Integrity report

A critical analysis of the cyber attack on Marks & Spencer in 2025: technical, organisational and governance perspectives

Anonymous

HUMAN SCORE
78%

READABILITY SCORE
13
/ 100

English · 3,920 words · 29,651 characters

Assessment

Winston has detected the text as 78% human. The content closely matches human linguistic structures and nuances. We are highly confident it was written by a human.

This text has a **readability score of 13/100** and has a **U.S. school College graduate level**, which means it is very difficult to read and is best understood by university graduates.

AI prediction map

Likely AI generated Possibly AI generated Unlikely AI generated

Abstract

In the spring of 2025, Marks & Spencer (M&S), a leading British food and clothing retailer was affected by a ransomware attack that led to significant disruptions of both digital and physical services. By using open-source analyses we can link the incident to the cybercriminal group Scattered Spider (also known as Octo Tempest/UNC3944) and the use of DragonForce ransomware (Microsoft, 2025; Google Threat Intelligence, 2025; Trend Micro, 2025; Darktrace, 2025). The incident resulted in the compromise of customer data and a substantial negative impact on the operational continuity and financial performance of the organisation (BBC News, 2025; Marks and Spencer Group plc, 2025a; Marks and Spencer Group plc, 2025b; Reuters, 2025).

This report aims to systematically analyse the incident based on three core aspects:

the characteristics of the incident and the involved actors

the technical attack chain and associated tactics, techniques and procedures (TTPs), and

the legal and organisational implications.

Based on primary sources and current threat intelligence, the timeline of the incident is reconstructed, from presumed initial access in the first quarter of 2025 to the phased recovery period in June–July 2025 (BBC News, 2025; Marks and Spencer Group plc, 2025a; Marks and Spencer Group plc, 2025b; Reuters, 2025), as also suggested in secondary analyses (Xuereb, 2025).

The technical analysis focuses on the application of social engineering, abuse of identity and helpdesk processes and lateral movement within hybrid IT environments, as described in recent threat-intelligence reports (CISA et al., 2025; Microsoft, 2025; Google Threat Intelligence, 2025; Trend Micro, 2025; Fortinet FortiGuard Labs, 2025; Darktrace, 2025). The impact of the incident is interpreted from a cyber risk-economic perspective (Xin et al., 2026). Finally, the case is placed in the broader context of ransomware attacks in the retail sector to identify recurring patterns and structural vulnerabilities.

My analysis shows that the attack was driven by the use of advanced social-engineering techniques, eventually gaining access to administrative accounts and lateral movement across critical systems, consistent with MITRE ATT&CK tactics in initial access, credential access and lateral movement. These attacks demonstrate that modern ransomware increasingly exploits organisational and identity-related weaknesses, posing a strategic risk for digitally dependent organisations, further amplified by AI.

Analysis of the incident

Cyber Kill Chain: type and methodology of the attack

Reconnaissance & Targeting

The criminal group Scattered Spider typically targets large commercial organisations who are highly dependent on digital services, including retail and cloud-based environments (Microsoft, 2025; CISA et al., 2025). In the preparation for the attack on M&S, the group likely gathered information via OSINT about the organisation, its suppliers, IT service providers and used identity and cloud platforms (Google Threat Intelligence, 2025; Phipps and Nurse, 2026).

This form of preparation indicates a targeted and well-organised attack and underlines the importance of organisational awareness and protection against social engineering, since such information is often publicly accessible and difficult to mitigate technically.

Initial Access

It is known that UNC3944/Octo Tempest gains initial access via social engineering, where attackers impersonate legitimate users to reset passwords or adjust MFA settings through manipulation of IT helpdesks (Microsoft, 2025; CISA et al., 2025).

