# Stuart Machin vows to strengthen M&S after £300m cyberattack setback



Stuart Machin, the chief executive of Marks and Spencer (M&S), finds himself in the crosshairs of a significant crisis following a cyberattack that has sent shockwaves through the retailer. This attack, which has considerably disrupted operations and is estimated to cost the company around £300 million, threatens the impressive resurgence M&S has experienced in recent years. Despite the severe implications of the breach, which included the theft of personal customer data and a substantial impact on online sales, Machin remains resolute in his commitment to steering the company through this turbulent period.

In a recent interview, Machin described the moment he learned of the cyber incident as one filled with panic. "I went into shock," he recounted, elaborating on the initial anxiety and emotional turmoil he faced as he scrambled to communicate with store managers and reassure staff. Even amid the chaos, he sought to maintain perspective, referring to the attack not as a crisis but as "an incident, a setback, a bump in the road." This refusal to label the situation more dramatically underscores Machin's intention to focus on recovery and resilience rather than fear.

The breach, linked to social engineering tactics that exploited a third-party supplier, represents a growing threat faced by retailers. Although M&S has invested heavily in cybersecurity—tripling its tech spend over five years—this incident has exposed vulnerabilities within its operations. The involvement of a third-party contractor raises critical questions about the security measures in place not just at M&S, but across the retail sector, particularly when many businesses are increasingly reliant on external vendors for technology solutions. As a result, Machin is now focusing on a thorough cleansing of over 600 applications, with the hope of restoring full e-commerce services by July.

While the situation is undoubtedly serious, it has also highlighted an unexpected element of customer sentiment. In the face of the disruption, many loyal shoppers have rallied behind M&S, with support outpacing criticism. Communication has been a pivotal aspect of the retailer's response strategy; the company has been transparent with updates and apologies, helping to sustain customer trust. Recent promotions for loyal Sparks members have also been strategically introduced to further bolster goodwill and drive traffic back to online platforms upon their relaunch.

Moreover, analysts have taken a generally forgiving stance towards M&S in light of the cyberattack. The company's proactive management and commitment to rectifying the issues have been commended, with some brokers even expressing admiration for Machin's leadership during this crisis, despite downgrading stock ratings. M&S's share losses have been notable, amounting to around £750 million, yet shareholders seemed somewhat reassured by the retailer's strong performance prior to the attack, including a notable 22% rise in adjusted pre-tax profits to £875.5 million.

As the investigation into the breach continues, with authorities examining possible points of entry within the third-party network, Machin is determined to extract valuable lessons. He acknowledges that “everyone is vulnerable” and that the attackers only need a single moment of luck to exploit weaknesses. The broader context of rising cybercrime facing UK retailers complicates the narrative, particularly as the technology consultancy connected to M&S grapples with its own reputation amidst scrutiny.

Looking ahead, M&S will need to balance urgent recovery with a long-term technological overhaul. Machin has indicated plans to compress a two-year transformation timeline into six months, driven by the urgency of these recent events. This ambitious goal aligns with his broader vision of embracing change to fortify the company’s resilience in the face of adversity. While the cyber incident poses immediate challenges, Machin’s leadership and the strength of M&S's brand ethos may ultimately determine how well the retailer navigates these waters, emerging from adversity not just intact but stronger than before.

Such determination amidst difficult circumstances is echoed by Machin's reflection on past challenges faced by M&S. “We've been around for 140 years with lots of challenges. We survived that and we'll survive this,” he stated confidently, framing the situation as part of a larger legacy of resilience ingrained in the company's culture. As he steers M&S through these uncertain times, that legacy may well serve as both a foundation and a guiding light for the future.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/money/markets/article-14745687/M-S-boss-Stuart-Machin-vows-intend-come-better-stronger-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.ft.com/content/71bf35b0-740f-472f-96c6-86a9458e5844)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/money/markets/article-14745687/M-S-boss-Stuart-Machin-vows-intend-come-better-stronger-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[6]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/)
* Paragraph 3 – [[3]](https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0), [[4]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2), [[5]](https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8)
* Paragraph 4 – [[2]](https://www.ft.com/content/71bf35b0-740f-472f-96c6-86a9458e5844), [[4]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2)
* Paragraph 5 – [[3]](https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0), [[5]](https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8)
* Paragraph 6 – [[6]](https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/), [[7]](https://www.ft.com/content/fa80b540-c836-4c45-a77f-38aa1693c656)
* Paragraph 7 – [[1]](https://www.dailymail.co.uk/money/markets/article-14745687/M-S-boss-Stuart-Machin-vows-intend-come-better-stronger-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[4]](https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2)

