Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	This morning, one of our interns got locked out of her account, which wouldn't be weird if her account hadn't been busy accessing customer data at the same time. Turns out she clicked a phishing email and handed over her credentials on a silver platter. Not only was data exposed, but some of it was tampered with or deleted entirely.
Identify	The incident response team dug into access logs and confirmed that someone used the intern's credentials to get into the customer database. This unauthorized access left to missing and altered records. The root of the problem? A phishing scam that tricked the intern into logging into a fake portal.
Protect	To prevent a repeat performance, we rolled out multi-factor authentication (MFA) across all employee accounts, limited login attempts, and delivered a crash course on "what not to click" for all interns and staff. We're also tightening up the firewall and bringing in an intrusion prevention system (IPS) to catch threats before they spread.
Detect	We've deployed intrusion detection systems (IDS) and enhanced our firewall logging to flag weird access patterns or suspicious traffic. Anything unusual will trigger alerts to the security team, hopefully no more silent takeovers.

Respond	We immediately disabled the compromised account and kicked off a security briefing for the entire team. Management notified customers about the breach (by mail) and we're fulfilling all reporting requirements to stay compliant with state and federal regulations.
Recover	We restored the database from a clean backup taken the night before. Employees were notified that any updates made this morning need to be re-entered manually. It's tedious but it ensures the records are clean and accurate again.

Reflections/Notes: One phishing email caused a whole lot cleanup. This is exactly why layered security and regular training matter. People are the weakest link, and also the first line of defense when they know what to look for.