In the case of M&S, it is therefore plausible that a combination of helpdesk manipulation, possible SIM-swaps and the abuse of third-party accounts led to access to identity and administrative accounts (Google Threat Intelligence, 2025; Xuereb, 2025). This points to weaknesses in identity verification processes and insufficiently robust controls around account recovery and MFA reset procedures. Moreover, this suggests that role-based access control (RBAC) and the principle of least privilege (PoLP) were not effectively implemented, as compromised accounts apparently provided access to critical systems and administrative functionalities that should normally be strictly restricted.

Privilege Escalation & Persistence

After initial access, Scattered Spider typically uses identity and SSO integrations to expand privileges, steal tokens and establish persistent access, among other things by creating new accounts and modifying MFA settings (Microsoft, 2025; Google Threat Intelligence, 2025).

Within the M&S environment, it is plausible that such techniques led to elevated access, even to virtualisation and storage layers, including backup systems (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025). This suggests shortcomings in privilege management and monitoring of critical (administrative) actions.

Discovery & Lateral Movement

The group conducts extensive network reconnaissance after compromise, including domain enumeration and identification of critical systems, often using legitimate tools ("living off the land") (CISA et al., 2025; Trend Micro, 2025).

For the attack on M&S, the attackers are believed to have moved laterally to critical core systems, like the onces used for order processing and operational processes, which is consistent with the observed disruptions (BBC News, 2025; Marks and Spencer Group plc, 2025a; Xuereb, 2025). This points to limited network segmentation and insufficient detection of unusual internal activities, as also described in threat intelligence on similar attacks (CISA et al., 2025; Microsoft, 2025). In addition, this suggests possible weaknesses in access management and privilege limitation, where compromised accounts were apparently able to gain access to systems with a higher criticality level.

Data Collection & Exfiltration

Scattered Spider combines ransomware attacks with data theft, targeting sensitive business and customer information (Microsoft, 2025; Google Threat Intelligence, 2025; Phipps and Nurse, 2026). In open-source threat intelligence, the group is linked to the use of DragonForce ransomware, which specifically targets the encryption of virtual infrastructure and file servers (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025).

M&S confirmed that personal customer data was exfiltrated, while secondary sources suggest that other datasets may also have been exfiltrated (Marks and Spencer Group plc, 2025a; BBC News, 2025; Xuereb, 2025). This indicates insufficient monitoring of data exfiltration and weaknesses in data loss prevention mechanisms.

Ransomware Deployment (DragonForce)

DragonForce is used by affiliates to encrypt virtual infrastructure and file servers at scale, often after disabling or manipulating security and backup systems (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025).

The scale and duration of the disruptions within M&S, including outages of online services and internal systems, are consistent with such a coordinated attack on critical infrastructure (BBC News, 2025; Marks and Spencer Group plc, 2025a; Xuereb, 2025). This suggests that backup and recovery mechanisms may have been insufficiently effective, for example because backups were accessible to attackers or not quickly deployable within the recovery strategy.

Impact, Extortion & Negotiation

After encryption of data, groups such as Scattered Spider use double extortion, where both decryption and the non-publication of stolen data are offered in exchange for payment (Phipps and Nurse, 2026; CISA et al., 2025).

Although it has not been publicly confirmed whether M&S paid a ransom, the prolonged disruptions and significant financial impact indicate a complex recovery and negotiation process (Reuters, 2025; Marks and Spencer Group plc, 2025b; Xuereb, 2025). This underlines the strategic impact of ransomware attacks on both operational and financial levels. The reconstructed attack chain above forms the basis for the following impact analysis.

Parties involved

The primary target of the incident was Marks & Spencer (M&S), a food and clothing retailer with a strong dependence on digital services, online sales and integrated operational systems (BBC News, 2025; Marks and Spencer Group plc, 2025a). It is precisely this combination of scale, brand value and high digital dependence that makes the organisation attractive to ransomware groups seeking to exert maximum operational and financial pressure (Phipps and Nurse, 2026; Xin et al., 2026).