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

## Bibliography

1. <https://www.dailymail.co.uk/money/markets/article-14745687/M-S-boss-Stuart-Machin-vows-intend-come-better-stronger-cyber-attack.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.ft.com/content/71bf35b0-740f-472f-96c6-86a9458e5844> - Marks & Spencer (M&S) is grappling with a major cyberattack, potentially costing the company £300 million in profits and severely disrupting online operations for over a month. The incident led to halted online orders, inventory shortages, and stolen customer data, with full system recovery possibly delayed until July. Despite this, the FTSE 100 retailer reported strong results in food and fashion, underscoring a business resurgence. To mitigate investor concerns, M&S raised its dividend by 20%, though its share price has dropped by approximately £750 million. Customer sentiment remains surprisingly positive, with many loyal shoppers expressing support rather than outrage. The company’s transparent crisis communication, including prompt warnings and apologies, has helped maintain trust. Other retailers like the Co-op and Harrods were also targeted, deflecting blame to a third-party supplier. M&S has boosted in-store staffing and ensured rapid customer service response times. Analysts caution against rushing restoration efforts, emphasizing the importance of getting it right. Despite the setbacks, M&S retains top rankings in customer trust surveys. The situation highlights the brand’s resilience and the key role of frontline staff in preserving customer loyalty. Going forward, rewarding Sparks loyalty members could help restore goodwill and drive online traffic upon relaunch.
3. <https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0> - Tata Consultancy Services (TCS) is conducting an internal investigation to determine if it was the entry point for a major cyberattack on Marks and Spencer (M&S) that compromised customer data and crippled the retailer's online clothing business for over three weeks. The attack caused an estimated £300 million hit to M&S's operating profit and resulted in a market capitalization loss of over £750 million. While M&S CEO Stuart Machin attributed the breach to human error involving a third-party contractor’s staff, he did not disclose whether a ransom was paid or if TCS—which has been M&S’s primary technology partner since 2018—was directly involved. Both TCS and M&S have refrained from official comments. The UK police have launched an investigation, and TCS expects to conclude its probe by the end of the month. The incident has cast a shadow over TCS’s reputation amidst a broader increase in cybercrime affecting UK retailers and India's tech industry. TCS, also partnered with UK retailer Co-op, confirmed its services were not linked to a separate cyberattack on that company. The event highlights growing cybersecurity challenges faced by global IT service providers.
4. <https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2> - Marks & Spencer (M&S) faced a significant cyber attack that compromised its operations and is expected to cut up to £300 million from this year’s operating profit. The attack forced the shutdown of its online clothing business for over three weeks, resulting in stolen customer data and a £750 million market capitalisation loss. The breach occurred due to social engineering tactics directed at a third-party supplier, allowing cybercriminals to bypass M&S’s internal defenses. Although M&S had significantly increased its investment in cybersecurity and expanded its security team, the incident exposed its vulnerability through third-party dependencies—a common risk for multinational retailers. In response, M&S is undertaking a comprehensive cleansing of more than 600 applications and thousands of servers, with full e-commerce operations expected to resume by July. CEO Stuart Machin described the attack as the most difficult challenge faced by his team, and the company is now focusing on a controlled and thorough recovery to ensure long-term security. The incident has also raised questions about potential cuts to executive bonuses and has heightened scrutiny of third-party IT partnerships in the retail industry.
5. <https://apnews.com/article/fef28bc0947576903cf83c3f42afc1e8> - British retailer Marks & Spencer (M&S) has estimated the cost of a recent cyberattack at approximately £300 million ($400 million). The attack, described as highly sophisticated and targeted, began around the Easter weekend and has significantly disrupted operations, particularly online sales of food, home, and beauty products. The disruption is expected to continue until July. The suspension of online shopping and the need for manual processes in stores have led to reduced food availability, increased waste, and higher logistics costs, adversely affecting profits. CEO Stuart Machin emphasized the company's focus on system recovery and declined to provide details about the attackers. M&S also revealed that hackers accessed customer personal data, including names, emails, addresses, and birth dates. The cyberattack is part of a broader wave affecting other British retailers, including Harrod’s and Co-op.
6. <https://www.reuters.com/business/aerospace-defense/ms-says-cyber-hackers-broke-through-third-party-contractor-2025-05-21/> - Marks & Spencer (M&S) disclosed that a recent cyberattack on its systems was carried out through a third-party contractor, bypassing its own digital defenses via social engineering tactics. CEO Stuart Machin revealed that despite increasing tech investment threefold over the past three years, the attackers exploited human vulnerabilities, gaining access through the contractor rather than a technical weakness. Although M&S has an IT contract with Tata Consulting Services (TCS), Machin did not confirm if TCS was the specific target. The breach was discovered over Easter weekend (April 19-20), and M&S promptly involved cybersecurity experts and authorities. The company halted online sales, anticipating full service restoration by July. The UK’s National Crime Agency is investigating a group of young English-speaking hackers believed to be responsible. So far, around 600 systems have been scanned and are being restored. M&S has not commented on any ransom demands due to law enforcement advice. The retailer, with annual sales of nearly £14 billion ($19 billion), emphasized the importance of vigilance against increasingly sophisticated cyber threats.
7. <https://www.ft.com/content/fa80b540-c836-4c45-a77f-38aa1693c656> - Marks & Spencer (M&S) anticipates a £300 million hit to its operating profits this year due to a cyber attack attributed to 'human error'. The attack, which has severely disrupted M&S's operations, has resulted in the theft of personal customer data and the shutdown of its online clothing business for over three weeks. It also impacted the supply of food items and caused nearly £750 million in market capitalisation losses. CEO Stuart Machin revealed that the breach occurred due to social engineering tactics targeting a third-party supplier, rather than flaws in M&S’s IT infrastructure. While the company declined to comment on whether a ransom was paid, it is working to mitigate losses through cost management, insurance, and other measures, hoping to recover half the anticipated losses. Despite the disruption, M&S remains committed to accelerating its technology overhaul, compressing a planned two-year timeline into six months. The setback has overshadowed strong annual financial results, including a 22% rise in adjusted pre-tax profits to £875.5 million and a 6.1% increase in sales to nearly £14 billion, though reported pre-tax profits dropped 24% due to a significant impairment in Ocado Retail.