National Security in a Cyber-Age:

Marks and Spencer plc – A risk Assessment.

Joshua Alexander Joseph McManus

(Edited and or reviewed by Microsoft Software)

2401049

BA (Hons) – Security, Intelligence and Cyber

The University of Buckingham (2024-2026)

[Author's Notes: https://archive.org/details/2401049-Dec2024-01]

Table of Contents

Introduction:

April 2025 saw Marks and Spencer Plc, a leading international retail company from Leeds[1], become the victim of a ransomware attack – alongside the Co-operative Group Limited and Harrods Group (Holding) Limited[2]. Marks and Spencer Plc (referred to outwith as M&S) is a key factor in the British retail sector, being the first to surpass the £1 Billion pre-tax profit threshold[3], highlighting its critical role in the British economy.

This attack, which is thought to be linked to the ransomware group DragonForce and the hacking collective Scattered Spider[4], disrupted core business operations and compromised sensitive customer data, leading to questions on who was truly behind this incident as an attack on national retail infrastructure could signal weakness to enemy states. This has since been in question as these groups have ties to the Russian state[5]. At the same time there has been mixed messages from Russian media as they have presented 'mocking remarks'[6]

[1] Marks & Spencer (2025). *Our History*. [online] Marks & Spencer. Available at: https://corporate.marksandspencer.com/about-us/our-history [Accessed 9 Jun. 2025].

[2] Ford, N. (2025). *The Co-Op, M&S, Harrods… You? Mitigating the Risk of Ransomware - IT Governance Blog*. [online] IT Governance Blog. Available at: https://www.itgovernance.co.uk/blog/the-co-op-ms-harrods-you-mitigating-the-risk-of-ransomware [Accessed 9 Jun. 2025].

[3] The Telegraph (2008). Marks & Spencer: A recent history | Ghostarchive. [online] Ghostarchive.org. Available at: https://ghostarchive.org/archive/bwkfE [Accessed 8 Jun. 2025].

[4] Al Jazeera (2025). *Harrods, M&S hit by cyberattack: What happened, who's behind it?* [online] Al Jazeera. Available at: https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it [Accessed 9 Jun. 2025].

[5] Wright, R. (2025). *Scattered Spider's Ties to Russia: Closer Than We Think?* [online] Darkreading.com. Available at: https://www.darkreading.com/cyberattacks-data-breaches/blurring-lines-scattered-spider-russian-cybercrime [Accessed 9 Jun. 2025].

[6] The Economic Times (2025). *Russian anchor mocks British army after UK pledges military aid to Ukraine, here's what he said*. [online] The Economic Times. Available at: https://economictimes.indiatimes.com/news/international/uk/russian-anchor-mocks-british-army-after-uk-pledges-military-aid-to-ukraine-heres-what-he-said/articleshow/118690015.cms?from=mdr [Accessed 9 Jun. 2025].

towards the UK and its military strength, however the Russian embassy has since stated that it "poses no threat to the United Kingdom and its people."[7] While the retail sector is not inherently one of the recognised sectors of the national critical infrastructure, it does stand to reason - with reference to Maslow's hierarchy of needs[8] - the readily accessible retail of food and garments that M&S provides is central to national security, especially within a cyber age.

It is theorised that the attackers used a SIM (Subscriber Identity Module) Swapping technique whereby a compromised phone number (that of someone with registered internal access) is transferred to a SIM card of an attacker, allowing for a manipulation of "helpdesk procedures to reset login credentials and gain elevated access to internal systems."[9] While this is still yet to be confirmed, this method could indicate that M&S lacked the human security aspect of the 'wholesome' approach to cybersecurity.

However, some have speculated that the Indian tech giant, Tata Consultancy Services (TCS) – which was in partnership with M&S – may have inadvertently allowed a backend into M&S which then created the whole in which scattered spider spun their web[10].

