Portfolio Activity: Use the NIST Cybersecurity Framework to respond to a security incident

Summary	This morning, an intern reported to the IT department that she was unable to log in to her internal network account. Access logs indicate that her account has been actively accessing records in the customer database, even though she is locked out of that account. The intern stated that she received an email this morning asking her to go to an external website to log in with her internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and customer database. A couple of other employees have noticed that several customer records are either missing or contain incorrect data. It appears that not only was customer data exposed to a malicious actor, but some data was deleted or manipulated as well.

Incident report analysis

Summary	This morning, an associate reported to the IT department that she couldn’t log in to her terminal account.
Identify	• The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. • The team found that an intern’s login and password were obtained by a malicious attacker through a phishing email and used to access data from our customer database. • Initial investigation indicates that customer data was exfiltrated and potentially altered. • The attack vector was identified as phishing, and the compromised system was the intern's workstation.
Protect	• People**:** Implemented mandatory security awareness training for all employees, with a focus on phishing recognition and password hygiene.

	• Process**:** Enhanced password policies to require strong, complex passwords, enforced password rotation, and implemented account lockout policies after multiple failed login attempts. • Technology**:** Deployed multi-factor authentication (MFA) for all user accounts, installed an intrusion prevention system (IPS) to monitor network traffic for malicious activity, and implemented a firewall with advanced threat protection.
Detect	• People**:** Established an incident response team with clear roles and responsibilities. • Process**:** Developed and implemented a comprehensive incident response plan, including procedures for detection, containment, eradication, recovery, and lessons learned. • Technology**:** Deployed an intrusion detection system (IDS) to monitor network traffic for anomalies, implemented log management and analysis tools to identify suspicious activity, and configured regular vulnerability scanning.
Respond	• People**:** Activated the incident response team to contain the incident. • Process**:** Isolated compromised systems, changed passwords for affected accounts, and notified relevant stakeholders. • Technology**:** Implemented temporary access restrictions to the customer database, conducted forensic analysis of compromised systems, and collected evidence for potential legal action.
Recover	• People**:** Communicated with affected employees and customers about the incident and steps taken to mitigate risks. • Process**:** Restored compromised data from backups, conducted a post-incident review to identify lessons learned, and updated incident response plans. • Technology**:** Implemented data loss prevention (DLP) measures to protect sensitive information, enhanced system hardening, and strengthened access controls.

Reflections/Notes: