Scenario: PHISHING

Details:

Finance receives an email, purportedly from a trusted vendor, asking for a review of an invoice. An employee clicks on the link, causing a malicious file to be downloaded to the Organization's network.

The file remains undetected and is used by hackers to conduct reconnaissance and password stealing for several days before the hackers become operational.

Hackers use administrative privileges to execute their attack and gain access to the building automation system, phone system, and multiple computers on the network.

Notes

- Can you identify the impacts to customers/employees if this happened?
- Which Roles would be involved in identifying, responding, and recovering from this incident?
- What are some precautions the organization can take to guard against this -- both technical and non-technical?
- Does your organization have a cyber incident response plan that identifies this type of threat and how to respond?