# British firms brace for rising cyberattacks amid AI risks and remote work vulnerabilities



British businesses are increasingly alarmed by the potential for cyberattacks to devastate their operations, a fear vividly highlighted by the recent assault on Marks & Spencer (M&S). A survey conducted by Absolute Security revealed that two-thirds of security leaders at medium and large firms in the UK perceive similar attacks as potentially crippling. They estimate that the financial burden from ransom demands and subsequent clean-up could reach millions, jeopardising the futures of numerous organisations. Following the Easter attacks, which inflicted a £300 million toll on M&S and shaved £1 billion off its market value, the dire implications for integrity and profitability resonate deeply across the retail sector.

The attack, attributed to the notorious hacker group Scattered Spider, employed sophisticated social engineering tactics, illustrating a worrying trend in cybercrime. This group's modus operandi involves meticulously researching personal information to impersonate employees and exploit vulnerabilities, particularly in help desk systems. Scattered Spider has been implicated in various high-profile breaches, showcasing their audacity and adaptability amidst ongoing efforts by cybersecurity firms to counteract their schemes. The fallout from the M&S incident alone—financial losses and compromised customer data—may now even escalate into a class action lawsuit, signalling the extended repercussions of such infractions.

Compounding these threats is the more profound issue of remote work. The survey underscored that 62% of cybersecurity leaders regard devices used by home-working staff as significant weak points in their defences. Andy Ward, SVP at Absolute Security, noted that recent breaches have highlighted the vulnerabilities that telecommuting has introduced. With many employees reluctant to return to the office, essential security updates on personal devices are often neglected for extensive periods, heightening exposure to cyber threats.

As businesses navigate these tumultuous waters, the financial implications of ransomware attacks loom large. Data reveals that over half of the surveyed companies experienced a ransomware incident in the last year, with the average cost to a victimised organisation reaching approximately £850,000. In severe cases, recovery costs can outstrip the initial demands, as seen with the Royal Mail, where the LockBit group demanded £65 million. Furthermore, the repercussions of cyber breaches are not merely financial; they can lead to job losses and even insolvency, as seen with companies like Travelex and KNP Logistics. Both fell victim to significant cyber assaults and subsequently shut down operations with devastating impacts on employment.

The growing prevalence and sophistication of cyber threats strain already overextended resources, particularly as the National Cyber Security Centre (NCSC) reported a threefold increase in severe attacks recently. This increase necessitates a proactive and robust approach to cybersecurity measures. Richard Horne, CEO of the NCSC, emphasised the need for improved cybersecurity hygiene and infrastructure resilience, particularly in high-stakes sectors such as health.

Looking ahead, the intersection of artificial intelligence with cybercrime poses an additional challenge. According to Cabinet Office Minister Pat McFadden, the expansion of AI technologies will likely amplify both the frequency and severity of attacks. The government's upcoming Cyber Security and Resilience Bill aims to bolster protections and urges both public and private sectors to enhance their defence strategies.

In summary, as UK businesses face an ever-evolving landscape of cyber threats, the imperative for robust cybersecurity measures is more pronounced than ever. With the stakes so high, protecting sensitive data and ensuring operational integrity are essential to safeguarding not just individual firms but the broader economic landscape.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14770439/WFH-staff-leaving-British-businesses-exposed-cyber-attacks.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.ft.com/content/6d47ef31-ed80-41cf-a2bd-d0e02a280e22)
* Paragraph 2 – [[2]](https://www.ft.com/content/6d47ef31-ed80-41cf-a2bd-d0e02a280e22), [[3]](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761)
* Paragraph 3 – [[1]](https://www.dailymail.co.uk/news/article-14770439/WFH-staff-leaving-British-businesses-exposed-cyber-attacks.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[4]](https://www.ft.com/content/5ce0a155-ddc2-43e4-a383-c6e78f51f836)
* Paragraph 4 – [[5]](https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53), [[6]](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/)
* Paragraph 5 – [[4]](https://www.ft.com/content/5ce0a155-ddc2-43e4-a383-c6e78f51f836), [[7]](https://www.hiscoxgroup.com/news/press-releases/2023/10-10-23)

