Anatomy of a Crisis:

Deconstructing the Marks and Spencer Cyber Attack

Databarracks

Contents

Executive summary

In April 2025, Marks and Spencer (M&S) was hit by one of the most costly and disruptive cyber attacks in UK history. The incident halted online sales for 46 days, led to a significant data breach and caused widespread disruption across stores and customer services, costing the 140-year-old business around £300 million.

The attack has been widely attributed to the Scattered Spider and DragonForce groups, with initial access gained through social engineering of a third-party provider. Reporting has linked this to IT service desk operations delivered by Tata Consultancy Services (TCS), which later stated that it found no indicators of compromise within its own systems.

The incident formed part of a wider wave of cyber attacks on UK retailers in 2025, including the Co-op and Harrods. The Cyber Monitoring Centre later assessed the M&S and Co-op incidents as a single “combined cyber event”, reflecting their close timing, the use of the same social engineering techniques and overlapping attribution to the same threat actors. It classified the event as “narrow and deep” – a Category 2 systemic incident with concentrated but significant impact.

The M&S cyber attack stands as a defining case study in modern cyber risk. Despite having invested heavily in cyber defences prior to the attack, a single successful social engineering event was enough to inflict an unprecedented operational and financial toll on the UK’s largest clothing retailer.

Drawing on publicly available sources, this report examines how the attack unfolded, the impact across the business and the road to recovery. It also sets out the key resilience lessons for organisations facing similar risks.

Timeline of events

This timeline reconstructs the key events of the M&S cyber attack from publicly available evidence, tracing the incident from initial access through to recovery.

Date	Event	Impact
17 April 2025	Initial breach of M&S systems through social engineering involving a third party.	Attackers gain access to internal systems.
19 April 2025	M&S identifies malicious activity and confirms unauthorised access to its systems.	Breach detected; escalation begins.
19 April 2025, 10pm	M&S convenes its first crisis management team meeting.	Executive-level incident response activated.
20 April 2025	M&S notifies the NCA, NCSC, FCA, ICO and Irish authorities and shares details of the attack vector with the NCSC to support wider sector alerting.	Incident escalates to national response; threat intelligence shared across sector.
21 April 2025	Customer-facing disruption begins over the Easter weekend, including failures in contactless tills and Click & Collect services across stores.	First visible signs of operational disruption across stores.
22 April 2025	M&S issues its first public statement via RNS confirming a cyber incident, and engages external cyber security experts.	Public disclosure; formal incident response underway.
23 April 2025	Hackers send a ransom demand directly to CEO Stuart Machin via a compromised employee email account, reported by the BBC to be associated with a Tata Consultancy Services employee.	Confirms progression to extortion phase and attacker presence within internal communications systems.
25 April 2025	M&S suspends online orders across UK and Ireland websites and apps. The company also takes core systems offline to contain the attack, later introducing manual processes across operations.	Immediate loss of ecommerce revenue – shutting down a channel worth approximately £3.5m per day – alongside disruption to stores, logistics and stock availability.

Timeline of events

28 April 2025	M&S market value falls sharply following disclosure, with approximately £678m wiped from valuation.	Significant shareholder impact; incident escalates financially.
30 April 2025	Co-op reports a cyber incident and implements precautionary system shutdowns.	Confirms second major UK retailer affected.
13 May 2025	M&S confirms customer personal data has been accessed.	Data breach confirmed; regulatory and reputational impact escalates.
21 May 2025	M&S website is brought back in a read-only state.	Customers can browse products but not complete purchases. Digital presence re-established.
10 June 2025	M&S resumes online orders after 46-day suspension – although not the full range of products.	Start of phased recovery of ecommerce operations – a key milestone in the recovery process.
20 June 2025	Cyber Monitoring Centre classifies M&S and Co-op incidents as a single "combined cyber event" (Category 2).	Incident recognised as systemic UK retail event.
8 July 2025	M&S leadership gives evidence to Parliament confirming the timeline and social engineering entry point; Chairman declines to comment on whether a ransom was paid.	Key details of the attack vector and response confirmed publicly.
10 July 2025	National Crime Agency arrests four individuals in connection with attacks on M&S, Co-op and Harrods: "two males aged 19, another aged 17 and a 20-year-old female..."	Law enforcement action; strengthens attribution to organised criminal group.
11 August 2025	M&S restores Click & Collect services after near four-month disruption.	Key customer channel restored - the last major system to be brought back online.
5 November 2025	M&S half-year results confirm £101.6m incident-related costs and £100m insurance recovery; recovery at advanced stage.	Financial impact crystallised; operational recovery nearing completion.

Adversaries

The attack on M&S reflects a coordinated, multi-actor intrusion model, combining social engineering and ransomware.

