# Cyber attacks on M&S and Co-op escalate urgency for UK retail cybersecurity investments



In recent weeks, incidents of cyber attacks have shaken the foundations of prominent retail operations in the UK, underscoring the urgent need for heightened cybersecurity awareness among both businesses and investors. A notable example can be seen with Marks & Spencer (M&S), which has faced significant operational disruptions after falling victim to a major cyber hack. As a result, the company has paused its online shopping services, and Deutsche Bank estimates that this incident is costing M&S approximately £15 million a week. The Co-op has similarly struggled, grappling with stock shortages and a breach of customer data that further highlights the vulnerabilities faced by well-known brands.

Experts are sounding the alarm about the rising scale and severity of cyber threats. Mike Seidenberg, portfolio manager at Allianz Technology Trust, cited that over six billion malware attacks were recorded globally in 2023. He noted that "bad actors have increased their ambition," posing risks to not just retail entities but also critical infrastructure and government sectors. With only 4% of businesses reaching what is termed a 'mature' stage of cybersecurity readiness, the vast majority remain ill-equipped to fend off such attacks. This reality poses a significant risk to shareholders, particularly as M&S’s stock has already fallen over 6% in the wake of its attack.

In light of these developments, investing in cybersecurity has become both a lucrative opportunity and a potential safeguard for investors. The UK government, represented by Cabinet minister Pat McFadden, is set to enhance investments in cybersecurity, emphasising that “cybersecurity is not a luxury but an absolute necessity.” This signals a shift in perspective for both corporate and public sectors, potentially making cybersecurity investments more attractive to shareholders.

Recent research from Cisco further clarifies the precarious stance of companies regarding cybersecurity—only 15% of organisations reported being adequately prepared for modern threats, with 82% expecting to encounter disruptions within the next 12 to 24 months. Alarmingly, 60% had experienced at least one cybersecurity incident in the past year, many of which incurred significant financial losses, with 41% of those cases costing over $500,000. As financial strain from cyber incidents continues to mount, many businesses are ramping up their budgeting for cybersecurity measures; a survey indicated that 56% of Chief Information Security Officers (CISOs) had increased their budgets since 2022.

Investment trends indicate a burgeoning interest in cybersecurity firms, particularly as spending allocations shift amid rising threats. Jason Hollands of investment platform BestInvest observes that capital is increasingly flowing into this sector alongside traditional domains such as aerospace and defence. Recent studies show that more than 90% of companies have increased their cybersecurity budgets within just the last two years. Investments in emerging technologies, including artificial intelligence and machine learning designed for enhanced threat detection, are also on the rise.

Though opportunities abound, analysts warn against complacency in investment strategies. Laith Khalaf, head of investment analysis at AJ Bell, points out the unpredictability facing investors, as even cybersecurity firms themselves have been victims of attacks. He advises maintaining a diversified portfolio to mitigate risks. Stocks of companies in the cybersecurity domain exhibit volatility, evidenced by the fluctuating performance of firms like SysGroup, which has experienced both a drop of 26% over six months and a recent rebound of 10%.

For investors looking to capitalise on the upsurge in cybersecurity investments, several individual stocks and funds stand out. The Legal & General Cyber Security ETF and the iShares Digital Security ETF are notable for their focus on cybersecurity as a primary theme. Meanwhile, recent launches like the HANetf Future of Defence ETF indicate that now might be an opportune moment to enter this market.

As cyber incidents like those experienced by M&S and the Co-op become more common, the imperative for companies to bolster their defences is clear. The pathway for investors is increasingly paved with opportunities in cybersecurity, representing not only a safeguard against potential losses but also a strategic area for future growth.

### Reference Map

* Paragraph 1: (1), (2), (7)
* Paragraph 2: (1), (2)
* Paragraph 3: (1), (4)
* Paragraph 4: (3), (5)
* Paragraph 5: (2), (4), (6)
* Paragraph 6: (1), (5), (7)
* Paragraph 7: (1), (4), (2)
* Paragraph 8: (1), (2), (3)
* Paragraph 9: (1), (2), (3), (4)
* Paragraph 10: (1), (2), (6)

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

## Bibliography

1. <https://www.dailymail.co.uk/money/markets/article-14698227/How-profit-rush-protect-firms-M-S-style-cyber-attacks.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.dailymail.co.uk/money/markets/article-14698227/How-profit-rush-protect-firms-M-S-style-cyber-attacks.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - The article discusses the increasing prevalence and severity of cyber attacks, highlighting incidents involving M&S and the Co-op. It emphasizes the significant financial impact of such attacks, citing Deutsche Bank's estimate of £15 million weekly losses for M&S. Experts warn that many companies remain vulnerable, with only 4% of businesses considered 'mature' in their cyber readiness. The piece also explores investment opportunities in the cybersecurity sector, noting that over 90% of companies have increased their cybersecurity budgets in the past two years.
3. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m03/new-cisco-study-finds-only-15-of-companies-surveyed-are-ready-to-defend-against-cybersecurity-threats.html> - A Cisco study reveals that only 15% of organizations globally are prepared to defend against modern cybersecurity threats. The study highlights that 82% of respondents expect a cybersecurity incident to disrupt their business in the next 12 to 24 months. Additionally, 60% of respondents experienced a cybersecurity incident in the last 12 months, with 41% of those incidents costing at least $500,000. The report underscores the need for integrated security platforms and increased investment in cybersecurity.
4. <https://www.businesswire.com/news/home/20230907584795/en/Despite-Global-Economic-Slowdown-56-of-CISOs-Report-That-Their-Budget-Has-Increased-Since-2022> - Despite global economic challenges, 56% of Chief Information Security Officers (CISOs) reported an increase in their cybersecurity budgets since 2022. The survey, which included 130 CISOs from prominent enterprises, indicates that organizations are prioritizing cybersecurity investments amid rising threats. The report also highlights that the majority of CISOs plan to expand their budgets further, reflecting the growing importance of robust cybersecurity measures in the current threat landscape.
5. <https://venturebeat.com/security/network-iam-cloud-top-3-cybersecurity-spending-priorities-2023/> - A survey reveals that large enterprises are experiencing a 20% average increase in cybersecurity budgets, with mid-sized enterprises averaging a 5% increase. The top spending priorities for 2023 include network security, identity and access management (IAM), and cloud security. The report also notes that spending on emerging technologies like artificial intelligence and machine learning security is on the rise, indicating a strategic shift towards advanced threat detection and response capabilities.
6. <https://www.csoonline.com/article/653504/cisos-are-struggling-to-get-cybersecurity-budgets-report.html> - A study by IANS Research indicates a 65% decline in cybersecurity budget growth in the 2022-2023 cycle, attributed to global instability and inflationary pressures. The survey of 550 CISOs found that 37% of organizations experienced flat or declining cybersecurity budgets year-over-year. The report highlights the challenges CISOs face in securing adequate funding for cybersecurity initiatives amid broader economic constraints.
7. <https://www.bishopsstortfordindependent.co.uk/national/m-s-stops-hiring-after-systems-taken-offline-due-to-cyber-attack-145398/> - Marks & Spencer (M&S) halted all online job advertisements following a significant cyber attack that disrupted its operations. The retailer confirmed the removal of job listings from its website as technical teams worked to resolve the issues. The cyber incident, believed to be a ransomware attack, also led to the suspension of online orders and affected contactless payment systems, highlighting the operational impact of such security breaches.