You are a security officer working for a medium-sized research company. You have been assigned to guard the facility. Two incidents occur. The first, a well-known manager walks out with a box of papers. The second, someone believed to be an outsider assesses the company information and goes away with the company blueprints for the next generation product.
Briefly list all security gaps, vulnerabilities, threats, risks, and exploits.
Describe how these incidents can be overcome.

CASE- I

In the first case, the manager walks out with a box of papers. It is the case of He could have taken the company's confidential information/data with him. This is a huge security risk which can expose the sensitive information belonging to the company to potential attackers, hackers and competitors. There is also the increased risk of huge monetary losses since the manager can sell the data to competitor's of the organization which will directly affect the customer's base of the company.

CASE-II

In the second case, the outsider takes the blueprint for the product which is under development. This increases the threat of compromises to the intellectual property of the company which can result in piracy of the company's valuable information. He can copy the blueprint and create a similar product which will directly affect the company's business plan. The person can even blackmail the company by threatening to sell the blueprint to other competitors in the market and demand for extortion.

To overcome these incidents, a proper high security surveillance system should be implemented in the company to prevent unauthorised access or copying of data by any outsiders. Nobody should be allowed to take the company's sensitive information/data with him outside the company's premises unless authorized by a senior official of the company. A security check could be monitored at the entrance to prevent this. Any sensitive product information should be classified as confidential by the company and access should be restricted to outsiders. Outsiders should be checked by the security guards while entering/exiting the company and any electronic media or devices that can potentially exploit the network of the company should be handed over to the security personnel and should not be allowed inside the company premises. In the first

case the company can also terminate the employment contract between themselves and their manager. If the information the company lost is serious and the business has suffered largely by the incident then you should consider legal action against the employee or the outsider.