Early reporting from BleepingComputer attributed the breach to DragonForce ransomware affiliates using social engineering tactics associated with Scattered Spider to gain access.

This combination – identity-based intrusion followed by ransomware deployment – is now a common attack pattern.

Scattered Spider

Scattered Spider is a cyber criminal collective known for targeting large organisations through identity-based attacks, particularly via IT service desks.

CISA notes that Scattered Spider actors "typically engage in data theft for extortion and also use several ransomware variants, most recently deploying DragonForce ransomware alongside their usual tactics, techniques and procedures (TTPs)."

Rather than a single, cohesive organisation, Scattered Spider is best understood as a loose network of actors operating with shared tactics and overlapping affiliations.

The group is typically composed of native English-speaking operators with strong social engineering capability, including impersonation and identity manipulation.

Modus operandi

Scattered Spider's defining capability is social engineering at scale, with a consistent focus on IT service desks.

The typical attack path involves:

- impersonating employees using real personal and organisational data
- contacting service desks via phone (voice phishing)
- bypassing identity verification processes
- requesting password or MFA resets

Attackers are often able to accurately answer verification questions and persuade service desk staff to grant access, enabling compromise of identity platforms including Entra ID, single sign-on (SSO) and virtual desktop infrastructure (VDI) environments.

Once access is established, the group:

- pivots into SaaS platforms
- searches for credentials, network architecture and sensitive data
- enables lateral movement and prepares for extortion

This approach avoids traditional intrusion methods, with no exploitation of software vulnerability or reliance on malware at entry.

DragonForce

DragonForce is a ransomware-as-a-service operation that provides tooling and infrastructure to affiliated threat actors. Unlike Scattered Spider, which focusses on initial access, DragonForce is used to monetise intrusions through encryption and extortion.

The group emerged in 2023 and operates a commercial model, providing ransomware capabilities to affiliates in exchange for a share of any ransom payments. DragonForce offers these services in exchange for a portion of any ransoms collected.

DragonForce provides the malware, leak infrastructure and negotiation capability required to execute ransomware attacks at scale. This includes data leak sites used to publish stolen information and platforms to manage ransom demands.

In the M&S incident, DragonForce was linked to the deployment of ransomware following initial access via social engineering. Reporting confirmed direct extortion activity, including a message sent to M&S leadership containing explicit threats and directing the company to DragonForce's darknet negotiation site.

DragonForce uses a double extortion model, combining encryption of systems with exfiltration of sensitive data.

This model allows affiliates to apply pressure even where systems are restored, by threatening the release of stolen data.

Impact

The April 2025 cyber attack had a severe, enterprise-wide impact, disrupting core operations, damaging financial performance and affecting millions of customers.

Online orders were suspended for 46 days, while Click & Collect services were unavailable for nearly four months, with full restoration not achieved until August 2025. The disruption extended into the second half of the year, with M&S later confirming a continued "tail end of recovery" affecting trading over the Christmas period.

Operational

The impact on operations became clear within days. On 25 April 2025, six days after its first crisis management meeting, M&S took core systems offline to contain the threat, disrupting ecommerce, warehouse management and store operations.

This forced the business to replace automated systems with manual processes in order to stay operational.

The consequences were visible across the business, with reduced stock visibility and availability, delays in replenishment and distribution and increased waste and logistics costs, particularly in Food.

Suppliers were also affected, with Greencore, a key food supplier, reporting increasing deliveries by around 20% to maintain availability during the disruption.

Financial

The primary driver of financial impact was business interruption resulting in loss of sales, reduced profit and reduction of share price.

The disruption removed a major revenue channel. Online sales account for around one-third of Clothing and Home revenue, with annual online sales of approximately £1.27 billion, equating to £3.5 million per day.

M&S initially estimated a £300 million reduction in operating profit and later confirmed in its half-year results that performance had been significantly impacted, with adjusted profit before tax falling from £413.1 million to £184.1 million and statutory profit before tax falling to £3.4 million.

The stock market reaction was swift, with approximately £678 million wiped from M&S's market value in the days following disclosure. It took 6 months to return to the pre-attack high.

M&S's core of food and drink, clothing and fast-moving consumer goods (FMCG), are all items that are easily substitutable and replaceable. Competitors therefore immediately benefited from the disruption. Retailers including Next, Tesco and Sainsbury's all gained market share during the outage period.

The incident interrupted a strong period of performance. M&S entered the year with its highest profit in over 15 years at £870 million and £425 million on the balance sheet. This financial strength was a critical factor in absorbing the shock and sustaining recovery.

M&S filed a substantial cyber insurance claim and recovered £100 million, although this covered only part of the total financial impact.

Legal and Regulatory

On 13 May 2025, M&S confirmed that the attackers had accessed a wide range of personally identifiable information (PII), including names, addresses, contact details, dates of birth, online order histories, household information and Sparks Pay reference numbers.

