Incident report analysis

Summary	This morning, an intern informed the IT department that she was unable to access her internal network account. Access logs show that her account has been actively accessing records in the customer database, even though she is locked out of the account. The intern mentioned receiving an email instructing her to visit an external website and log in with her internal network credentials to retrieve a message. We suspect that this method was used by a malicious actor to gain access to our network and customer database. Additionally, several employees have observed 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 also that some data was deleted or altered.
Identify	The incident management team conducted an audit of the systems, devices, and access policies related to the attack to pinpoint security deficiencies. During the audit, it was discovered that a malicious attacker had obtained an intern's login credentials and used them to access data from the customer database. Preliminary investigation indicates that some customer data was deleted from the database.
Protect	The team has introduced new authentication measures to deter future attacks, including multi-factor authentication, limiting login attempts to three tries, and providing training for all employees on safeguarding login credentials. Moreover, we plan to deploy a more robust firewall configuration and acquire an intrusion prevention system.
Detect	In order to identify future unauthorized access attempts, the team plans to

	utilize a firewall logging tool and an intrusion detection system to monitor incoming traffic from the internet.
Respond	The intern's network account was disabled by the team. Following this, training was conducted for both interns and employees on safeguarding login credentials in the future. Upper management was promptly notified of the incident. They will be reaching out to our customers via mail to notify them about the data breach. Additionally, management will liaise with law enforcement and other relevant organizations as per local legal requirements.
Recover	The team plans to recover the deleted data by restoring the database from the full backup taken last night. We have notified the staff that any customer information updated or entered this morning will not be included in the backup. Therefore, they will need to re-enter this information into the database once the restoration from last night's backup is complete.
