The 2025 Marks & Spencer Cyberattack: Applying the Diamond Model

Joseph Severino
jseverino@gatech.edu

***Abstract*—**On April 22, 2025, Marks & Spencer (M&S) publicly acknowledged a cyber incident that disrupted retail operations and disabled parts of its online shopping infrastructure. The attack, attributed to the Scattered Spider cybercrime group, caused significant operational disruption across the company's digital systems. According to multiple statements to the London Stock Exchange, the incident was both sophisticated and costly, with a projected operating profit loss of £300 million. This paper analyzes the M&S cyberattack using the Diamond Model of Intrusion Analysis, examining the incident's adversary, infrastructure, capabilities, and victims.

1 INCIDENT DESCRIPTION

1.1 Background

Marks & Spencer (M&S) is a UK-based retailer founded in 1884, with revenue reaching $17 billion in the fiscal year 2025 (Wikipedia Contributors, 2026). M&S specializes in clothing, food, home products, and beauty items. Since launching their e-commerce store in 1999, they have become heavily reliant on their online ordering systems, with recent financial statements noting that over 30% of revenue is generated by online sales (London Stock Exchange, 2025c).

1.2 Timeline

During Easter weekend 2025, customers reported issues and glitches with contactless card payments. Customers also noted issues with their "Click & Collect" service online, which allows customers to place pickup orders at a physical store (Harpur, 2025). M&S found that several internal systems were no longer operational and began investigating the incident. On April 25, 2025, online shopping was suspended indefinitely. As investigations continued, the

scope of the breach kept increasing. It was not until June 10, 2025, that M&S resumed online orders, following approximately 46 days without the capability.

1.3 Impact

M&S revealed that customer data, including names, addresses, phone numbers, email addresses, and dates of birth, was exposed to the hackers (Whittaker, 2025). Many workloads had to revert to manual operations, such as logging shipments on paper and losing the ability to track millions of products because IT systems were offline. M&S estimated a total loss of £300 million profit as a direct result of this attack.

2 DIAMOND MODEL

2.1 Adversary

While not entirely confirmed, the M&S cyberattack is widely attributed to the efforts of cybercriminal group Scattered Spider, according to the National Crime Agency (NCA) (Tidy, 2025). Scattered Spider is a native English-speaking cybercriminal collective that has been active since at least 2022 and is known for targeting large organizations through social engineering and helpdesk impersonation ("Scattered Spider", n.d.). The group is financially motivated and has been linked to similar attacks, including the Co-op cyberattack (Tidy, 2025).

2.2 Infrastructure

To breach M&S, Scattered Spider targeted a third-party vendor contracted by the company, Tata Consultancy Services (TCS) (Alder, 2025). By exploiting the IT helpdesk password reset process, the attackers gained access to a compromised employee account. This access allowed them to infiltrate internal IT systems that supported online orders and logistics. These systems represent Type-2 infrastructure within the Diamond Model, since they are legitimate systems controlled by both the victim and trusted third parties that were abused without the victims' knowledge.

2.3 Capability

The attackers tricked Tata Consultancy Services (TCS) employees through social engineering, posing as legitimate M&S employees. They called their IT helpdesk impersonating a real M&S internal IT employee who needed to reset their

password. While helpdesk impersonation was the confirmed initial access vector, some reports suggest SIM-swapping may have also been used to bypass MFA controls, though this has not been officially confirmed (How, 2025). Once system access was obtained, the attackers successfully exfiltrated sensitive data and deployed DragonForce ransomware. DragonForce is an illicit service that not only steals customer records but also encrypts the affected servers, then demands payment. Using a double-extortion strategy causes damage, creates urgency, and results in data loss (Harpur, 2025). M&S refused to comment on whether any ransom was paid. These techniques show how attackers combine both human manipulation and ransomware deployment to achieve initial access and financial extortion.

