Incident report analysis

Summary	An intern reported being unable to access her internal network account. However, logs revealed her account had been used to access the customer database during her lockout. She had received a phishing email directing her to enter her credentials on an external site. This led to unauthorized access, during which customer records were viewed, altered, or deleted.
Identify	The incident response team audited systems, user activity, and access policies. They confirmed the intern's credentials were compromised and used by a malicious actor to gain database access. Preliminary analysis indicated deletion of certain customer data.
Protect	To mitigate future risks, the organization implemented: • Multi-factor authentication (MFA) • Login attempt limits (maximum of three) • Employee credential safety training • Updated firewall settings • Plans to deploy an Intrusion Prevention System (IPS)
Detect	To identify unauthorized access attempts going forward, the organization will deploy: • Firewall logging tools • An Intrusion Detection System (IDS) to monitor incoming internet traffic
Respond	The affected intern's account was disabled. Awareness training was provided to staff. Leadership was informed and will notify customers by mail, alongside

	reporting the breach to law enforcement and relevant regulatory bodies.
Recover	Customer data will be restored using the previous night's backup. Employees have been asked to re-enter any information updated or entered since that backup.

Reflections/Notes: Further review will ensure policies remain effective and future vulnerabilities are addressed pre-emptively.