This ransomware attack involved the encryption of M&S's servers and the theft of sensitive customer data, including names, email addresses, postal addresses, and dates of

[7] The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland (2025). 'RUSSIA HAS NO PLANS TO ATTACK BRITAIN'. [online] X (formerly Twitter). Available at: https://x.com/RussianEmbassy/status/1929885787744809206 [Accessed 9 Jun. 2025].

[8] McLeod, S. (2025). Maslow's Hierarchy of Needs. [online] Simply Psychology. Available at: https://www.simplypsychology.org/maslow.html [Accessed 9 Jun. 2025].

[9] PureCyber (2025). *SIM-swap fraud*. [online] PureCyber. Available at: https://purecyber.com/news-1/retail-sim-swap-fraud [Accessed 9 Jun. 2025].

[10] Consultancy.uk (2025). *M&S hackers may have gained access via IT partner TCS*. [online] Consultancy.uk. Available at: https://www.consultancy.uk/news/40295/ms-hackers-may-have-gained-access-via-it-partner-tcs [Accessed 9 Jun. 2025].

birth[11]. This data breach, coupled with the prolonged disruption to online ordering and hiring, underscores the severe consequences of cyber-attacks on retail infrastructure.

Identification of Assets:

For a retailer, that operates on the scale of M&S, their assets (especially those at risk of cyber-attacks) would include Customer data systems (which includes databases that host information regarding the consumers personal information), Operational infrastructure (such as online order system and the loyalty programme known as 'Sparks'[12]), and the physical counterparts (such as their extensive network of physical stores, warehouses, and the valuable stock held within them) Each of these asset types have associate risks, as discussed below.

Identification of Risks:

Risk factors that major retailers such as M&S may face within the cyber domain are highly multi-faceted. For example, Risks to operational infrastructure – such as the Sparks reward programme – will have effects on other risk sectors. Consumer data systems are highly intertwined with the operational infrastructure, which is showcased by the 2025 ransomware attack which led to the compromission of said data[13] and the suspension of the online order system[14].

Consumer Data Systems:

[11] Tidy, J. (2025). M&S hackers sent abuse and ransom demand directly to CEO. *BBC News*. [online] 6 Jun. Available at: https://www.bbc.co.uk/news/articles/cr58pqjlnjlo [Accessed 9 Jun. 2025].

[12] M&S (2023). *Welcome to Sparks and rewards you'll love*. [online] www.marksandspencer.com. Available at: https://www.marksandspencer.com/mysparks/about [Accessed 9 Jun. 2025].

[13] BBC News (2025). Marks & Spencer says customer data stolen in cyber attack | BBC News. [online] YouTube. Available at: https://www.youtube.com/watch?v=VVDBmBsp-rc [Accessed 9 Jun. 2025].

[14] M&S (2025). *Shopping in-store & online*. [online] Marksandspencer.com. Available at: https://www.marksandspencer.com/help-and-support/shopping-in-store-and-online [Accessed 9 Jun. 2025].

- Data Theft: The exfiltration of customer Personally Identifiable Information (PII) presents long-term consequences, including identity theft, phishing exploitation, and data resale on dark web markets.
- Regulatory Risks: Under GDPR and UK Data Protection regulations, M&S could face steep penalties and fines, mandatory reporting obligations, and class-action lawsuits[15] from affected customers.

Operational Digital Infrastructure:

- Disruption and suspension of services: The ransomware attack encrypted core systems, halting online orders and Sparks loyalty functions. This led to service outages, financial losses nearing £300 million, and a backlog of customer fulfilment.[16]

Physical Assets and Infrastructure:

- Supply chain vulnerabilities: Cyber-attacks on operational systems can lead to disruption of logistics, affecting warehouse operations and stock management.
- Site Vulnerabilities: Risks associated with physical access to the network.

