**Sample Incident Response Process for VietPhat Transportation Company**

#### **Incident 1: Ransomware Attack**

**Scenario:** An organization's network is infected with ransomware that encrypts critical data and demands a ransom payment for the decryption key.

1. **Detection**
   * **Identification:** The IT department receives alerts from security monitoring tools or employees report inability to access certain files.
   * **Analysis:** Confirm the presence of ransomware by examining the encrypted files, ransom note, and any malicious processes running on the network.
2. **Containment**
   * **Isolation:** Disconnect the affected systems from the network to prevent the ransomware from spreading further.
   * **Blocking:** Identify and block the ransomware's communication channels (e.g., IP addresses, domains) at the firewall level.
3. **Eradication**
   * **Malware Removal:** Use antivirus and anti-malware tools to remove the ransomware from the infected systems.
   * **Forensic Analysis:** Conduct a thorough forensic investigation to ensure all instances of the ransomware are eradicated and to identify the initial point of compromise.
4. **Recovery**
   * **Data Restoration:** Restore encrypted data from the most recent clean backups.
   * **System Rebuild:** Rebuild and reimage infected systems to ensure they are clean and secure.
   * **Monitoring:** Monitor systems for any signs of lingering malware or reinfection.
5. **Lessons Learned**
   * **Post-Incident Review:** Conduct a detailed post-incident review to identify how the ransomware entered the network and why it was able to spread.
   * **Training:** Educate employees on recognizing suspicious emails, links, and attachments that could lead to ransomware infections.
   * **Improvements:** Update security protocols, patch known vulnerabilities, and implement more robust backup and recovery procedures.

### **Incident 2: Data Breach**

#### **Scenario:** A hacker gains unauthorized access to a company's database containing sensitive customer information, including names, addresses, and payment details.

1. **Detection:**
   * Anomalous database activity is detected by security monitoring tools.
   * Security software alerts the IT department about the breach of data
2. **Containment:**
   * Immediately restrict access to the compromised database.
   * Identify and close the vulnerability used by the hacker to gain access.
3. **Eradication:**
   * Remove any malicious software or unauthorized user accounts created by the hacker.
   * Patch the vulnerability and ensure no other points of entry exist.
4. **Recovery:**
   * Notify affected customers about the breach and provide steps they can take to protect themselves.
   * Enhance security measures around sensitive data storage and access.
   * Monitor systems for any further suspicious activity.
5. **Lessons Learned:**
   * Perform a detailed analysis of the breach to understand the attack vectors.
   * Update data protection policies and implement stronger encryption and access controls.
   * Provide ongoing security training for employees and conduct regular security audits.