Marks & Spencer (M&S) Cybersecurity Incident – April 2025

By: Tyler Royster

The major cybersecurity breach at Marks & Spencer (M&S) during April 2025 impacted three critical services, including the Click and Collect platform, along with payment processing systems and gift card redemption functionality. The incident at M&S highlights the rising cyber risks that organizations experience when operating in digital-first environments, particularly those businesses that operate extensive customer networks combining digital and physical systems. The broad retail network and established global brand of M&S create a prime target environment for cybercriminals who search for digital system vulnerabilities.

M&S operates more than 1,400 stores across over 60 nations, with its workforce totaling around 64,000 employees. The company delivers services to millions of consumers who interact through both physical stores and its expanding digital platform. A disruption to these services produces wide-reaching consequences that impact both operational operations and customer base as well as business partners and the economy as a whole. A critical study emerges from this incident because it demonstrates how established organizations remain exposed to advanced cyber threats that exist in modern digitally connected environments.

The company made its breach announcement in April 2025 while disclosing that various essential systems at the firm experienced cyber attacks. The first clear consequence of the data breach was the service outage of M&S's Click and Collect service, because it is a core service for the company. The service enables online purchases for in-store collection by customers at their convenience. The system has gained popularity because of its user-friendly interface and increased consumer interest in pick-up options rather than home delivery. Customers encountered major delays during order processing because of the cyberattack, and numerous problems arose from the inability to retrieve their items. Customers faced

additional complications when the system failed to deliver email notifications, which made the process even more complicated.

The data breach compromised two essential services operated by M&S: the Click and Collect system, together with payment processing functions. Several contactless card users encountered transaction rejections when they attempted payments at checkout points. The service outage prevented numerous customers from finishing their purchases while generating both revenue losses and extensive consumer anger. Gift card customers experienced system non-functionality because they were barred from using their gift cards and vouchers at stores while the breach remained active. The disruption caused by this issue presents a major operational challenge to M&S since gift cards function as one of its most common payment methods.

M&S established that its physical stores operated without interruption during the data breach despite the widespread impact on core digital services. The disruption seemed to affect only the digital platforms and online operations. The company's website together with its mobile application operated normally yet the systems faced possible minor performance delays because of the general strain on internal infrastructure.

M&S rapidly summoned cybersecurity experts both internally and externally to evaluate the situation while securing their systems following the attack. The company officially apologized to its affected customers while M&S assured its customer base that the company took immediate action to resolve the situation and prevent additional harm. M&S disclosed the breach to the National Cyber Security Centre (NCSC), which manages UK cybersecurity issues, along with the Information Commissioner's Office (ICO), which enforces data protection regulations in the country. M&S demonstrates its commitment to transparency through disclosure, which maintains continuous communication with both customers and regulators during the resolution process. M&S omitted revealing the nature of the cyberattack but security professionals theorize the attack could stem from phishing

attacks or ransomware or DoS/DDoS events. All three attack types have previously been used against large organizations operating complex digital systems such as M&S.

Phishing attacks represent a probable source of the breach. Attackers create deceitful emails that deceive recipients into believing they originate from trustworthy sources, including suppliers and business partners, and internal colleagues. The deceptive communications through emails include damaging content that allows hackers to extract important details like passwords or distribute malware to target computers. The attackers could have utilized spear-phishing techniques against M&S to compromise employee accounts, which would enable them to shut down essential business functions, including Click and Collect and payment operations.

Phishing attacks are dangerous because they exploit the inherent trust in email communications. Attackers apply social engineering techniques to create authentic-looking emails, which enhances victim vulnerability to phishing scams. A phishing assault against staff members who control essential organizational systems would provide sufficient explanation for how cybercriminals disabled major M&S services.

The breach might have occurred due to a ransomware attack. A ransomware attack involves attackers using malicious software to lock files so that authorized users cannot access them. Attackers typically request ransom payments through cryptocurrency while offering decryption of files and system access in return. Modern ransomware attacks continue to rise in both complexity and occurrence rates while specifically targeting organizations maintaining intricate digital networks like M&S.