Classification of Risk:

This risk assessment classifies the risks under the following metric:

- **Customer Data Systems** – High Risk

[15] Price, C. (2025). M&S faces 'unprecedented' Scottish lawsuit over cyber attack data breach - Tech Digest. [online] Tech Digest. Available at: https://www.techdigest.tv/2025/06/ms-faces-unprecedented-scottish-lawsuit-over-cyber-attack-data-breach.html [Accessed 9 Jun. 2025].

[16] Butler, S. (2025b). *M&S expects cyber-attack to last into July and cost £300m in lost profits*. [online] the Guardian. Available at: https://www.theguardian.com/business/2025/may/21/cyber-attack-cost-marks-and-spencer-lost-sales-company-results-reveal [Accessed 9 Jun. 2025].

The breach of customer PII affects millions, with serious consequences: identity theft, phishing campaigns, legal fines, and reputational damage.

- **Operational Infrastructure** – High Risk

Disruption to retail operations had immediate financial impact and undermined customer confidence.

- **Physical Assets and Infrastructure** – Medium/High Risk

The contractor's compromised account shows a significant threat vector for future breaches via vendor/supply-chain weaknesses. Access to internal systems to initiate such an attack indicates structural weakness within M&S's digital systems.

Asset Risk Analysis

As stated above, this assessment has categorised the major assets of M&S into three main sections: Customer Data Systems, Operational Infrastructure and Physical Assets and Infrastructure. This qualitative risk assessment employs the following scales to evaluate the potential for, and ramifications of cyber threats faced by Marks & Spencer Plc. The Likelihood Scale ranges from Very Rare to Very Likley, while the Impact Scale ranges from Insignificant (negligible consequences) to Catastrophic (existential and/or immediate threat)

Asset: Customer Data Systems | Risk: Data Breach/Theft

The likelihood of a data breach affecting M&S's Customer Data Systems is high. Large retailers like M&S are attractive targets due to the vast amount of Personally Identifiable Information (PII) they store. The April 2025 breach confirmed this risk, with the DragonForce ransomware group claiming responsibility for stealing millions of customer records, including names, addresses, dates of birth, and loyalty card data[17]. Heavy reliance on external partners and social engineering increases the likelihood of similar attacks across the industry.

The impact is catastrophic. Although no payment card data or passwords were accessed[18], the stolen PII opens avenues for identity theft and phishing. Financial penalties under GDPR could reach millions, alongside costs for incident response, and legal claims.

[17] Zansys ICT (2025). *M&S Data Breach 2025: Cybersecurity Lessons for UK Businesses*. [online] Zansys ICT. Available at: https://www.zansys.co.uk/ms-data-breach-2025-cybersecurity-lessons/ [Accessed 9 Jun. 2025].

[18] Ibidem [Footnote № 10 – BBC News (2025)]

Furthermore, Brand trust, a cornerstone of M&S's model, has been seriously damaged - with long-term reputational fallout and potential customer churn.

Asset: Operational Digital Infrastructure | Risk: Ransomware and Disruption

The likelihood of a ransomware attack disrupting M&S's operational infrastructure is high. The 2025 attack encrypted core IT systems, halting operations and exposing the vulnerabilities of interconnected digital ecosystems[19]. The breach again originated via third-party credential compromise, underscoring the risks of outsourced IT and the ongoing threat from ransomware-as-a-service models.

The impact ranges from major to catastrophic. Online orders were frozen, with recovery not expected until July, resulting in an estimated £300 million loss in operating profits and key business functions - including hiring and in-store services like contactless payments[20] - were being disrupted. Reports of "empty shelves" show how IT failures can cascade into severe supply chain issues, affecting both operations and customer trust, leading into our third asset category:

Asset: Physical Assets and Infrastructure | Risk: Supply Chain & Site Vulnerabilities

M&S's physical infrastructure - warehouses, stock, stores - faces a medium likelihood of disruption from indirect cyber incidents. Although not directly targeted, these assets

[19] Ibidem [Footnote № 8 – Tidy, J. (2025)]
[20] Butler, S. (2025a). *M&S apologises after 'cyber incident' hits contactless payments and online orders*. [online] the Guardian. Available at: https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders [Accessed 9 Jun. 2025].

depend heavily on IT-controlled logistics. The ransomware attack crippled digital infrastructure, indirectly impacting supply chains and store operations.