As for the attacking party, the incident is linked in open-source threat-intelligence analyses to the cybercriminal group Scattered Spider, also known as UNC3944 or Octo Tempest, using DragonForce ransomware (Poireault, 2025; CISA et al., 2025; Microsoft, 2025; Trend Micro, 2025). M&S itself has not publicly confirmed this attribution and consistently refers in its official communication to a "cyber incident", which means the link to Scattered Spider and DragonForce must be presented cautiously as a likely, but not formally confirmed attribution (Marks and Spencer Group plc, 2025a; 2025b).

In addition to M&S and the presumed attackers, third parties also play a role in the analysis. Various threat-intelligence reports emphasise that Scattered Spider frequently abuses supplier relationships, third-party accounts, identity providers and helpdesk processes to gain initial access or escalate privileges (Google Threat Intelligence, 2025; CISA et al., 2025; nquiringminds Ltd, 2025). As a result, external service providers, cloud and identity providers and outsourced IT support chains become relevant involved parties within the broader attack environment, which underlines the necessity of robust identity and supply-chain governance, including clear responsibilities and control mechanisms across organisational boundaries.

Motivation of the attackers

The attack on Marks & Spencer must first of all be understood against the background of financially motivated cybercrime, as described in recent analyses of ransomware ecosystems and groups such as Scattered Spider/UNC3944 (Phipps and Nurse, 2026; CISA et al., 2025). Scattered Spider operates to a large extent opportunistically but preferably targets large organisations with a strong digital dependence and substantial revenue, because this combination increases the likelihood of paying large ransom sums and generating additional financial gains through data theft and extortion (Microsoft, 2025; Google Threat Intelligence, 2025). M&S fits within this profile as a leading British food and clothing retailer with an extensive digital ecosystem of online sales, loyalty programmes and supply-chain integrations (BBC News, 2025; Marks and Spencer Group plc, 2025a).

In addition, the economic value of the exfiltrated data plays a key role in the motivation. The combination of customer and transaction data, loyalty points, contact information and possibly other alternative internal datasets forms a rich source for follow-up fraud, identity misuse and further social-engineering campaigns, both by the original attackers and by third parties to whom this data may be resold (Phipps and Nurse, 2026; Xuereb, 2025). The use of double-extortion techniques, where both decryption and the non-publication of exfiltrated data are used as leverage, reinforces this economic motive, because the reputational and trust damage for a consumer-focused organisation such as M&S can be directly translated into additional negotiation power for the attackers (CISA et al., 2025; Trend Micro, 2025).

Finally, the simultaneous targeting of multiple large retailers, including Co-op and Harrods, points to a deliberate sector-specific strategy. Threat reports describe this campaign as an attempt to create maximum leverage within a sector where margins, customer trust and supply-chain stability are closely intertwined (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025; CISA et al., 2025). This combination of direct financial gain, secondary data monetisation and strategic sector disruption underlines that the attack on M&S should not be seen as an isolated incident, but as part of a deliberate, economically driven campaign against the broader retail infrastructure.

Impact of the incident (non-legal)

The ransomware attack on Marks & Spencer had far-reaching consequences for operational continuity, financial performance and trust relationships with stakeholders. Operationally, the incident led to prolonged disruptions of both online and physical processes. Shortly after the initial report in April 2025, M&S paused all new online orders and the functionality of the website and app was significantly limited, while stores had to revert to manual procedures for inventory management and transaction processing (BBC News, 2025; Marks and Spencer Group plc, 2025a; Xuereb, 2025). This combination of limited digital service, inefficient emergency procedures and logistical delays translates directly into loss of revenue, increased operational costs and a negative customer experience.

The disruption extended over several weeks, with M&S indicating that full normalisation was only expected towards June–July 2025 (Marks and Spencer Group plc, 2025b; Reuters, 2025). This indicates that not only peripheral applications, but also core systems for order processing, inventory planning and payment infrastructure were affected. From a business continuity perspective, this illustrates that critical processes were insufficiently robustly designed against a scenario in which both IT systems and operational processes are disrupted simultaneously, despite the known threat of large-scale ransomware attacks against the retail sector (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025).

