# Cybersecurity Incident Report:

Network Security Breach

|  |
| --- |
| Step 1: Identifying Potential Security Incidents and Scenarios |
|  Monitor network traffic for unusual patterns or anomalies such as:   * Unauthorized access to network devices or systems. * Unusual outbound connections to unknown IP addresses. * Excessive bandwidth usage or data transfers. * Suspicious logins from unauthorized locations.    Common scenarios include:   * **Phishing attacks** compromising user credentials. * **Malware infections** causing network disruptions. * **DDoS attacks** overwhelming network resources. * **Unauthorized access** to sensitive systems or databases. |
|

|  |
| --- |
| Step 2: Defining Roles and Responsibilities for the Response Team |
| 1. Incident Response Lead: Oversees the entire incident response process, ensures coordination, and communicates with stakeholders. 2. Network Security Analyst: Investigates network activity and identifies the breach source, containing the breach where possible. 3. IT Infrastructure Team: Works to restore network functionality, isolates compromised systems, and deploys patches or other mitigations. 4. Communication Officer: Manages internal and external communications to keep all parties informed, including customers, partners, and regulators. 5. Legal and Compliance Team: Ensures the response aligns with regulatory obligations and advises on breach disclosure requirements. |

|  |
| --- |
| Step 3: Developing Step-by-Step Response Procedures |
|  **Detection and Analysis**:   * Monitor alerts from Intrusion Detection Systems (IDS) or logs for abnormal network behavior. * Analyze the scope and severity of the breach.    **Containment**:   * Isolate affected systems to prevent further data loss or breach propagation. * Implement network segmentation to control the spread.    **Eradication**:   * Remove malware, unauthorized accounts, or rogue services from the affected systems. * Patch vulnerabilities or misconfigurations that allowed the breach.    **Recovery**:   * Restore network services and data from backups. * Monitor the network for lingering threats or reinfection after recovery.    **Post-Incident Review**:   * Conduct a post-incident analysis to assess the breach's root cause, evaluate the response, and implement changes to prevent future incidents. |

|  |
| --- |
| Step 4: Conducting Training and Simulation Exercises |
|  **Simulate incidents** such as malware outbreaks or DDoS attacks to test the team's preparedness.   Conduct **tabletop exercises** where team members review potential breach scenarios and practice their response.   Ensure ongoing **security awareness training** for all employees to prevent phishing and other social engineering attacks. |

|  |
| --- |
| Step 5: Reviewing and Updating the Plan Regularly |
| * The plan should be reviewed and updated **quarterly** or after any major security incident. * Incorporate lessons learned from previous incidents or new threats that emerge. * Update the contact information, procedures, and roles as organizational changes occur. |