The impact is moderate to major. The knock-on effects of digital compromise - while not existential, sustained disruption damage's reliability, frustrates customers, and incurs high recovery costs. It contributes meaningfully to brand degradation, especially when combined with digital chaos. The 'write off' of perishable stock is also a notable impact of the incident, as much of the planned stock throughout this period may have been held back and not sold.

Risk Appetite:

It is the conclusion of this assessment that M&S's risk appetite was in favour of taking risks when, and only when, they appeared necessary for the continuation of business and the increase in profits. That being said – the use of third-party access (via TCS) or internal helpdesk controls, potentially prioritising efficiency over rigorous access validation, was not a strategically viable move in hindsight. Ideally, M&S should have adopted a risk mitigation strategy for such high-value systems - focusing on zero-trust protocols, social engineering countermeasures, and stricter third-party oversight - given their exposure to reputational and regulatory consequences. This implies that M&S's risk appetite may have been higher than it should have been, which resulted in the cyber incident reach an extent much further than theorised in procedural plans.

Continuous Monitoring

The 2025 M&S cyber incident stands as a testimony to remind us that cybersecurity is never a one-time patch that fixes all that ails, but rather a continuous approach to evolving times, full of perpetual and continuous monitoring and vigilance. To prevent similar incidents and enhance resilience, this assessment recommends a course of continual and holistic strategy building, particularly in the prevention of access points and the building of resilience and recover plans. If M&S were to follow the United States' National Institute of Standards and Technology (NIST)'s Security Framework to build such a strategy, one could foresee a potentially more secure foundation.

The NIST framework is split into 5 key sections: Identify, Protect, Detect, Respond, and Recover – these 5 segments give the guidance on how to build a more secure foundation for businesses and organisations[21]. There is evidence to suggest. That M&S have implemented, at least in part, the NIST framework into their internal policies – as outlined in the "Group Risk Management Policy"[22]

For M&S, the 'Identify' function emphasises continuously understanding and managing cybersecurity risks to its systems, assets, data, and capabilities. This includes regularly updating its inventory of digital assets, including all customer data systems, operational infrastructure, and the interconnected third-party systems like TCS. Ongoing risk

[21] NIST (2024). *Cybersecurity Framework*. [online] National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework [Accessed 9 Jun. 2025].

[22] M&S (2019). *GROUP RISK MANAGEMENT POLICY*. [online] *M&S*. Available at: https://corporate.marksandspencer.com/sites/marksandspencer/files/marks-spencer/policies/risk-management-policy-new.pdf [Accessed 9 Jun. 2025].

assessments are crucial, not just initial ones, to continually analyse emerging threats (like new ransomware variants or social engineering tactics) and evaluate their potential impact on M&S's specific environment. By thoroughly understanding its digital ecosystem and potential vulnerabilities, M&S can prioritise its security investments effectively.

'Protecting' all the assets and systems identified is one of the most crucial steps in cyber-security. M&S must develop and implement appropriate safeguards to ensure the continued delivery of their critical services. This includes developing a culture of security awareness with training to spot and report preventable social-based cyber-attacks (such as phishing attempts), creating a "human firewall"[23] of best practises. Historically, M&S has been viewed as an early adopter of physical security measures in the retail sector, including restrictions on personal devices in areas handling sensitive data[24] – a return to this security first approach may be beneficial for the continuation of M&S in the cyber age.