Financially, the impact is estimated at approximately £300 million in operating profit loss, mainly as a result of lost sales, recovery costs and enhanced security, and possible contractual and reputational consequences (Reuters, 2025; Marks and Spencer Group plc, 2025b). From a risk management perspective, this magnitude shows that the residual risk around ransomware and identity-based attacks may have been underestimated for an organisation with the scale and system dependence of M&S. Placed within the context of economic risk models such as CYREM-ORM, this underlines that the combination of high threat likelihood and large potential impact has not been sufficiently translated into proportional preventive investments in security and resilience (Xin et al., 2026).

In addition to the direct financial and operational effects, the incident also had important implications for data and trust relationships with customers and staff. M&S confirmed that personal customer data, including identity and contact information and order history, was exfiltrated, exposing affected individuals to increased risks of phishing, social-engineering attacks and potential forms of identity misuse (Marks and Spencer Group plc, 2025a; BBC News, 2025; Xuereb, 2025). Although no evidence was presented that payment card data or passwords were compromised in

readable form, the impact on customer trust is significant, especially in a context where multiple major British retailers were affected by similar attacks in a short period of time (BBC News, 2025; CISA et al., 2025).

Reputational and strategic impact are difficult to quantify, but equally relevant. The media attention and comparisons with other retail incidents reinforced the perception that M&S was insufficiently prepared for identity-driven ransomware campaigns (Xuereb, 2025; Phipps and Nurse, 2026). This may have consequences for customer loyalty, supplier relationships and the perception of M&S as a reliable handler of sensitive data. At the same time, the case creates pressure on the board and senior management to reassess governance structures, risk assessments and investment decisions in cyber security and resilience (Marks and Spencer Group plc, 2025b; Xin et al., 2026). Taken together, these effects illustrate that cyber incidents are no longer purely technical disruptions, but strategic events that directly affect operations, trust and competitive position.

Legal and regulatory framework

Applicable UK privacy legislation

The cyber attack on Marks & Spencer falls within the scope of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, since the organisation processes customer and transaction data on a large-scale and structural basis as part of its commercial activities (Marks and Spencer Group plc, 2025a; BBC News, 2025). As such, the incident is subject to obligations relating to, among other things, the security of personal data, accountability and breach notification.

Within this framework, M&S has the obligation to implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss or destruction. The confirmed compromise of customer data indicates that the implemented measures may not have been sufficiently effective in relation to the risk profile of the organisation, although it cannot be determined exactly where the protection failed based on publicly available information (Marks and Spencer Group plc, 2025a; Xuereb, 2025).

The available sources do not provide insight into retention periods, data minimisation practices or the legal grounds for the relevant processing activities, making it not possible to assess to what extent M&S actually complied with the principle of storage limitation. Nevertheless, the scale of the compromised datasets underlines the importance of strict data minimisation and limited storage duration, because both the scale and sensitivity of the stored data significantly increase the potential impact of a data breach (BBC News, 2025; Xuereb, 2025).

In addition, the UK GDPR obliges organisations to report data breaches that pose a risk to the rights and freedoms of individuals within 72 hours to the supervisory authority and, where appropriate, also to the affected individuals. Given the nature of the leaked information, including contact details and order history, it is evident that this incident presents a relevant risk in terms of privacy violation, targeted phishing and potential fraud, and therefore activates notification and communication obligations (Marks and Spencer Group plc, 2025a; 2025b; Reuters, 2025).

Sectoral standards and guidelines

In addition to formal data protection legislation, M&S operates within a broader ecosystem of sector-specific standards, guidelines and best practices for cyber security, including guidance from the UK National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO). These guidelines function in practice as an important framework for 'good practice' in the area of cyber hygiene, incident response and resilience in the UK market.

