# Marks & Spencer hit by £300 million cyber attack amid rising global ransomware threats



Global companies are increasingly facing the fallout from a surge in cyber and ransomware attacks that threaten to compromise sensitive data and disrupt operations across various sectors, including healthcare, finance, and retail. This year, incidents have been reported by numerous firms and regulatory bodies in the U.S., UK, and Europe, underlining the scale and sophistication of these attacks.

Notably, Marks & Spencer (M&S) in the UK suffered a cyber incident that is projected to cost the company approximately £300 million, equivalent to about 30% of its operating profit from the previous year. This incident serves as a stark reminder of the growing threat posed by cybercrime, as more than 40% of UK businesses report having encountered such threats in the past 12 months. In fact, in 2023, a staggering 94% of IT leaders in the U.S. reported experiencing significant cyber attacks, pushing companies to ramp up their cybersecurity budgets and strategies. M&S had already doubled its cybersecurity spending since 2021 but found itself vulnerable, particularly due to weaknesses introduced by third-party access, which played a role in the breach.

Across the Atlantic, in the U.S., the financial sector remains a primary target for cybercriminals. Not only are traditional data breaches prevalent, but cyber incidents are becoming increasingly complex, with methods such as social engineering and ransomware attacks now commonplace. One prominent case involved MGM Resorts, which approved a $45 million settlement in a class-action lawsuit related to data breaches affecting millions of customers. Meanwhile, Clorox also faced challenges following a cyber attack that disrupted its distribution, although the company claimed to have fully restored services thereafter.

The situation in Europe reflects a broader trend. In France, luxury powerhouse LVMH was reportedly hit by a cyber attack that extracted customer data, while the UK grocery chain Co-op reported that it too had been compromised, with hackers gaining access to and extracting sensitive customer information. Such breaches highlight the vulnerability that many organisations face, with the potential for severe reputational and financial damage as incidents disrupt operations and erode consumer trust.

The nefarious activities of cybercriminals extend to sophisticated state-sponsored campaigns as well. A recent report from the cybersecurity firm ESET has detailed a notable Russian hacking operation, 'RoundPress,' attributed to the infamous Fancy Bear group. This campaign targeted government and military entities across several regions, employing advanced techniques to exploit vulnerabilities in webmail platforms, illustrating the increasingly geopolitical nature of cyber threats.

On a positive note, initiatives are underway to combat these cyber threats. Collaboration between international law enforcement agencies has led to significant disruptions in cybercriminal networks. A coordinated operation, involving entities such as the FBI and the National Crime Agency, successfully dismantled the Lockbit ransomware group, which had extorted over $120 million from numerous victims globally. This kind of multinational cooperation signals growing recognition of cybersecurity as a critical issue that transcends borders.

As companies and regulatory bodies navigate this perilous digital landscape, there is an urgent need for improved cybersecurity literacy at the executive level. Effective strategies now include adopting a zero-trust security framework, enhancing employee training about cyber hygiene, and maintaining constant vigilance in monitoring for breaches. The swift evolution of cyber threats, notably with the emergence of AI-driven risks, further complicates this task.

In conclusion, as cyber threats become ever more sophisticated and prevalent, companies across sectors must not only fortify their cyber defences but also foster a culture of security awareness within their organisations. The incidents of 2023 provide a crucial wake-up call, demanding that businesses be vigilant and proactive in their approach to cybersecurity, ensuring they are equipped to withstand the rising tide of cybercrime.

### Reference Map

1. Paragraph 1: [[1]](https://whbl.com/2025/05/21/factbox-cyber-threats-disrupt-global-firms-in-us-uk-and-europe/)
2. Paragraph 2: [[2]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[4]](https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf)
3. Paragraph 3: [[1]](https://whbl.com/2025/05/21/factbox-cyber-threats-disrupt-global-firms-in-us-uk-and-europe/), [[4]](https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf)
4. Paragraph 4: [[1]](https://whbl.com/2025/05/21/factbox-cyber-threats-disrupt-global-firms-in-us-uk-and-europe/), [[3]](https://www.techradar.com/pro/security/global-russian-hacking-campaign-steals-data-from-government-agencies)
5. Paragraph 5: [[5]](https://apnews.com/article/ce415e9ea0f11d31e6cf3e401a264d3c), [[7]](https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/)
6. Paragraph 6: [[4]](https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf), [[7]](https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/)
7. Conclusion: [[2]](https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b), [[4]](https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf), [[5]](https://apnews.com/article/ce415e9ea0f11d31e6cf3e401a264d3c)