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

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14770439/WFH-staff-leaving-British-businesses-exposed-cyber-attacks.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/6d47ef31-ed80-41cf-a2bd-d0e02a280e22> - Scattered Spider, a notorious hacking group, was behind the recent breach of British retailer Marks and Spencer (M&S), causing significant financial losses up to £300 million in operating profits and over £600 million in market capitalization. The gang, composed of mainly English-speaking members, uses advanced social engineering and online traps to gain access to corporate systems. Their strategy involves impersonating employees through well-researched personal information and exploiting help desk vulnerabilities. Scattered Spider has also been linked to the 2023 MGM Resorts hack and appears to collaborate with other cybercriminals like ransomware gang Dragon Force for negotiations. The group has targeted companies like Tinder, Louis Vuitton, and News Corp, though there is no confirmation of successful breaches. Despite arrests made in Spain, the UK, and the US, the group seems resilient. Cybersecurity firms, including Mandiant and Silent Push, have tracked their activity and warned potential victims. The motive for these hackers often extends beyond financial gain, seeking recognition and notoriety. As part of the complex ransomware ecosystem, Scattered Spider focuses on initial access while other gangs handle encryption and ransom negotiations. Their slogan, 'Mischief before money,' reflects their penchant for notoriety over profit. ([ft.com](https://www.ft.com/content/6d47ef31-ed80-41cf-a2bd-d0e02a280e22?utm_source=openai))
3. <https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761> - A recent cyber attack on Marks and Spencer (M&S) underscores the growing vulnerability of businesses to cyber threats. The attack, attributed to the hacker group Scattered Spider, disrupted services including online clothing sales and contactless payments, with the company facing a potential £300 million hit to operating profits. The breach, linked to third-party human error, exposed customer data and has prompted a class action lawsuit. M&S is still recovering, expecting full operational restoration by July. Cyber attacks like this—often involving ransomware that encrypts vital data—represent a form of asymmetric warfare against unprepared corporate infrastructures. Many companies grapple with outdated or patched-together IT systems and rely on external vendors. Experts stress that while total prevention is unlikely, better practices such as software updates, multi-factor authentication, backups, and operation segmentation can mitigate damage. Building cyber resilience through early detection, response, and containment is essential. More than half of UK businesses faced cyber attacks in the past five years, highlighting the need to expect disruptions and prepare systematically to endure them. ([ft.com](https://www.ft.com/content/c9bd0a6a-eedf-4c98-8e2d-8deffd851761?utm_source=openai))
4. <https://www.ft.com/content/5ce0a155-ddc2-43e4-a383-c6e78f51f836> - Chief legal officers are facing increasing pressure due to the growing sophistication of cyber threats. One notable incident involved a UK engineering company losing $25 million in Hong Kong through a deepfake scam. A survey by the Association of Corporate Counsel identified cybersecurity as one of the top concerns for these legal professionals. Regulators and organizations like the European Central Bank are urging better preparation against cyber attacks, which have become more frequent and costly. Legal teams are critical in planning and responding to such threats, frequently engaging in war-gaming exercises and scenario planning. Ransomware attacks are particularly concerning, with legal counsel playing a significant role in decision-making. Companies also focus on educating staff about cyber threats and ensuring third-party suppliers comply with cybersecurity standards. Compliance with global regulations, such as Europe's upcoming Digital Operations Resilience Act (Dora), further stresses the importance of legal counsel in maintaining cyber resilience and preventing litigation. ([ft.com](https://www.ft.com/content/5ce0a155-ddc2-43e4-a383-c6e78f51f836?utm_source=openai))
5. <https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53> - The UK's National Cyber Security Centre (NCSC) has reported a significant increase in severe cyber attacks over the past year, warning of a widening gap in the nation's ability to combat such threats. The NCSC observed a tripling of these attacks, affecting key organizations like London hospitals and the British Library. Chief executive Richard Horne emphasized the need for increased efforts to keep up with rapidly advancing cyber threats, particularly those from state-led entities such as Russia, China, and North Korea, as well as sophisticated criminal organizations. The NCSC received nearly 2,000 reports of cyber attacks, with a significant number requiring agency support. The agency highlighted the critical need to improve the cyber security of public infrastructure and supply chains and underscored the importance of basic cyber hygiene and strong password practices to fend off commodity cyber attacks. However, the increasing sophistication and volume of state-led and criminal cyber activities pose a growing challenge exacerbated by the use of AI in cyber operations. ([ft.com](https://www.ft.com/content/6603dac2-1c01-41e7-9925-4042500ccc53?utm_source=openai))
6. <https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/> - As AI technology becomes more widespread, the United Kingdom is expected to face an increase in both the frequency and severity of cyberattacks, according to Cabinet Office Minister Pat McFadden. Speaking at the CyberUK 2025 conference, McFadden announced the declassification of an intelligence assessment revealing that AI will escalate cyber threats in the coming years. In 2024, the National Cyber Security Centre (NCSC) received nearly 2,000 cyberattack reports, with 90 considered significant and 12 classified as highly severe—a threefold increase in major incidents from the previous year. Recent ransomware attacks have targeted notable British retailers including Marks & Spencer, the Co-op Group, and Harrods, resulting in significant operational disruptions. McFadden emphasized that cybersecurity is a vital necessity, not a luxury, and urged both public and private sectors to strengthen their defenses. The government plans to introduce a new cyber security strategy and legislate new powers under the upcoming Cyber Security and Resilience Bill. NCSC CEO Richard Horne also advocated for ending ransom payments to undermine the attackers' business model. ([reuters.com](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/?utm_source=openai))
7. <https://www.hiscoxgroup.com/news/press-releases/2023/10-10-23> - Over half (53%) of businesses suffered at least one cyber attack over the last 12 months—a five-point increase on the previous year (48%) according to new data from the latest Hiscox Cyber Readiness Report. The Hiscox Cyber Readiness Report—based on the views of over 5,000 organisations of all sizes across eight countries—found that cyber attacks have increased for the fourth consecutive year. Attacks on small businesses with less than ten employees have risen from 23% to 36% over the last three years, as cyber criminals look to leverage vulnerabilities in IT technology. Small businesses of less than 250 employees also report a lack of confidence around cyber, with only three in five (61%) confident that they could handle an attack, compared to 71% of larger businesses. Companies with 1,000 or more employees felt that cyber attacks were more commonplace than ever before, with seven out of ten (70%) experiencing at least one attack—up from 62% a year ago. ([hiscoxgroup.com](https://www.hiscoxgroup.com/news/press-releases/2023/10-10-23?utm_source=openai))