The joint CISA advisory on the Scattered Spider group, together with threat reports from Microsoft, Google Threat Intelligence (Mandiant) and Trend Micro, show that the TTPs relating to identity abuse, helpdesk social engineering and DragonForce ransomware were already well documented and publicly known before and during the attack on M&S (CISA et al., 2025; Microsoft, 2025; Google Threat Intelligence, 2025; Trend Micro, 2025). From a regulatory and governance perspective, this strengthens the expectation that an organisation of the scale of M&S proactively implements measures aligned with these known threats, including identity governance but more importantly also organisational measures such as targeted training and awareness regarding social engineering, given the central role of the human factor in this attack chain. This raises broader questions regarding the effectiveness of governance structures and risk management within this organisation.

Although Marks & Spencer does not necessarily fall within the formal scope of the Network and Information Systems Regulations 2018 (NIS Regulations), these regulations do provide a relevant reference framework for cyber security and operational resilience. The NIS Regulations emphasise the implementation of appropriate and proportionate technical and organisational measures and the safeguarding of continuity of essential services. In the context of the M&S incident, this underlines the broader expectation that organisations with a high societal and economic impact implement comparable levels of cyber resilience and incident response capability.

Following an incident of this scale, it is evident that Marks & Spencer has implemented a combination of technical, operational and organisational recovery measures. Based on the nature of the disruptions and the phased recovery period, it is plausible that priority was given to isolating affected systems, limiting further lateral movement, restoring critical business processes and investigating the scope of the compromise (Marks and Spencer Group plc, 2025a; 2025b; Reuters, 2025). The confirmation of exfiltrated customer data also implies that forensic investigation, breach assessment and communication with affected individuals were part of the response (Marks and Spencer Group plc, 2025a; BBC News, 2025; Xuereb, 2025).

Although not all technical details are publicly known, the available sources suggest that recovery was complex and time-consuming. This indicates that not only endpoints or individual user accounts were affected, but also core systems and virtualisation and backup environments were involved in the incident (BBC News, 2025; Xuereb, 2025; Trend Micro, 2025; Fortinet FortiGuard Labs, 2025). In such scenarios, recovery typically consists of revoking or resetting compromised accounts, re-enforcing strong multi-factor authentication, validating administrative privileges, reviewing identity and SSO configurations and gradually restoring systems to production (Microsoft, 2025; Google Threat Intelligence, 2025).

Based on the reconstructed attack chain, it is evident that additional measures were required that focus on identity and access governance. Because the presumed initial access is linked to helpdesk social engineering, abuse of MFA reset procedures and abuse of third-party accounts,

M&S would have benefited from stricter verification processes for account recovery, excluding high-risk resets based solely on telephone verification and additional controls on changes in privileged accounts (Microsoft, 2025; Google Threat Intelligence, 2025; CISA et al., 2025). Likewise, more granular role-based access control, host-based access control and stricter application of the principle of least privilege could have limited the impact of compromised accounts (Phipps and Nurse, 2026).

In addition, the later stages of the attack indicate the necessity of stronger network segmentation, improved detection of unusual internal activities and stricter separation between production, management and backup environments. When attackers can move relatively unhindered from identity compromise to critical systems for order processing and operational processes, this indicates an insufficiently layered security architecture; improved monitoring, behavioural analysis of accounts, network detection and clearly defined access boundaries could have increased the chance of early detection (CISA et al., 2025; Microsoft, 2025; Darktrace, 2025).

Finally, the likely use of DragonForce ransomware underlines the importance of ransomware resilience at infrastructure level. Effective countermeasures include isolated and regularly tested backups, minimal necessary management connections to virtualisation and storage layers, accelerated recovery procedures for business-critical systems and scenario exercises focused on double-extortion scenarios (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025). Given that the TTPs of Scattered Spider and related groups were already documented, an organisation of the scale and digital dependence of M&S could be expected to have translated these threats into preventive and detective security measures (CISA et al., 2025; Microsoft, 2025; Google Threat Intelligence, 2025). This underlines that effective ransomware resilience is dependent on an integrated approach of identity management, organisational processes and continuous monitoring.

