Cybersecurity Case Study Worksheet

🛡 Analyzing the ArrowTrack Solutions Breach 🛡

Student Name: ____

Class/Course: ____

Case Study Scenario: ArrowTrack Solutions

A small logistics company named ArrowTrack Solutions had been doing well for years. Their operations were smooth, their employees were cooperative, and their systems had never experienced any major issues—at least none that anyone noticed.
But everything changed one Monday morning.

Employees arrived to find that several shared folders were suddenly inaccessible. Some computers displayed odd pop-ups the night before, but most people simply clicked them away and continued working. A few staff members also mentioned receiving emails that looked like they came from HR, asking them to “reconfirm” their login details for a new benefits system. Several clicked the link without thinking twice.

The network team noticed unusual outbound traffic reaching unknown IP addresses overseas. Their firewall logs were full of denied and allowed connections that no one had ever reviewed. To make things worse, the company had not applied system updates in over six months because the IT team was short-staffed, and updates often caused delays in operations, so management kept postponing them.

By noon, half the company’s files were encrypted and renamed with unfamiliar extensions. A note appeared on multiple desktops demanding payment in exchange for restoring the files. Some employees also reported that their accounts had been locked, while others had permissions they shouldn’t have—such as access to financial reports. ArrowTrack’s system administrator tried to trace where things started breaking down. They discovered an old server that had been left running in the corner of a storage room. It still had admin-level access, had never been patched, and was connected to the main network the entire time. Someone had used it as an entry point.

The company now needed to figure out what exactly went wrong, how the attack escalated so quickly, and what they had to fix to prevent this from happening again.

Identify the Threats and CIA Triad Elements

Instructions: Identify three specific threats (the cause of potential harm, e.g., an attack type) that occurred in the scenario. Then, specify which element(s) of the CIA Triad (Confidentiality, Integrity, Availability) were directly compromised by that th

No.	Threat (Specific Attack/Action)	CIA Affected
1.	____________________	____________________
2.	____________________	____________________
3.	____________________	____________________

Identify the Vulnerabilities

Instructions: A vulnerability is a weakness in the system, security procedures, or internal controls that could be exploited. List three distinct and critical vulnerabilities present at ArrowTrack Solutions.

Vulnerability 1.

____

____

____

Vulnerability 2.

____

____

____

Vulnerability 3.

____

____

____

Assess the Risks

Instructions: A risk is the potential for loss when a threat exploits a vulnerability. Match one threat (from Section I) with one vulnerability (from Section II) to form a risk pair. Rate the overall risk (Low / Medium / High) and provide a concise explanation for your rating based on the severity of the potential impact.

Risk Assessment 1

Threat + Vulnerability Pair: ______________________**Exploits** ________________________

Risk Rating: ____

Explanation: ____

____

____

____

Risk Assessment 2

Threat + Vulnerability Pair: ______________________**Exploits** ________________________

Risk Rating: ____

Explanation: ____

____

____

____

Risk Assessment 3

Threat + Vulnerability Pair: ______________________**Exploits** ________________________

Risk Rating: ____

Explanation: ____

____

____

____

Propose Fixes (Mitigation Strategies)

Instructions: Suggest three realistic and targeted solutions (fixes) that ArrowTrack Solutions should implement immediately. Explain how each fix directly addresses the problems identified in the previous sections.

Fix 1:

Proposed Fix: ____

____

How it helps (Mitigation):

____

____

____

Fix 2:

Proposed Fix: ____

____

How it helps (Mitigation):

____

____

____

Fix 3:

Proposed Fix: ____

____

How it helps (Mitigation

____

____

____