**Cyberattack Response SOP for IT Departments**

Date: 2025/5/25

Author: Darson Lai

**1. Preparation (Before the Attack)**

* Maintain up-to-date **asset inventory** and **network diagrams**
* Ensure **backups** are current and tested
* Define and train an **Incident Response Team (IRT)**
* Establish **communication protocols** (internal and external)
* Regularly update **antivirus, firewalls, and patch management**

**2. Detection & Identification**

* Monitor logs, SIEM alerts, and endpoint behavior
* Identify the **type of attack** (e.g., ransomware, phishing, DDoS)
* Determine **scope and impact** (systems affected, data at risk)

**3. Containment**

* Isolate affected systems from the network
* Disable compromised accounts or services
* Block malicious IPs or domains at the firewall

**4. Eradication**

* Remove malware or unauthorized access
* Patch exploited vulnerabilities
* Reset credentials and revoke unnecessary privileges

**5. Recovery**

* Restore systems from clean backups
* Monitor for signs of reinfection
* Gradually reconnect systems to the network

**6. Post-Incident Review**

* Conduct a **root cause analysis**
* Document the timeline, actions taken, and lessons learned
* Update SOPs and security controls based on findings
* Report to stakeholders and regulatory bodies if required

**7. Communication**

* Notify leadership, legal, and PR teams
* Inform affected users or customers (if applicable)
* Coordinate with law enforcement or cybersecurity agencies if needed