1. **What kind of attack has happened and why do you think so?**

   This attack appears to be a spear phishing attack that is combined with malware deployment. The initial attack involved phishing emails that tricked employees into clicking a link that led to a fake company portal. The goal of the fake company portal was to harvest user credentials (usernames and passwords). Due to the numerous phishing emails received by the Risk Department, the attack appears to specifically target the department. The Risk Department likely has access to sensitive financial or operational data, making this a valuable target for the attackers. After stealing credentials, the phishing emails delivered malware to the victims' systems. The file-shares becoming inaccessible and Word documents not opening suggest that the malware could be ransomware or another destructive form of malware designed to halt business processes.

2. **As a cyber security analyst, what are the next steps to take? List all that apply.**

   After confirming that a phishing attack and malware deployment has occurred, the next steps involve containing the incident, investigating it thoroughly, mitigating further damage, and preventing recurrence.

   Confirming the Attack: Verify the phishing emails are malicious and identify the malware being facilitated through the emails. Identifying the users affected by the attack and investigating if any critical systems are compromised. Then determining whether sensitive data has been stolen, encrypted, or systems disrupted.

3. **How would you contain, resolve and recover from this incident? List all answers that apply.**

   Containing the Incident: Immediately isolate infected systems from the network to prevent the malware from spreading further. Block access to the phishing website through network firewalls and proxies to prevent other users from interacting with it. Reset passwords for all

affected employees and implement multi-factor authentication (MFA) if not already in place.

Investigation and Root Cause Analysis: Investigate email, web, and endpoint logs to track how the phishing emails were delivered, where they came from, and which systems were affected. Identify how the malware spread through the network and whether any lateral movement occurred. Investigate whether the attacker may have installed backdoors or persistence mechanisms to maintain long-term access to the network.

Eradication: Use antivirus, anti-malware, and endpoint detection and response (EDR) tools to scan and remove malware from infected systems. Apply patches and updates to software, applications, and systems that may have been exploited by the attacker.

Recovery: If files were encrypted or corrupted by malware, restore them from secure backups. Ensure that backups are clean and free from infection. Gradually re-enable network services and shared drives once systems are verified to be secure and free from malware. Closely monitor the network for any signs of recurring infections or continued malicious activity. Watch for abnormal behavior from systems or accounts that were previously compromised.

4. **What activities should be performed post-incident?**
   The incident response team, IT, and stakeholders should hold a review of the entire incident, including the causes, responses, and outcomes. Documenting any lessons learned and any weaknesses identified in the attack. Revising the incident response plan based on the lessons learned from the attack. Phishing awareness and cybersecurity training for employees, focusing on recognizing and avoiding suspicious emails, attachments, and links should also be conducted. Any form of endpoint detection and hardening must be administered.