While no fully usable payment card details or account passwords were compromised, the exposed data increased the risk of targeted phishing and identity theft.

M&S reported the personal data breach to the Information Commissioner's Office (ICO) in compliance with UK General Data Protection Regulation. The ICO subsequently launched an investigation to assess whether M&S and its third-party providers had implemented appropriate technical and organisational measures.

The company also faces the risk of civil litigation. Multiple UK law firms initiated group claims on behalf of affected customers, seeking compensation for financial loss, distress and increased exposure to fraud.

Reputational

M&S avoided serious reputational damage. This was due both to its position as a long-established and trusted brand and to its handling of the response – keeping stores trading, maintaining consistent communication and not overpromising on recovery timelines.

The extended service outage did, however, leave customers frustrated and resulted in short-term displacement of demand to competitors.

The most significant reputational risk arose from the data breach. It was not until 13 May that M&S confirmed that customer data had been accessed – more than three weeks after the initial disclosure of the incident. The delay drew criticism and increased customer concern, particularly around exposure to phishing and fraud.

Response

The M&S cyber attack required a sustained response across technology, operations and leadership. It became a dual-front crisis: the technical restoration of compromised systems and the operational challenge of running more than 1,000 stores with key digital systems unavailable.

Initial response and containment

Once unauthorised access was identified on 19 April, M&S escalated rapidly. A crisis management team was convened the same evening, and law enforcement, regulators and the NCSC were notified within 24 hours.

The company took decisive action to contain the threat. Core systems were taken offline, including ecommerce and elements of store and logistics infrastructure. M&S consistently framed these as proactive, defensive decisions taken to protect customers and the wider business. This limited further spread but came at significant operational cost.

External cyber security specialists were engaged to support investigation, containment and recovery. M&S also shared details of the attack vector with the NCSC to support wider sector alerting.

This highlights a key trade-off in ransomware response: containment reduces risk but can amplify immediate business disruption.

Crisis management under pressure

The incident quickly escalated beyond an IT issue into a full business crisis.

Operational teams were forced to revert to manual processes to maintain continuity. Leadership managed simultaneous pressures across customers, suppliers, regulators and investors, while technical teams worked to contain and understand the attack.

The intensity of the response was significant and senior leadership described the experience as “traumatic”, with technology teams working extended hours over a sustained period.

M&S also faced a complex decision environment, including how to handle contact from the threat actor, how to communicate with customers and when to restore systems safely.

Crisis communications

M&S implemented a multi-channel crisis communications response.

From the early stages of the incident, the company maintained communication with regulators and law enforcement, including the NCA, NCSC and ICO (from 20 April). At the same time, it provided formal updates to the market through disclosures to the London Stock Exchange, informing investors of the incident, its operational impact and subsequent data breach.

As recovery progressed, more detailed updates were incorporated into formal corporate reporting.

In parallel, M&S responded directly to customers via social media during the disruption, providing updates on service availability and addressing queries as systems were gradually restored.

Recovery

System rebuild and recovery approach

M&S did not attempt a rapid restoration of systems. Instead, it adopted a controlled rebuild strategy.

Each system had to be verified as clean before being brought back online, with no residual malware or attacker persistence remaining, significantly increasing the complexity of recovery.

More than 600 applications and thousands of servers were reset and restored, with a focus on security and long-term integrity rather than speed.

The result was a prolonged but controlled recovery timeline.

Phased restoration of services

Recovery was gradual and uneven.

A first tentative step came on 21 May, when Marksandspencer.com returned in a read-only format. Customers could browse products, but not complete purchases. This re-established a digital presence while transaction and fulfilment systems continued to be rebuilt.

Online orders resumed after 46 days, initially with a limited product range. Click & Collect, a key customer channel, was not fully restored until August, nearly four months after suspension.

Other systems, including stock management and customer-facing services, continued to experience disruption into the second half of the year.

This reflects the complexity of restoring interconnected retail systems, where dependencies across ecommerce, supply chain and stores must be re-established carefully.

Recovery as transformation

This was one of the most complex and high-stakes operational challenges in M&S's modern history. It also became a catalyst for change.

M&S used the incident to accelerate its technology transformation. In its full year results, the company confirmed it would bring forward investment in infrastructure, networks and supply chain systems. The objective was to reduce system interdependency, simplify architecture and improve resilience.

This reflects a shift from recovery to redesign. Rather than restoring systems to their previous state, M&S used the disruption to address structural weaknesses exposed by the attack.

Key resilience lessons

With cyber attacks growing in frequency and impact, the question is no longer whether an attack will happen, but how well the organisation can contain it, continue operating and recover.

All organisations must assume they are targets and design for resilience – not just prevention.