2.4 Victim

M&S was the primary victim of this attack in part due to the company's reliance on e-commerce systems. As a major retail brand holding roughly 10.5% of the entire UK clothing market share, M&S represents a lucrative target for cybercriminal groups to target (Davey, 2025). At this scale of operations, M&S stores millions of customer records, creating the potential for attackers to access sensitive personal information. It also places a large operational dependence on IT systems that all rely on each other for tasks like logistics, online ordering, payment systems, and inventory tracking. This incident shows how "sophisticated cyberattacks can propagate quickly across the attacked networks while remaining covert during this process and consequently can cause substantial damages to their intended target, "(Gilad & Tishler, 2024). In addition to M&S, Tata Consultancy Services (TCS) was also a victim in this attack, as TCS employees were manipulated through social engineering to gain access to M&S's IT systems initially. Lastly, customers were victims as their personal information was stolen without their consent, resulting in potential privacy and fraud risk.

2.5 Meta-Features

Social-Political: Scattered Spider's financial motivation and M&S's scale created the natural adversary-victim pairing. The alleged cybercriminal group simply targeted M&S since the operational disruption could create enough urgency to enable a ransomware payment. At the same time, M&S had personal records for millions of customers, making a breach valuable. This is consistent with

Scattered Spider's approach of targeting large retailers, such as Co-op and Harrods.

Technology: This attack was enabled by a convergence of multiple exploits enabled by exploitable gaps in M&S's security posture. The attackers were aware that M&S IT services were outsourced and made use of their weak identity verification processes for resetting passwords. Ransomware-as-a-service was also utilized enabling fast and efficient data exfiltration that went undetected once the attacker gained access to the systems.

3 POLICY ASSESSMENT AND RECOMMENDATIONS

This incident clearly exposed policy gaps at the organizational level. Attackers successfully breached M&S due to weaknesses in their internal security practices. The helpdesk password reset procedures were exploited, highlighting weaknesses in identity verification and account recovery processes. While outsourcing IT services can be cost-effective, vendor access relationships must be properly managed, and employees must be trained to detect potential attackers. Organizational governance is, therefore, the most appropriate level for addressing this issue. Helpdesk identity verification and password recovery procedures are internal controls that are managed by the organization itself. Many recent ransomware attacks have exploited similar social engineering weaknesses, reinforcing the need for even stronger internal governance.

While policies are also important at the national, transnational, and industry level, none of these solve the root cause of this specific attack. The attackers illegally gained access by impersonating employees and using human error to their advantage. Cybersecurity frameworks already exist. The issue was simply an implementation failure rather than a lack of regulation. Government policy cannot realistically regulate how internal helpdesks verify users requesting assistance.

Several recommendations to M&S's organizational policies could help prevent future incidents like these from recurring. SMS-based authentication should not be relied upon as the primary method of authentication due to known weaknesses such as SIM-swapping and interception. SMS authentication introduces additional attack surfaces involving telecommunications providers and network infrastructure, and the protocol itself is unencrypted and

susceptible to interception. SIM-swapping was a potential exploit method that the attackers in this case may have used. This is where an adversary can gain access to the SIM (typically eSIM) of a target to receive their SMS-based multifactor authentication codes. Instead, M&S should utilize authenticator apps on company-managed devices. When a company provides mobile device management (MDM), this ensures employee devices maintain minimum levels of security measures to protect not only their own data, but company data as well, like an authenticator app. Even better, they could support passkeys for verification. "These keys (one public, one private) are two pieces of data that must match each other for the user's identity to be confirmed" (Wolek, 2024) making passkeys a much more viable option.

M&S should ensure that stronger account recovery verification is in place when users forget their passwords. The IT helpdesk should always ensure the user is verified using multiple forms of verification, preferably involving a passkey. They should also enact an approval process when trying to reset passwords or even require a time delay if a user has elevated privileges as well. Lastly, M&S should implement data loss prevention (DLP), so its internal systems can be monitored for abnormal data movement. Many traditional security systems only detect external threats rather than uncovering internal threats that exfiltrate data outbound. A viable DLP system likely would've flagged or even prevented any attacker from being able to export sensitive data out of the databases.

