# M&S cyber-attack exposes escalating risks of remote work for UK businesses



This week, Marks & Spencer (M&S) experienced a severe cyber-attack, resulting in significant operational disruptions. The attack led to an immediate halt on remote access to some IT systems, aimed at curtailing the spread of ransomware, a malicious software that locks users out of their systems until a ransom is paid. Financial repercussions include millions in lost sales and a nearly 7 per cent drop in share prices, alongside the freezing of over 230 new job hires.

The attack, which has drawn attention to the vulnerabilities of businesses amidst a growing trend of remote work, is suspected to have been executed by a group known as 'Scattered Spider', which is reported to comprise a network of young hackers operating from the UK and the US. This incident is part of a wider wave of cyber threats, as other notable retailers, including Co-op and Harrods, have faced similar threats in recent days.

The National Cyber Security Centre has revealed alarming statistics, noting that a staggering 76 per cent of UK businesses reported attempts at cyber attacks in the past year. Experts attribute this rising trend, in part, to a significant cultural shift towards working from home, a change catalysed by the pandemic. Currently, around 27 per cent of workers in Britain engage in ‘hybrid working’, with 13 per cent working remotely full time.

The vulnerabilities associated with remote working practices, as highlighted by various business leaders, include decreased productivity, as a recent Stanford University report indicates a potential 20 per cent reduction in efficiency amongst those working from home. The communal benefits of a dedicated workplace, including the spontaneous sharing of ideas and heightened supervision, are perceived as diminishing in a remote setting.

Further complicating this issue is the fact that employees working from home are often more susceptible to online threats. Cybersecurity experts point out that individuals working in domestic settings typically use outdated software and devices, distracting home environments diminish vigilance, and critical security updates frequently go unaddressed. This environment increases the likelihood of falling victim to phishing scams—malicious emails designed to appear legitimate that entice users to click on harmful links.

Moving forward, industry experts have expressed concerns regarding the impact of remote work on national security. Many employees, including those working in sensitive positions such as the Government Communications Headquarters (GCHQ), are granted the flexibility to work remotely, raising questions about the potential risks associated with such practices. Moreover, the diversity of Wi-Fi networks now involved in remote working setups may present additional vulnerabilities.

This situation is compounded by the fact that portable devices used in remote work increase the risk of theft. Recent reports indicate that members of Parliament and their staff have experienced numerous losses of digital devices, with almost 70 incidents recorded over the past year. The potential consequences of these devices falling into malign hands raise significant concerns over personal data security and broader implications for national security.

Currently, the economic impact of cybercrime in the UK is estimated at £27 billion annually, with the NHS Counter Fraud Authority citing cyber attacks as a major contributor to a total annual fraud loss of £1.3 billion. This is equivalent to the salaries of approximately 40,000 nurses or the acquisition of 5,000 ambulances.

In light of the increasing sophistication of cyber attackers, experts emphasise the need for substantial investment in advanced cybersecurity measures by leading institutions. They advocate for a shift in GCHQ from a primarily protective role to a more offensive stance to outpace online threats. Additionally, some specialists argue for reconsidering remote work policies for businesses deemed critical to national health and economic stability to mitigate the risks posed by remote working environments.

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

## Bibliography

1. <https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf> - This article discusses the increasing concern of cybercrime for both nation-states and private sectors, highlighting the rise in cyber attacks and the need for enhanced cybersecurity measures.
2. <https://www.reuters.com/technology/cybersecurity/us-charges-five-scattered-spider-hacking-scheme-2024-11-20/> - This report details the U.S. charges against five individuals connected to the hacking group 'Scattered Spider,' who were involved in a series of phishing attacks targeting various U.S. companies.
3. <https://en.wikipedia.org/wiki/Scattered_Spider> - This Wikipedia page provides comprehensive information about 'Scattered Spider,' a hacking group composed mainly of young individuals from the UK and the US, known for their involvement in various cyber attacks.
4. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a> - This advisory from the Cybersecurity and Infrastructure Security Agency (CISA) discusses the tactics, techniques, and procedures (TTPs) used by the 'Scattered Spider' threat actors against commercial facilities sectors.
5. <https://www.computerweekly.com/news/366560680/An-inside-look-at-a-Scattered-Spider-cyber-attack> - This article provides an in-depth analysis of how a 'Scattered Spider' cyber attack unfolded, including the methods used to gain access to an IT admin account through social engineering.
6. <https://cyberresilience.com/threatonomics/resilience-threat-researchers-identify-new-campaigns-from-scattered-spider/> - This report identifies new campaigns from 'Scattered Spider,' highlighting their expansion into various industries and the use of advanced social engineering techniques.
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