

Incident report analysis - Example

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 indicated 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 that some data was
	deleted or manipulated as well.
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 and
	used to access data from our customer database. Upon initial review, it
	appears that some customer data was deleted from the database.
Protect	The team has implemented new authentication policies to prevent future
	attacks: multi-factor authentication (MFA), login attempts limited to three
	tries, and training for all employees on how to protect login credentials.
	Additionally, we will implement a new protective firewall configuration and
	invest in an intrusion prevention system (IPS).
Detect	To detect new unauthorized access attacks in the future, the team will use a
	firewall logging tool and an intrusion detection system (IDS) to monitor all
	1

	incoming traffic from the internet.
Respond	The team disabled the intern's network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The team will recover the deleted data by restoring the database from last night's full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night's backup.