**CASE STUDY**

At 10 am, the service desk of your organization begins receiving numerous calls from users reporting an inability to access templates stored on a specific file share. While troubleshooting this issue, one user contacts the service desk an hour later, reporting a concerning message displayed on their workstation screen: "Your files have been encrypted." The message demands payment in bitcoin for a decryption key, also threatening that copies of the files have been made and will be destroyed only upon further payment. The user reveals that this message had been displayed for an hour before contacting IT.

In response to the reported incident, the IT team swiftly isolates the affected workstation from the network by disabling its network interfaces. They proceed to take a forensic image of the workstation's files and export event logs and Windows Firewall logs onto a USB drive. The infected workstation is then securely placed in a designated room, while the user is relocated to another workstation to resume their tasks.

Further investigation by the IT team reveals that the ransomware has not only encrypted files on the affected workstation but has also targeted files on two file servers. Most of the encrypted files are templates, but one notable file, "Customers-2017.xlsx," seems to be an export from a previous sales system. A thorough examination of all workstations and servers confirms that no other systems have been infected.

Additionally, evidence suggests that significant data, amounting to several gigabytes, has been transmitted over HTTP to a Command & Control (C&C) server with a foreign IP address over the past week. This indicates a potential breach of the organization's network security.

Amidst this critical situation, the organization faces a pressing need to formulate an effective response plan to address the ransomware attack, mitigate its impact, and prevent future incidents.

1. Given the scenario of a ransomware attack targeting your organization's network, describe the steps you would take to prevent future incidents and enhance the organization's cybersecurity posture. Include measures to detect and mitigate ransomware threats, as well as strategies for incident response and recovery.
2. Identify the key stakeholders and outline how you would communicate with stakeholders, both internal and external, during and after the incident to ensure transparency and accountability.
3. Describe how you would collaborate with external parties, such as law enforcement agencies, cybersecurity experts, and regulatory bodies, in response to the ransomware incident. Discuss the importance of reporting the incident to relevant authorities and sharing threat intelligence to prevent similar attacks across other organizations.