Incident report analysis

Summary	A ransomware attack occurred at a small U.S. healthcare clinic when an employee unknowingly opened a malicious email attachment. The phishing email, crafted by a cybercriminal group, initiated the execution of ransomware which quickly encrypted critical patient files and internal documents. The attack disrupted daily operations, locking staff out of key systems and threatening patient care continuity.
Identify	The incident was traced to a phishing email that bypassed existing email filters. The employee downloaded an attachment disguised as a billing update, which activated ransomware and encrypted files across the internal network. Endpoint detection and SIEM tools confirmed unusual encryption activity beginning at 9:00 a.m. on a Tuesday morning. Attack signatures aligned with known ransomware behavior.
Protect	To prevent similar incidents, the cybersecurity team recommended mandatory cybersecurity awareness training for all staff. Technical defenses were strengthened by improving email filtering rules, deploying multi-factor authentication, and tightening user privilege controls. Endpoint protection policies were also revised to automatically isolate devices exhibiting suspicious file encryption behavior.
Detect	An upgraded endpoint detection and response (EDR) system was configured to detect rapid file modification patterns indicative of ransomware. The SIEM was adjusted to correlate email metadata with endpoint behavior. Antivirus tools were updated with new signatures, and rules were implemented to flag

	uncommon executable file types arriving via email.
Respond	The infected device was isolated from the network immediately. IT support launched the incident response plan, performed forensic imaging of the compromised system, and reported the breach to clinic leadership. In accordance with HIPAA and local regulations, affected patients were notified. Law enforcement and a third-party cyber forensics team were engaged to investigate the origin and scope of the attack.
Recover	Patient records were restored from backups made 12 hours prior to the attack. IT staff reviewed and tested the backup recovery process to ensure it was resilient against future compromise. Plans were initiated to transition to a more frequent backup schedule and to validate the integrity of backups using automated testing protocols.

Reflections/Notes: