceiving the target into clicking harmful links.

The implications extend beyond just financial losses for M&S and other affected retailers. Cyber experts stress that the so-called 'right' to work from home poses significant challenges, notably as essential secure networks have expanded to include numerous private Wi-Fi connections. Criminals could potentially invade personal networks, intercept data, and access connected devices, leading to severe security breaches.

A wider scrutiny of cyber security across various sectors is warranted, especially given recent statistics that suggest a rising trend of stolen workplace devices. Reports reveal that Members of Parliament and their staff have encountered significant losses of tablets and laptops from public places over the past year.

The economic impact of cyber crime in the UK is substantial, with estimates placing the cost at approximately £27 billion annually. The NHS Counter Fraud Authority highlights that cyber-related fraud alone accounts for around £1.3 billion of this total each year, equating to the salaries of thousands of nurses or the procurement of ambulances.

Experts caution that the skills of those intending harm may now exceed those tasked with cybersecurity. There is an urgent need for enhanced investment in advanced software and hardware within key national institutions. Given the severity of the risks, particularly regarding essential services and national security, a discussion about the potential prohibition of remote work for companies crucial to public welfare has emerged.

This evolving scenario underscores the complex nature of modern work arrangements, where the agility of cyber attackers may outpace the defensive capabilities intended to protect vital sectors of the economy.

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

## Bibliography

1. <https://www.reuters.com/world/us/fbi-working-towards-nabbing-scattered-spider-hackers-official-says-2024-05-10/> - This article discusses the FBI's efforts to charge members of the Scattered Spider hacker group, known for aggressive cyber attacks on U.S. and Western organizations, including high-profile breaches of MGM Resorts and Caesars Entertainment.
2. <https://www.stornowaygazette.co.uk/news/marks-spencer-cyber-attack-5104977> - This report details Marks & Spencer's response to a cyber attack, including the suspension of online services and collaboration with cybersecurity experts to resolve the issue.
3. <https://www.techmonitor.ai/technology/cybersecurity/security-breach-forces-ms-website-offline-4704078> - This article covers the security breach that forced Marks & Spencer to suspend its website, resulting in customers being able to see other people's details when logging into their accounts.
4. <https://www.s-rminform.com/cyber-intelligence-briefing/cyber-intelligence-briefing-21-november-2023> - This briefing includes a joint advisory from the FBI and CISA about the Scattered Spider ransomware group, highlighting their use of social engineering techniques and BlackCat/ALPHV ransomware.
5. <https://industrialcyber.co/threats-attacks/fbi-cisa-warn-of-scattered-spider-hackers-targeting-commercial-facilities-adopt-social-engineering-techniques/> - This article discusses the FBI and CISA's warning about the Scattered Spider hackers targeting commercial facilities, employing social engineering techniques to gain unauthorized access.
6. <https://www.cybersecurityhq.com/blog/cybersecurityhq-news-roundup-december-6-2024> - This roundup includes information about a California teen charged in connection with the Scattered Spider cybercrime group, highlighting the group's activities and the FBI's efforts to apprehend its members.
7. <https://www.dailymail.co.uk/news/article-14670167/Working-Home-vulnerable-malign-hackers.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data