On the other hand, 'Detection' involves continuously monitoring for anomalies and incidents within their extensive digital ecosystem. This necessitates the deployment of robust Security Information and Event Management (SIEM) systems to aggregate and analyse logs from all critical systems, including customer databases and operational infrastructure. Furthermore, Intrusion Detection/Prevention Systems (IDS/IPS) should be active across the network to identify malicious activities, while regular vulnerability scanning and penetration testing proactively seek out weaknesses. Integrating real-time threat intelligence feeds specific to retail and ransomware trends would enable M&S to anticipate and rapidly identify emerging threats, significantly reducing the dwell time of attackers within their systems.

[23] KPMG (2023). *Human firewalling*. [online] kpmg.com. Available at: https://kpmg.com/us/en/articles/2023/human-firewalling.html [Accessed 9 Jun. 2025].

[24] Hyslop, M. (2025). National Security in a Cyber-Age.

Once an incident is detected, M&S's "Respond" capabilities are crucial to minimising damage. Like with any accident or threat, a well-defined and regularly practiced Incident Response Plan is paramount, outlining clear roles and responsibilities, and procedures and protocols. For an attack like the 2025 ransomware incident, this would involve immediate isolation of affected servers and networks to prevent further encryption or data exfiltration. Communication protocols must be established for timely internal stakeholders, legal counsel, and regulatory bodies (e.g., ICO for data breaches), alongside transparent customer communication to manage reputational impact. A dedicated and skilled incident response team, whether internal or external, is essential for effective execution.

Finally, the "Recover" function focuses on restoring M&S's capabilities and services impaired by a cybersecurity incident. Central to this is a comprehensive data backup and recovery strategy, ensuring that critical customer data systems and operational infrastructure are regularly backed up to secure, isolated locations and tested for integrity. This allows for rapid restoration of services following encryption or data loss. At the time of which this risk assessment is written, M&S will be in the ‘Response & Recover’ phase, thus a later look into their post-incident analysis will be crucial to identifying root causes and implement lessons learned, strengthening future resilience planning

Conclusion

This risk assessment concludes with the following sentiments: One) When all else failed - M&S responded in a respectable manner given the threat received. Two) As this is an ongoing situation, it is best to keep researching into information as it comes. Three) To further the security of the assets mentioned (Customer Data Systems, Operational, and Physical Assets and Infrastructure) M&S should further adapt their current strategic plan with relevant lessons learnt, and continue to engage with agencies such as the National Cyber Security Centre (UK's NCSC) and the National Institute of Standards and Technology (U.S.A's NIST) with special regards to their framework programme.

Reference List.

Al Jazeera (2025). *Harrods, M&S hit by cyberattack: What happened, who's behind it?* [online] Al Jazeera. Available at: https://www.aljazeera.com/news/2025/5/2/harrods-ms-hit-by-cyberattack-what-happened-whos-behind-it [Accessed 9 Jun. 2025].

BBC News (2025). *Marks & Spencer says customer data stolen in cyber attack | BBC News*. [online] YouTube. Available at: https://www.youtube.com/watch?v=VVDBmBsp-rc [Accessed 9 Jun. 2025].

Butler, S. (2025a). *M&S apologises after 'cyber incident' hits contactless payments and online orders*. [online] the Guardian. Available at: https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders [Accessed 9 Jun. 2025].

Butler, S. (2025b). *M&S expects cyber-attack to last into July and cost £300m in lost profits*. [online] the Guardian. Available at: https://www.theguardian.com/business/2025/may/21/cyber-attack-cost-marks-and-spencer-lost-sales-company-results-reveal [Accessed 9 Jun. 2025].

Consultancy.uk (2025). *M&S hackers may have gained access via IT partner TCS*. [online] Consultancy.uk. Available at: https://www.consultancy.uk/news/40295/ms-hackers-may-have-gained-access-via-it-partner-tcs [Accessed 9 Jun. 2025].