The service disruptions at M&S might result from a ransomware breach. The attackers would have either encrypted essential company data or prevented users from accessing their orders and payment processing, as well as gift card functionality. The company would need to assess the monetary and reputational expenses of ransom payment against the expected customer distrust consequences. The company remains cautious about revealing complete details about the attack, partly because it needed to

safeguard sensitive customer data from potential leaks. The company's need to adhere to GDPR data protection regulations and other regulatory requirements affected its approach to handling the data breach.

A DDoS or DoS attack represents the third possible explanation for the breach. A DDoS attack occurs when cybercriminals direct an excessive amount of traffic toward a company's servers, which results in system slowdowns and total system unavailability. Online services operated by M&S, such as Click and Collect and payment processing, became unavailable because of targeted attacks, which disrupted these services and prevented customers from accessing them. Service disruptions from this attack type primarily affect digital transaction-dependent businesses since it does not lead to data theft but causes service unavailability.

Attackers could have disrupted M&S's online services hosted on external servers or cloud platforms by overwhelming these platforms which caused critical functions to fail and order processing to halt. The servers that manage financial transactions became inoperable which would explain why M&S experienced payment system failures.

The evaluation of the breach's impact and its associated security risks heavily depends on understanding the technological systems M&S operates. M&S uses cloud-based infrastructure as its main digital service foundation, similar to most contemporary retailers. Through this system, M&S handles large datasets while providing efficient order management capabilities. Cloud services establish centralized points that become targets for potential attacks. The attackers could have obtained control of customer orders and payment details, and other sensitive data when they compromised M&S's cloud environment, which resulted in major disruptions of service delivery.

The company's payment processing systems based on EMV (Europay, MasterCard, and Visa) and NFC (Near Field Communication) for contactless payments were also affected by the breach. The systems were designed to protect customer financial information in transactions but if the system was

compromised the attackers could have caused major transaction failures so customers would not be able to make purchases or get their money from their gift cards.

Furthermore, identity and access management systems are crucial for ensuring that only authorized personnel can access business-critical systems. If these systems were breached, then attackers could have gained access to internal systems and be able to shut down services or steal sensitive information. Security measures like multi-factor authentication (MFA) and encryption are usually put in place to prevent unauthorized access, but if these safeguards were circumvented, the consequences could have been serious.

The M&S cyber attack not only impacted the company's operations but also had a huge impact on society and the economy. As more and more people rely on digital services for shopping the daily business, such kind of disruptions make the customers lose trust in the brand. In today's world, where everything is about convenience, speed, and security, service failure can be detrimental to a company's brand. The customers who were unable to get their orders or make transactions may have decided to shift to other companies that offer better services.

On a larger scale, the impact of the breach is not limited to the company itself. When a major retailer such as M&S faces system disruptions, the impact can be felt by partners, suppliers, and logistics providers in the supply chain. For M&S, the incident would have involved considerable costs for incident response, forensic analysis, system recovery, and potential fines from regulatory bodies such as the ICO for failing to meet cybersecurity standards or for failing to protect customer data properly.

The cyber attack on Marks & Spencer is a clear example of the dangers that companies face in the digital world. As digital services are now a must for every business, cybersecurity measures have become more important than ever. The M&S breach shows that even the most well-known companies are at risk of cyber threats and how these threats can affect not only the company but also its customers, partners, and the economy at large.

M&S's response to the breach – conducting an investigation with the help of external cybersecurity experts, notifying the relevant authorities, and informing the customers – shows how important it is to act quickly and transparently in case of a cyber incident. However, the incident also shows the need to improve the cybersecurity posture of the industries to safeguard essential infrastructure, customer information, and last but not least, the trust of the public. This will require the collaboration of businesses, regulators, and cybersecurity experts to handle the changing nature of cyber threats and guarantee a secure digital future.