Comparable cyber attacks in the retail sector

Co-op (2025)

The cyber attack on the British retailer Co-op in 2025 shows strong similarities with the incident at Marks & Spencer, both in terms of attack vector and techniques used. Open-source reporting links the attack to the same group, namely Scattered Spider (UNC3944), which uses intensive social-engineering techniques and identity abuse to obtain initial access (CISA et al., 2025; Microsoft, 2025; Google Threat Intelligence, 2025). As with M&S, Co-op reported helpdesk manipulation, abuse of identity and third-party accounts and subsequent escalation to critical systems, indicating similar vulnerabilities in identity and access management and network segmentation.

The attack resulted in the compromise of large volumes of customer and member data and led to significant disruptions in digital services and physical store operations, in line with the pattern also observed at M&S (Google Threat Intelligence, 2025; Xuereb, 2025). Several analyses describe the financial impact as substantial, partly because the combination of data theft and ransomware was used in a double-extortion strategy where both decryption and non-publication of data were used as leverage (CISA et al., 2025; Microsoft, 2025).

Harrods (2025)

The cyber attack on Harrods in 2025 is also linked to the same broader campaign of ransomware attacks in the retail sector. Threat-intelligence reports on DragonForce and Scattered Spider describe this attack as part of a coordinated wave in which similar tactics, techniques and procedures (TTPs) were used against multiple large retailers, including M&S, Co-op and Harrods (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025; CISA et al., 2025).

Although less detailed public information is available about the exact attack chain at Harrods than at M&S and Co-op, analyses point to a similar pattern of social engineering, identity compromise and presumed use of ransomware against core systems (Trend Micro, 2025; Microsoft, 2025). The impact manifested itself, among other things, in disruptions of digital services and reputational damage, which is consistent with the effects also observed at M&S and Co-op (Xuereb, 2025; BBC News, 2025). This overlap in targets and attack methods suggests that larger retail organisations with similar digital dependencies and identity architectures are particularly attractive and vulnerable to such campaigns.

Comparative analysis

As shown in Table 1, the attacks on Marks & Spencer, Co-op and Harrods show strong similarities in attack vector and impact. The attacks show similarities in attack methods within the retail sector. In all three cases, initial access is obtained via social engineering and identity abuse, whereby traditional perimeter security is bypassed because attackers compromise legitimate accounts and processes rather than primarily exploiting software vulnerabilities (CISA et al., 2025; Microsoft, 2025; Google Threat Intelligence, 2025; Darktrace, 2025).

In addition, it is notable that the attacks target core systems and critical infrastructure, such as virtualisation platforms and order and inventory systems, which leads to significant operational disruptions and financial damage in all three cases (Trend Micro, 2025; Fortinet FortiGuard Labs, 2025; Xuereb, 2025). The combination of data theft and ransomware points to a consistent application of double-extortion strategies, where both business continuity and reputation are put under pressure (Phipps and Nurse, 2026; CISA et al., 2025).

An important pattern is the central role of identity and access management as the primary attack vector. Instead of only exploiting technical vulnerabilities in software, the attackers use human and organisational weaknesses, such as insufficient verification procedures at helpdesks, weak control over privileged accounts and limited detection of unusual activities (Microsoft, 2025; Google Threat Intelligence, 2025; Darktrace, 2025). Taken together, these cases illustrate a broader shift in the threat landscape, where identity-based attacks and social engineering play a dominant role in advanced ransomware campaigns. This underlines that effective defence is not only dependent on technical security measures, but also on robust governance, access management and organisational resilience (Phipps and Nurse, 2026; Xin et al., 2026).