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

## Bibliography

1. <https://whbl.com/2025/05/21/factbox-cyber-threats-disrupt-global-firms-in-us-uk-and-europe/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/a47dc006-c4f3-442f-8ab8-88633582958b> - A recent cyber attack on Marks & Spencer (M&S) is projected to cost the company £300 million, or about 30% of its previous year's operating profit. This incident underscores the rising threat of cybercrime, which more than 40% of UK businesses have encountered in the past year, according to the UK government's Cyber Security Breaches Survey. While retail headlines dominate, other sectors are even more exposed. For tech companies, however, such breaches are creating business opportunities as organizations invest heavily in cybersecurity—global spending on anti-hacking software is seeing double-digit annual growth and is projected to reach $300 billion by 2028. The evolving nature of cyber threats complicates the defensive landscape. Malware has declined to 20% of attacks, while 'vishing' has surged, and generative AI presents both risks and defensive potential. M&S had already doubled its cybersecurity spending since 2021 and is now accelerating its digital initiatives. Experts suggest that corporate boards need better cyber literacy, especially considering vulnerabilities caused by third-party access, which contributed to the M&S breach. Online sales at M&S will remain impaired for weeks, severely impacting its integrated retail strategy and reputation. The attack serves as a wake-up call for executives to enhance their cybersecurity frameworks.
3. <https://www.techradar.com/pro/security/global-russian-hacking-campaign-steals-data-from-government-agencies> - A recent report by cybersecurity firm ESET has uncovered a widespread Russian state-sponsored cyber espionage campaign named 'RoundPress,' active since 2023. The attackers, linked to the hacking group Fancy Bear (APT28), have targeted government and military entities across Eastern Europe, Africa, and Latin America, including countries like Greece, Ukraine, Serbia, and Ecuador. The campaign exploited multiple zero-day and known (n-day) vulnerabilities in webmail platforms such as Roundcube, MDaemon, Horde, and Zimbra. By embedding JavaScript-based malware within seemingly benign political-themed emails, the hackers exploited cross-site scripting (XSS) flaws to silently collect sensitive information such as login credentials, emails, contact lists, and two-factor authentication data. These attacks required no user interaction beyond opening the email. Though the malware lacked persistence and only operated while the email was open, the data exfiltrated was extensive. Victims included critical government, military, defense, and infrastructure organizations.
4. <https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf> - Cyber crime is a growing concern for both nation-states and private sectors, with the US and UK increasing their IT security budgets significantly in recent years. In 2023, 94% of IT leaders reported significant cyber attacks, and companies are ramping up spending on cyber security. Ransomware attacks, data breaches, and social engineering are common methods used by cyber criminals, with the financial sector being a prime target. Regulations are tightening, with initiatives such as the US's Circia and the EU's NIS2 and Dora aiming to enhance cyber security compliance and resilience. Effective strategies include adopting a zero-trust security model, simplifying security processes, leveraging cloud services, and educating employees about cyber hygiene. Collaboration and sharing of threat intelligence within and across sectors are crucial for combating cyber crime. Companies are encouraged to integrate security into their operational fabric, maintain constant monitoring, and have a robust response plan for potential breaches.
5. <https://apnews.com/article/ce415e9ea0f11d31e6cf3e401a264d3c> - U.S. authorities, collaborating with European partners, have dismantled the significant Qakbot malware network, active for over 15 years and responsible for numerous cybercrimes, including ransomware attacks. The joint operation, involving the FBI and law enforcement agencies from France, the U.K., Germany, the Netherlands, Romania, and Latvia, has successfully disabled Qakbot by seizing over 50 servers and remotely removing its malware from more than 700,000 infected computers. This takedown has notably impacted ransomware operations, affecting diverse sectors and resulting in nearly $58 million in illicit gains. However, experts caution that this disruption is likely temporary, with cybercriminals potentially reviving or shifting to other networks. The operation, named 'Duck Hunt,' highlights Qakbot's critical role in facilitating global cybercrime, affecting millions of users worldwide. Although $8.6 million in cryptocurrency was seized, no arrests were announced, and the investigation continues.
6. <https://www.axios.com/newsletters/axios-codebook-f0ed5092-1e1f-4d98-a553-8b79d68d0a7f> - In 2023, Americans lost approximately $1.3 billion to impersonation scams, a record-breaking amount driven by fraudsters posing as government officials or tech support agents. These scams have significantly increased since 2019 due to the rise of generative AI tools and remote work. The FBI's latest data highlights the growing prevalence of these scams, although only reported cases are considered. Additionally, concerns over TikTok's Chinese parent company, ByteDance, stem from cybersecurity fears, with the intelligence community warning about China's persistent cyber threat. China is also accused of creating TikTok accounts to influence the 2022 midterm elections, although they deny this claim. In other news, Microsoft continues to face cyberattacks from Russian hackers targeting its networks and source code. There's also a significant ransomware attack affecting Change Healthcare, causing daily losses of up to $1 billion for healthcare providers. Lastly, various cybersecurity threats and breaches are increasingly affecting different sectors, from state election workers worried about AI deepfakes to automakers collecting driver data for insurance purposes.
7. <https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/> - Operation Cronos, an international law enforcement effort led by Britain’s National Crime Agency (NCA) and the FBI, has successfully dismantled the Lockbit ransomware gang. This notorious group has targeted over 2,000 victims globally, extorting more than $120 million in ransom payments. Two Russian nationals, Artur Sungatov and Ivan Kondratyev, have been charged in connection with deploying Lockbit ransomware. The operation, involving ten countries, managed to seize control of Lockbit’s infrastructure, websites, source code, and decryption keys. The NCA, FBI, U.S. Department of Justice, and Europol also transformed Lockbit’s own website to release the gang's internal data, essentially locking out the cybercriminal group. In addition to arrests, 34 servers were seized, 200 cryptocurrency accounts frozen, and 14,000 rogue accounts closed. Lockbit’s operations have caused significant financial damage globally, with victims including major corporations like Boeing and Britain’s Royal Mail.