TASK 5

RECENT MALWAR INCIDENTS AND THE PRECAUTIONARY MEASURES TAKEN

1. MARKS & SPENCER RANSOMWARE ATTACK (APRIL 2025)

INCIDENT DETAILS:

The DragonForce group, using Scattered Spider–style techniques such as social engineering, Multi-Factor Authentication (MFA) fatigue, and identity abuse, gained access to Mark & Spencer (USA) systems and deployed ransomware. This disrupted online orders, contactless payments, and click-and-collect services, and exposed customer data.

MITIGATION METHODS TAKEN:

- Services were restored in phases from June to August 2025.
- M&S worked with national agencies, notified customers, and strengthened authentication and identity controls.
- Several suspects linked to the attack were arrested.

2. MALWARE BREACH AT SK TELECOM(SOUTH KOREA) (APRIL 2025)

INCIDENT DETAILS:

Malware infiltrated SK Telecom’s Home Subscriber Server (HSS), allowing attackers to access Universal Subscriber Identity Module (USIM) authentication data (IMSI, MSISDN, and encryption keys). This raised risks of SIM-swap fraud and impersonation of subscribers.

MITIGATION METHODS TAKEN:

- SK Telecom reported the incident to authorities and implemented stronger controls over SIM-swap processes.

- Added extra protections to customer accounts while forensic investigations continued.

3. LOUIS VUITTON DATA EXFILTRATION (JULY 2025)

INCIDENT DETAILS:

Hackers, reportedly linked to the ShinyHunters group, gained unauthorized access to Louis Vuitton systems and exfiltrated global customer data such as personal details and purchase history (though not payment card data). The stolen data was intended for extortion.

MITIGATION METHODS TAKEN:

- The company notified affected customers in multiple countries and assured that financial data was safe.
- Contained the breach, and enhanced monitoring.
- Customers were advised to stay alert for misuse of their data.

4. KETTERING HEALTH RANSOMWARE ATTACK (MAY 2025)

INCIDENT DETAILS:

he Interlock ransomware gang infiltrated Kettering Health’s (USA) network, encrypted hospital systems, and exfiltrated sensitive data for double extortion. This forced electronic health record downtime, canceled medical procedures, and ambulance diversions.

MITIGATION METHODS TAKEN:

- The hospital system restored its HER(Electronic Health Record) in stages, engaged law enforcement, and reinforced system security.
- Public updates and patient notifications were issued, and indications suggest ransom was not paid.