# AI-driven cyberattacks triple severe incidents, hitting UK retailers hard



# The Rising Tide of Cyber Threats: Challenges Ahead for UK Cybersecurity

The recent surge in cyberattacks has become a significant concern for the United Kingdom, particularly as technology, especially artificial intelligence (AI), continues to advance. Cabinet Office Minister Pat McFadden underscored this alarming trend during the CyberUK 2025 conference, noting that AI is poised to not only increase the frequency but also the intensity of cyber threats targeting British institutions and businesses. This forewarning follows a spate of high-profile cyber incidents affecting major retail players, including Marks & Spencer, the Co-op Group, and Harrods, which have collectively experienced operational disruptions that demand urgent attention and robust responses.

In recent weeks, the UK retail sector has faced an alarming wave of cyberattacks. Marks & Spencer, for instance, reported ongoing issues following a cyber incident that hit its systems around Easter, leading to significant disruptions in its ability to process online orders and manage staff operations. The company has since experienced a £600 million drop in its market value, drawing attention to the severe financial fallout associated with these breaches. Investigations are ongoing, with many experts suggesting a coordinated attack possibly linked to groups like Scattered Spider, known for their sophisticated tactics that exploit system vulnerabilities. The Co-op Group is reported to have suffered a similar attack, further highlighting the systemic risks plaguing the retail industry.

During his address, McFadden revealed that in 2024, the National Cyber Security Centre registered nearly 2,000 reports of cyberattacks, with around 90 being classified as significant. Alarmingly, the number of highly severe incidents tripled compared to the previous year. McFadden’s comments serve as a stark reminder that cybersecurity is no longer a luxury but a necessity, demanding immediate action from both public and private sectors to bolster defences. The forthcoming Cyber Security and Resilience Bill is set to equip the government with new powers to mandate enhanced cybersecurity measures across regulated organisations, a move that many experts regard as crucial for safeguarding against the evolving threat landscape.

The reliance of retailers on real-time operations and legacy systems—often laden with vulnerabilities—makes them attractive targets for cybercriminals. The recent attacks on major retail chains displayed a sophisticated tactic where cybercriminals impersonated employees to manipulate IT help desks into resetting passwords, granting them access to sensitive internal networks. Reports indicate that the group DragonForce claimed responsibility for these high-profile breaches, alleging the theft of potentially 20 million customer records, despite reassurances that sensitive financial data remains protected. Cybersecurity professionals have urged organisations to reevaluate their help desk protocols to prevent such infiltrations, emphasising the need for vigilance.

Richard Horne, CEO of the National Cyber Security Centre, echoed McFadden's sentiments, advocating for a future where paying ransoms becomes an obsolete practice. By systematically undermining the financial viability of cybercriminal operations, the hope is to deter attacks and encourage organisations to view cybersecurity as a fundamental obligation rather than an afterthought. The urgency of this message is palpable: as AI technologies proliferate, so will the sophistication of cyber threats.

In conclusion, the convergence of advancing technology and increasingly audacious cyberattacks represents a formidable challenge for the UK. As the nation grapples with these evolving threats, it is critical for businesses, government bodies, and individuals alike to adopt a proactive stance towards cybersecurity. The government's impending initiatives are steps in the right direction, yet only through collective vigilance and robust strategies can the UK hope to navigate this precarious landscape effectively.

## Reference Map:

* Paragraph 1 – [[1]](https://www.insurancejournal.com/news/international/2025/05/07/822863.htm), [[2]](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/)
* Paragraph 2 – [[3]](https://apnews.com/article/7d3c01faa7380775598a517df4db1250), [[4]](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9)
* Paragraph 3 – [[2]](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/), [[6]](https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/)
* Paragraph 4 – [[5]](https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/), [[4]](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9)
* Paragraph 5 – [[1]](https://www.insurancejournal.com/news/international/2025/05/07/822863.htm), [[2]](https://www.reuters.com/business/retail-consumer/britain-face-more-cyberattacks-ai-adoption-grows-minister-says-2025-05-07/)
* Paragraph 6 – [[6]](https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/)

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

## Bibliography

1. <https://www.insurancejournal.com/news/international/2025/05/07/822863.htm> - Please view link - unable to able to access data
2. <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))
3. <https://apnews.com/article/7d3c01faa7380775598a517df4db1250> - British retailers are facing a wave of cyberattacks, with Marks & Spencer (M&S) and Harrods among the latest high-profile victims. M&S has been grappling with an ongoing cyber incident since Easter weekend, disabling its ability to process online orders, hire new staff, or maintain regular website functions. Although some services like contactless payments have been restored, the disruption continues as M&S works intensively to resolve the issue. Meanwhile, Harrods acknowledged a cyber threat and has taken precautionary steps, including limiting internet access. The attacks, which may be linked to a group called Scattered Spider, have raised concerns in the UK retail sector following a similar incident at Co-op. Authorities, including London’s Metropolitan Police and the UK’s National Cyber Security Centre, are investigating and providing support. Experts across the cyber defense industry warn that the growing use of generative artificial intelligence is intensifying the cyber threat landscape and urge organizations to strengthen their digital defenses. ([apnews.com](https://apnews.com/article/7d3c01faa7380775598a517df4db1250?utm_source=openai))
4. <https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9> - Several major UK retailers, including Marks and 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. ([ft.com](https://www.ft.com/content/5444d2e4-e258-45d2-8ca9-7927e502e3b9?utm_source=openai))
5. <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> - Cyberattacks on UK retailers Marks & Spencer (M&S) and the Co-op Group were initiated by hackers impersonating employees and deceiving IT help desks into resetting passwords, according to BleepingComputer. This allowed the intruders access to internal networks. The UK's National Cyber Security Centre has advised organizations to revise their help desk protocols to prevent similar breaches. M&S, having disclosed the cyber incident on April 22, witnessed a 12% share decline and subsequently suspended online clothing and home orders; food product availability has also been disrupted. Analysts from Deutsche Bank estimate the financial impact at approximately £30 million ($40 million), with ongoing losses of around £15 million weekly, though cyber insurance is anticipated to cover most of the initial losses. Full recovery may take weeks, as rebuilding networks is a complex process. Meanwhile, a group named DragonForce claimed responsibility for attacks on M&S, the Co-op, and Harrods, alleging theft of staff and potentially 20 million customer records. The attack on M&S has also been tentatively linked to the hacking group "Scattered Spider" using DragonForce ransomware, though the National Cyber Security Centre has not confirmed any direct connection between these incidents. ([reuters.com](https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/?utm_source=openai))
6. <https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/> - The British government is set to urge all UK businesses to prioritize cyber security following recent cyberattacks on major retailers Marks & Spencer (M&S), the Co-op Group, and Harrods. Cabinet Office Minister Pat McFadden, in coordination with national security officials and Richard Horne, CEO of the National Cyber Security Centre, outlined governmental support for affected companies. At the upcoming CyberUK conference in Manchester, McFadden will stress the need for heightened cyber precautions, describing the attacks as a "wake-up call" and advocating for cyber security to be treated as an "absolute priority." New measures, including the Cyber Security Bill, are being introduced to strengthen national defense. M&S experienced significant disruption on April 25 due to a suspected ransomware attack by the group "Scattered Spider," which affected their online and contactless services. This incident follows a growing trend of cyberattacks causing extensive financial and operational damage across UK industries. ([reuters.com](https://www.reuters.com/business/retail-consumer/britain-warn-companies-cyber-security-must-be-absolute-priority-2025-05-02/?utm_source=openai))