Ford, N. (2025). *The Co-Op, M&S, Harrods… You? Mitigating the Risk of Ransomware - IT Governance Blog*. [online] IT Governance Blog. Available at: https://www.itgovernance.co.uk/blog/the-co-op-ms-harrods-you-mitigating-the-risk-of-ransomware [Accessed 9 Jun. 2025].

Hyslop, M. (2025). *National Security in a Cyber-Age*.

KPMG (2023). *Human firewalling*. [online] kpmg.com. Available at: https://kpmg.com/us/en/articles/2023/human-firewalling.html [Accessed 9 Jun. 2025].

M&S (2019). *GROUP RISK MANAGEMENT POLICY*. [online] *M&S*. Available at: https://corporate.marksandspencer.com/sites/marksandspencer/files/marks-spencer/policies/risk-management-policy-new.pdf [Accessed 9 Jun. 2025].

M&S (2023). *Welcome to Sparks and rewards you'll love*. [online] www.marksandspencer.com. Available at: https://www.marksandspencer.com/mysparks/about [Accessed 9 Jun. 2025].

M&S (2025). *Shopping in-store & online*. [online] Marksandspencer.com. Available at: https://www.marksandspencer.com/help-and-support/shopping-in-store-and-online [Accessed 9 Jun. 2025].

Marks & Spencer (2025). *Our History*. [online] Marks & Spencer. Available at: https://corporate.marksandspencer.com/about-us/our-history [Accessed 9 Jun. 2025].

McLeod, S. (2025). *Maslow's Hierarchy of Needs*. [online] Simply Psychology. Available at: https://www.simplypsychology.org/maslow.html [Accessed 9 Jun. 2025].

NIST (2024). *Cybersecurity Framework*. [online] National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework [Accessed 9 Jun. 2025].

Price, C. (2025). *M&S faces 'unprecedented' Scottish lawsuit over cyber attack data breach - Tech Digest*. [online] Tech Digest. Available at: https://www.techdigest.tv/2025/06/ms-faces-unprecedented-scottish-lawsuit-over-cyber-attack-data-breach.html [Accessed 9 Jun. 2025].

PureCyber (2025). *SIM-swap fraud*. [online] PureCyber. Available at: https://purecyber.com/news-1/retail-sim-swap-fraud [Accessed 9 Jun. 2025].

The Economic Times (2025). *Russian anchor mocks British army after UK pledges military aid to Ukraine, here's what he said*. [online] The Economic Times. Available at: https://economictimes.indiatimes.com/news/international/uk/russian-anchor-mocks-british-army-after-uk-pledges-military-aid-to-ukraine-heres-what-he-said/articleshow/118690015.cms?from=mdr [Accessed 9 Jun. 2025].

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland (2025). *'RUSSIA HAS NO PLANS TO ATTACK BRITAIN'*. [online] X (formerly Twitter). Available at: https://x.com/RussianEmbassy/status/1929885787744809206 [Accessed 9 Jun. 2025].

The Telegraph (2008). *Marks & Spencer: A recent history | Ghostarchive*. [online] Ghostarchive.org. Available at: https://ghostarchive.org/archive/bwkfE [Accessed 8 Jun. 2025].

Tidy, J. (2025). M&S hackers sent abuse and ransom demand directly to CEO. *BBC News*. [online] 6 Jun. Available at: https://www.bbc.co.uk/news/articles/cr58pqjlnjlo [Accessed 9 Jun. 2025].

Wright, R. (2025). *Scattered Spider's Ties to Russia: Closer Than We Think?* [online] Darkreading.com. Available at: https://www.darkreading.com/cyberattacks-data-breaches/blurring-lines-scattered-spider-russian-cybercrime [Accessed 9 Jun. 2025].

Zansys ICT (2025). *M&S Data Breach 2025: Cybersecurity Lessons for UK Businesses*. [online] Zansys ICT. Available at: https://www.zansys.co.uk/ms-data-breach-2025-cybersecurity-lessons/ [Accessed 9 Jun. 2025].