IT Complete
THE Kaseya PLATFORM

Incident Response Checklist

A security incident could happen to anyone at any time. What should follow is an organized approach to address the aftermath in a bid to reduce damages and speed up the recovery process. To help you manage a security incident effectively, we have come up with this incident response checklist, which works as a step-by-step framework that ensures preparedness to mitigate and recover from any cybersecurity-related incidents.

Preparation for Incident: Responsibility and Training

The following roles, responsibilities and plans should be predefined to reduce recovery time and mitigate the impact of an incident on the organization.

Form a Risk Commitee

- ☐ Determine who is responsible for monitoring and measuring the risk level
- ☐ Designate a Company Security Officer
- ☐ Define reporting obligations and processes (includes reporting timeframe)
  - ☐ Report to Company Management
  - ☐ Report to Client Management
  - ☐ Report to Regulatory Agency and Organization
- ☐ Determine what external parties are involved

Form an Incident Management Committee

- ☐ Departments involved should include an executive team, public relations, legal, technical, finance, HR and customer support
- ☐ Define their roles and responsibilities so they understand what's expected of them
- ☐ Explain how a cybersecurity incident can develop and train them to take the appropriate response that will mitigate the impact on their team

Define Primary and Alternate Members to Decrease Dependency on Each of the Following Roles:

- ☐ Security Officer
- ☐ Privacy Officer
- ☐ Network
- ☐ Operating Systems
- ☐ Line of Business Applications
- ☐ Internal Auditing
- ☐ Marketing/PR/Communications
- ☐ Executive Management

Ongoing Reviews

- ☐ Monthly validation that system and software logs are working
- ☐ Quarterly meetings to review procedures and modify as needed
- ☐ Biannual and annual tests and reviews
- ☐ Annual incident drill
- ☐ Review of annual incident drill

Periodically Review Incident Response Procedure and Train Participants

- [ ] Update members as changes occur
- [ ] Conduct internal training
- [ ] Send personnel to training classes\conferences
- [ ] Require team members to subscribe to printed and online publications to stay abreast of new threats and response options

Communication Plans

- [ ] Determine risk level classification
  - [ ] Risk level 1 (Critical) — may cause serious damage to business and relationships, non-compliance with regulations, and criminal prosecution
  - [ ] Risk level 2 (High) — may cause some damage to business and relationships
  - [ ] Risk level 3 (Low) — minimal impact to business and relationships
- [ ] Ensure your response plan outlines the following:
  - [ ] How to communicate with the affected customers, non-affected customers, shareholders and the public
- [ ] Develop your escalation matrix
- [ ] Create a contact list of who needs to be notified and in what order of priority

Incident Response: Detection and Identification

Documenting your response to any incident is the key to identifying what aspects of your systems are compromised and the potential damage.

- [ ] Determine the nature or type of incident
  - [ ] Detect by observation
  - [ ] Detect by informants
  - [ ] Detect by evidence
- [ ] Determine the severity of the incident and the services or systems impacted
- [ ] Determine if business-critical information has been compromised or lost
- [ ] Determine if the incident put you in violation of standards, regulations or contracts
- [ ] Monitor your network and systems for irregularities and flag them immediately
- [ ] Document incident timeline information
  - [ ] What was the original source: external or internal?
  - [ ] How was the incident discovered: system alert or other?
  - [ ] Date/time the incident was detected
  - [ ] Date/time the incident occurred
  - [ ] Type of incident (web defacement, virus, malware, misconfiguration, system compromised, unauthorized access)
  - [ ] Method of intrusion (vulnerability exploited, compromised account)
  - [ ] Level of unauthorized access attained (root administrator, user)
  - [ ] Document log extracts, if available

Incident Response: Containment

Once a vulnerability is detected, take immediate steps to mitigate the spread — aka your incident response "playbook."

- [ ] Compartmentalize, shut down or disconnect the compromised systems/network
- [ ] Identify and quarantine any malware discovered
- [ ] Identify and remove any personnel involved
- [ ] Review and strengthen access credentials where necessary
- [ ] Update protections where possible
- [ ] Evaluate affected apps, servers, networks, etc.
- [ ] Eradicate infected files and, if necessary, replace hardware
- [ ] Apply temporary fixes to affected systems
- [ ] Gather and document evidence for forensic analysis
- [ ] Report vulnerabilities to the authorities
- [ ] Identify and validate the attacking host's IP address
- [ ] Monitor all possible attacker communication channels and take appropriate steps to secure them

Incident Response: Remediation

Next, you will want to eliminate whatever caused the breach and start working to repair the damage.

- [ ] Identify any internal staff that have contributed to the incident and take necessary actions
- [ ] Ensure all artifacts of the incident are fully removed from your system
- [ ] Repair or update systems as needed
- [ ] Check that all software patches are current and strengthen protections
- [ ] Ensure backups are in place and functioning properly

Incident Response: Recovery

Once the threat is eliminated and the damage repaired, your focus should cautiously turn to recovery. Ensure all procedures and steps taken are fully documented and all necessary software and hardware backups are in place.

- [ ] Test all systems for remaining or new vulnerabilities caused by the breach or the remediation process
- [ ] Continue monitoring to ensure no further potential threats
- [ ] Prepare a formal response for your customers and the public
- [ ] Have an SOP ready for the recovery process
- [ ] Remediate vulnerabilities and restore systems to normal operation
- [ ] Change passwords and tighten network security
- [ ] Ensure systems integrity and confidentiality is regained
- [ ] Document where and how changes are implemented

Incident Response: Analysis and Assessment

Document each step you took in response to the incident to ensure similar events do not happen again.

- [ ] Review "what happened" — conduct incident recovery root cause analysis
  - [ ] Identify the type of breach
  - [ ] Identify security weaknesses
  - [ ] Identify methods, products, services to correct weaknesses
  - [ ] Report information to Company Management
- [ ] Evaluate personnel and incident response effectiveness
  - [ ] Management review of incident response
  - [ ] Third-party review of incident response
  - [ ] Determine that root cause is identified
  - [ ] Determine that security weaknesses are addressed
  - [ ] Review policies and procedures and update as needed
- [ ] Determine if additional changes are needed to secure your systems
- [ ] What preventive measures have been taken/ are needed?
- [ ] Perform a "lessons learned" activity across the organization for awareness
- [ ] Determine who to include in changes or new preventative strategies
- [ ] Modify the incident response checklist as needed

Learn more, schedule a demo today!