***Hands-On Threat Analysis: Identifying, Assessing, and Countering Cyber Threats***

### **Selected Company**

* **Company:** TechSolutions Inc.
* **Sector:** Information Technology
* **National Affiliation:** United States of America

### **Key Assets:**

1. **Customer Relationship Management (CRM) System**
2. **Employee Database**
3. **Server Infrastructure**

### **Potential Attackers and Their Motivations:**

1. **Financial Hackers**
   * **Nationality:** Various
   * **Motives:** Obtaining sensitive financial information
   * **TTPs (Tactics, Techniques, and Procedures):** Phishing, malware, ransomware
2. **Competitors (Industrial Espionage)**
   * **Nationality:** Various
   * **Motives:** Acquiring confidential information for competitive advantage
   * **TTPs:** Social engineering, network infiltration, data exfiltration
3. **Hacktivists**
   * **Nationality:** Various
   * **Motives:** Advocating political or social causes
   * **TTPs:** DDoS attacks, defacing websites, unauthorized access

### **Threat Analysis Using STRIDE Methodology:**

1. **Customer Relationship Management (CRM) System:**
   * **Spoofing:** An attacker could impersonate a legitimate user to access client data.
   * **Tampering:** Unauthorized modification of client records.
   * **Repudiation:** Denying actions performed in the system by an attacker.
   * **Information Disclosure:** Exposure of sensitive client information.
   * **Denial of Service:** Blocking access to the CRM system.
   * **Elevation of Privilege:** An attacker gains higher privileges than allowed.
2. **Employee Database:**
   * **Spoofing:** An attacker impersonates an employee to access records.
   * **Tampering:** Unauthorized changes to employee data.
   * **Repudiation:** Denying actions related to accessing or modifying records.
   * **Information Disclosure:** Leaking personal details of employees.
   * **Denial of Service:** Blocking access to the database.
   * **Elevation of Privilege:** Unauthorized escalation of privileges within the system.

### **Risk Mitigation Measures:**

1. **Customer Relationship Management (CRM) System:**
   * **Spoofing:** Implement multi-factor authentication (MFA) for users.
   * **Tampering:** Use data encryption and audit logs to detect unauthorized modifications.
   * **Repudiation:** Implement detailed audit logs for tracking user actions.
   * **Information Disclosure:** Encrypt data both in transit and at rest; enforce role-based access control.
   * **Denial of Service:** Deploy Intrusion Detection and Prevention Systems (IDS/IPS).
   * **Elevation of Privilege:** Apply the **Principle of Least Privilege** and conduct regular permission reviews.
2. **Employee Database:**
   * **Spoofing:** Implement multi-factor authentication (MFA) for database access.
   * **Tampering:** Encrypt data and maintain audit logs.
   * **Repudiation:** Use detailed audit logs to track access and modifications.
   * **Information Disclosure:** Encrypt sensitive data, enforce role-based access control, and implement strict access management.
   * **Denial of Service:** Utilize IDS/IPS for network security.
   * **Elevation of Privilege:** Regularly review permissions and enforce the **Principle of Least Privilege**.