Incident Response Playbook: Manual Response Steps

Siddhartha Devkota

Purpose & Scope

The objective is to manage incidents in an orderly and effective manner. The key objectives are damage containment, restoration of operations as quickly as possible, and lesson learning for future improvement. The approach equally suits a variety of disrupting events like system outages, security intrusions, and other disruptions affecting the continuity of the business.

How We Understand Key Terms

• Incident: Any event that disrupts service or exhibits suspicious activity.
• Major Incident: A big one — affecting lots of people, involving personally identifiable information, or financial or reputational risk.
• Containment: Prevention of the problem's diffusion.
• Elimination: Removal of the root cause.
• Recovery: Putting systems back online and verifying they're safe.

Who Does What

• Incident Commander: Oversees the response and makes the final decisions.
• Response Team: Investigating engineers, repair engineers, and reporting engineers.
• Communications Lead: Keeps everyone up-to-date internally and externally.
• Legal/Compliance: Looks for regulations, privacy, and rules.
• Ops/Infrastructure: Provides access, handles backups, handles systems.
• Executive Sponsor: Offers resources and executive sponsorship.

Step-by-Step Answer

1. **Detection & Alerting**
   Pinpoint the problem — from a log, report, or alert. Mention when it happened and what's affected.
2. **Triage / Initial Assessment**
   Identify how severe it is: small, medium, or significant. Identify which systems or users are impacted.
3. **Contain**
   o Short term: quarantine measures, suspend impacted accounts.
   o Long term: plug leaks, seal access ways, secure further.
4. **Communication**
   Inform the right people: managers, lawyers, ops, and possibly customers. Brief and simple updates.
5. **Investigation**
   Collect logs, study evidence, and determine what went wrong. Note things down so nothing gets lost.
6. **Eradication**
   Eliminate the issue: eradicate malware, rescind access, fix vulnerabilities.
7. **Recovery**
   Carefully bring systems online. Test them beforehand so all functions as intended and take notice.
8. **Post-Inc**
   After the situation calms down, assemble and discuss what occurred. Identify what worked and what requires a change.
9. **Escalation**
   If the event is getting too big, includes sensitive information, or makes a big impact — escalate immediately.

Keeping Records

Every step matters. Record:

- Dates and times of actions
- Who did what
- Logs, screenshots, and evidence
- Internal and external communication
- Conclusion with impact, cause, and solutions

References

- NIST SP 800-61: Computer Security Incident Handling Guide
- Atlassian: How to Create an Incident Response Playbook
- Swimlane: Construction Procedure for Incident Response Playbook