Homework 3: Building the Incident Response Playbook

Topic: Incident Response & Crisis Management

The Scenario

Your start-up compaby has grown. You now have real customers. But success brings attention.

The Event: On a Saturday morning at 3:00 AM, your Lead Engineer receives an alert from the SIEM: *"Unusual outbound traffic detected from the Database Server to an unknown IP address in Eastern Europe. 50GB of data transferred."*

Your Job: You are the **Incident Commander**. You need to have a plan *before* this happens. You will create the **"Break Glass" Playbook** for this specific scenario.

Part 1: The Call Tree & Roles

Task: In a crisis, you cannot be looking for phone numbers. Create a **Communication Table** defining who gets woken up and what their job is.

Role	Job Description (One sentence)	Who fills this role? (Job Title)
Incident Commander	Makes final decisions; does not touch keyboard.	CTO or VP of Engineering
Tech Lead		
Legal Counsel		
Public Relations (PR)		
Scribe		

Critical Thinking: Why is the CEO usually *not* the Incident Commander? (Explain in 1-2 sentences).

Part 2: The Response Phases

Task: Detail the specific actions your team will take during the first **4 hours** of the incident, mapped to the NIST Lifecycle.

1. Identification (Detection):

- How do you verify this isn't a false positive? (e.g., "Check if the IP belongs to a known vendor").
- What tool gives you this information?

2. Containment (Stopping the Bleeding):

- **Option A:** Shut down the database server immediately.
- **Option B:** Disconnect the network cable/virtual interface but keep the server running.
- **Decision:** Which option do you choose? **Explain why.** (Hint: Think about *RAM Forensics* vs. *Stopping Data Theft*).

3. Eradication & Recovery:

- You find a "backdoor" account named admin_backup that was created yesterday. How do you remove the threat?
- How do you know it is safe to turn the system back on for customers?

Part 3: Crisis Communication

Task: The leak is confirmed. Customer names and addresses were stolen. You must notify your customers.

Write a **150-word "Holding Statement"** to be emailed to your users.

Requirements for the Email:

1. **Be Transparent but Cautious:** Acknowledge the issue without admitting fault (legal liability).
2. **Actionable Advice:** Tell customers what *they* should do right now (e.g., Change passwords? Monitor bank accounts?).
3. **The "We Care" Factor:** Reassure them that you are taking this seriously.

Constraint: *Do not* promise "We have fixed everything" if you aren't sure yet. *Do not* speculate on who the attacker is.