Cyber resilience is now a fundamental part of business resilience.

Imperative 1: Treat cyber insurance as a core part of your resilience strategy

The M&S incident highlights the role of cyber insurance in absorbing financial impact. The company recovered around £100 million through insurance, offsetting a significant portion of direct incident costs.

Organisations should:

- Ensure cover includes business interruption and recovery costs
- Understand policy terms, exclusions and response conditions
- Align insurance with incident response plans and approved suppliers
- Review coverage regularly as risk and dependencies change

The Databarracks Data Health Check shows cyber insurance uptake continues to rise, increasing from 52% in 2022 to 73% in 2025, with around 4 in 5 large organisations now covered.

Imperative 2: Make identity the primary security boundary

In the M&S attack, the attackers did not breach a technical perimeter. They walked in "through the front door" using legitimate credentials.

Identity is the primary control point.

Organisations must:

- Enforce strong authentication across all access points, including resets
- Apply least privilege consistently across all users
- Continuously monitor for abnormal access and privilege escalation
- Adopt phishing-resistant MFA (e.g. FIDO2 keys or passkeys), particularly for privileged and third-party access

Imperative 3: Secure service desk processes

Service desks are a primary attack vector.

Phishing and impersonation remain the most common attack methods, and service desks are specifically targeted because of the pressure to resolve issues quickly.

Controls should include:

- Mandatory MFA for all credential resets
- Strict limits on help desk privileges, particularly for admin and executive accounts
- Non-bypassable verification workflows, with clear escalation paths for high-risk requests
- Full logging and monitoring of all reset and authentication activity

Social engineering awareness is critical. Service desks are under pressure to be helpful and fast, and threat actors know how to exploit this.

Build processes to prevent your service desk staff from being able to be pressured or manipulated. Security must take precedence over speed.

Imperative 4: Prioritise third-party resilience

Third-party risk has been a blind spot for too long. It cannot be managed through questionnaires alone. Organisations must move to continuous assurance, including deeper audits of supplier controls, identity processes and human vulnerabilities.

Access must be tightly controlled and monitored.

Organisations should:

- Maintain full visibility of third-party access
- Apply the same controls as internal users
- Define clear accountability in contracts, including breach notification requirements
- Exercise incident scenarios with key suppliers

Supplier resilience is part of an organisation's own resilience.

Imperative 5: Test, exercise and continuously improve

Plans must be proven in practice. Training and exercising should be structured, frequent and realistic. Intervals between exercises should be no longer than six months, as response capability degrades quickly when not practised.

Organisations should:

- Test both technical response and leadership decision-making
- Include realistic social engineering and deepfake attack scenarios
- Run regular wargaming exercises, including ransomware scenarios
- Validate crisis communications under pressure
- Conduct post-incident analysis to identify gaps and stop procedural drift

Imperative 6: Integrate cyber recovery with business continuity

Organisations must plan for scenarios where core systems are unavailable for an extended period. Cyber recovery cannot sit separately from business continuity. Every part of the business must be able to continue operating in some form. Continuity planning must move beyond documentation to practical, rehearsed capability that links cyber response, operational processes and leadership decision-making.

Organisations should:

- Define minimum viable operations across critical functions
- Build the ability to operate in a "degraded state"
- Establish fallback procedures for manual operations
- Stress-test business continuity against prolonged outages
- Ensure financial resilience to absorb disruption, including access to capital and insurance

The objective is to continue operating, even when systems are compromised.

Imperative 7: Design for containment through segmentation

Assume attackers will gain access and design systems to limit the blast radius.

Network segmentation should isolate critical services such as ecommerce, payments and store operations. This prevents lateral movement and reduces operational impact.

The contrast between M&S and Co-op is clear. Both organisations were targeted using similar social engineering techniques. However, Co-op experienced significantly less operational disruption, as its more heavily segmented architecture allowed it to contain the attack within a limited part of its estate. Core retail operations and online services continued to function at Co-op, while M&S was forced to take systems offline across the business.

Containment is what separates an incident from a crisis.

Sources

This analysis is based exclusively on publicly available information, including company announcements, financial reports, regulatory disclosures and credible third-party reporting. No non-public or privileged information has been used.

M&S Annual report 2025, M&S Full Year Results 2025, M&S Half-Year Results 2025, London Stock Exchange RNS announcements (April–May 2025), UK Parliament Business and Trade Committee evidence (Marks and Spencer and Co-op), National Crime Agency, National Cyber Security Centre, Cyber Monitoring Centre, Reuters, BBC News, Financial Times, The Guardian, IT Pro, TechRadar Pro, Infosecurity Magazine, BleepingComputer

Databarracks
1 Bridges Court
London, SW11 3BB

0800 033 6633
contact@databarracks.com
www.databarracks.com

Databarracks

Databarracks