Pre-Incident Preparedness Checklist

Pre-Incident Preparedness Checklist

Risk Assessment & Asset Identification

- Conduct a business risk assessment using a common framework like NIST 2.0.
- Create and maintain a comprehensive asset inventory of all hardware, software, and data. Use a CMDB or asset management tool for an up-to-date, searchable list.
- Rank assets by business criticality to prioritize protection and recovery efforts.
- Classify data by sensitivity (e.g., PII, PHI) and document its storage location.
- Regularly perform automated vulnerability scans on all systems, especially internet-facing ones.
- Prioritize patching critical and high-severity vulnerabilities, particularly those on CISA's Known Exploited Vulnerabilities list.
- Form a "tiger team" to continuously flag and discuss possible solutions.
- Perform threat modeling for critical assets using the MITRE ATT&CK framework to anticipate attacker tactics.
- Identify and assess the security of all third-party vendors and supply chain dependencies.

Security Controls & Monitoring

- Deploy and tune Network IDS/IPS sensors at key network points (perimeter, cloud VPCs) to monitor for malicious traffic.
- Implement a SIEM platform to centralize logs from all critical sources (servers, endpoints, cloud, firewalls).
- Configure SIEM correlation rules to detect complex attacks that span multiple systems.

- Integrate threat intelligence feeds into your SIEM to map detected indicators against known malicious ones.
- Deploy EDR agents on all endpoints and servers.
- Enable EDR features for real-time threat blocking and automated response actions like host isolation.
- Enforce strong Identity and Access Management (IAM) practices, including MFA for all accounts, and enforce the principle of least privilege.
- Harden system configurations by disabling unused services and enforcing security benchmarks like CIS hardening guides.
- Continuously monitor authentication logs for anomalies like impossible travel logins.
- Use Infrastructure as Code (IaC) to enforce consistent, secure configurations for cloud assets.
- Conduct regular access control audits to remove excessive privileges and dormant accounts.
- Implement a process for continuous monitoring of third-party vendors.
- Integrate threat intelligence feeds into your security tools to proactively hunt for new IOCs.

Data Backup & Recovery

- Isolate backup environments from the primary network using separate VLANs and dedicated credentials.
- Encrypt all backup data at rest and in transit.
- Enforce the 3-2-1 backup rule (3 copies, 2 media types, 1 offsite).
- Use immutable storage (e.g., AWS S3 Object Lock, Azure immutable blobs) to prevent backups from being altered or deleted.
- Maintain and regularly refresh "golden images" of systems for rapid rebuilds.
- Regularly test backup restorations to verify they work and to track your Recovery Time Objective (RTO).
- Conduct full disaster recovery exercises involving multiple systems and their dependencies.

- Integrate security checks into recovery, including scanning backups for malware before restoration.

People & Training

- Implement a mandatory, ongoing phishing awareness program with regular simulated phishing campaigns.
- Establish a simple, no-blame incident reporting channel for all employees (e.g., a one-click button, hotline, or chat).
- Train employees on what to do during a suspected incident, such as immediately disconnecting from the network.
- Create an internal communication plan for emergencies, including out-of-band communication methods.

Incident Response Team & Contacts

- Form an IR team with clearly defined roles: IR Lead, SOC Lead, Endpoint Lead, Forensics, Legal, etc.
- Define clear roles and responsibilities for everyone involved in incident response, including executive leadership, PR, and HR.
- Establish a single hotline or communication channel to immediately page on-call personnel.
- Test the on-call system monthly to ensure reliability.
- Develop and practice specific playbooks for various types of incidents like ransomware attacks, data breaches, and insider threats.
- Establish a secure facility or "war room" for the incident response team to coordinate their efforts.
- Harden key security platforms (Okta, CrowdStrike, Splunk) with IR-specific configurations and pre-staged scripts.
- Document the entire evidence collection process, from what to collect to where to store it in an immutable vault.

- Create a pre-approved list of external contacts, including Legal Counsel/Breach Coach, Cyber Insurance Firm, Incident Response Retainer Firm, and Law Enforcement (FBI, CISA, etc.).
- Prepare "jump kits" with necessary hardware and software for forensic analysis.
- Maintain an offline and up-to-date copy of key documents like network diagrams and system build documents.
- Ensure executive-level buy-in and approval for the IR plan.
- Conduct periodic tabletop exercises to simulate a cyber incident and test the response plan.
- Define a clear incident classification system to prioritize and categorize incidents based on severity and business impact.
- Develop a documented and rehearsed plan for data exfiltration detection.
- Establish a clear and accessible library of incident response runbooks.
- Create a documented legal and regulatory notification matrix that maps incident types to specific reporting requirements.