As social engineering is becoming increasingly common, organizational policies need to be addressed to prevent attacks. Identity systems are a major attack vector that must have proper guidelines for processes such as password resets. Organizations like M&S had to deal with the costly impact due to not following practices recommended by frameworks such as the NIST Cybersecurity Framework. Specifically, PR.AA writes out guidelines to manage identities and enforce proper authentication. PR.AC addresses access control and the principle of least privilege, which would limit attacker control once actually inside the network. DE.CM provides monitoring guidelines that directly support a DLP implementation to detect abnormal data movement. By transitioning away from SMS-based authentication, ensuring stronger account recovery practices are in place, and investing in proper data loss prevention, M&S will be in a much stronger security position.

4 REFERENCES

1. Alder, S. (2025, June 10). *MSPs & IT Vendors Targeted by Scattered Spider Threat Group*. The HIPAA Journal. https://www.hipaajournal.com/msps-it-vendors-targeted-scattered-spider
2. BBC News. (2025, May 13). *Marks & Spencer says customer data stolen in cyber attack | BBC News*. YouTube. https://www.youtube.com/watch?v=VVDBmBsp-rc
3. Davey, J. (2025, November 12). M&S shakes up fashion supply chain to spark online growth. *Reuters*. https://www.reuters.com/business/retail-consumer/ms-shakes-up-fashion-supply-chain-spark-online-growth-2025-11-12/
4. Ellery, B., & Sellman, M. (2025, May 11). *Cases of Sim-swap fraud — the method used to hack M&S — surge*. Thetimes.com; The Times. https://www.thetimes.com/uk/crime/article/cases-of-sim-swap-fraud-the-method-used-to-hack-m-and-s-surge-3bhs5csff
5. Fortinet. (2022). *Recent Cyber Attacks—News on Data and Security Breaches*. Fortinet. https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks
6. Gilad, A., & Tishler, A. (2024). Measuring and Mitigating the Risk of Advanced Cyberattackers. *Decision Analysis*, *21*(4), 215–234.
7. Harpur, R. (2025, August 7). *Marks & Spencer Breach: How a Ransomware Attack Crippled a UK Retail Giant*. BlackFog. https://www.blackfog.com/marks-and-spencer-ransomware-attack/
8. How, F. (2025, May 22). *PureCyber*. PureCyber. https://purecyber.com/news-1/retail-sim-swap-fraud
9. *London Stock Exchange | London Stock Exchange*. (2025a). Londonstockexchange.com. https://www.londonstockexchange.com/news-article/MKS/cyber-incident-further-update/17033373
10. *London Stock Exchange | London Stock Exchange*. (2025b). Londonstockexchange.com. https://www.londonstockexchange.com/news-article/MKS/cyber-incident-update/16999905
11. *London Stock Exchange | London Stock Exchange*. (2025c). Londonstockexchange.com.

https://www.londonstockexchange.com/news-article/MKS/final-results/17046629

12. *Scattered Spider, Roasted oktapus, Group G1015 | MITRE ATT&CK®*. (n.d.). Attack.mitre.org. https://attack.mitre.org/groups/G1015/
13. Tidy, J. (2025, May 20). M&S and Co-op hacks: Scattered Spider is focus of police investigation. *BBC*. https://www.bbc.com/news/articles/ckgnndrgxv30
14. White, M. (2025, April 30). *M&S ransomware hack: Active Directory security lessons*. Specops Software. https://specopssoft.com/blog/marks-spencer-ransomware-active-directory/
15. Whittaker, Z. (2025, May 13). *Marks & Spencer confirms customers' personal data was stolen in hack | TechCrunch*. TechCrunch. https://techcrunch.com/2025/05/13/marks-spencer-confirms-customers-personal-data-was-stolen-in-hack/
16. Wikipedia Contributors. (2026). *Marks & Spencer*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Marks_%26_Spencer
17. Wolek, K. (2024). UNLOCKING THE POTENTIAL OF PASSKEYS: Fundamental ideas, practical applications, and key cybersecurity considerations. *AALL Spectrum*, *28*(5), 17–19.