

Assignment 1.1: Incident Response Plan Responsibility Chart

Joshua A. Wortz

University of San Diego

CSOL-590

Prof. Fulton

01/12/2026

Incident Response Plan Responsibility Chart

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
Preparation					
Define what constitutes an incident	Organizes and maintains the overarching response plans (Ellis, 2025).	Aligns definitions with organizational business priorities and risk tolerance (Althobaiti & Alsufyani, 2024).	Ensures definitions are compatible with current IT infrastructure and logging capabilities (Skulkin, 2022).	Advises on the types of digital evidence (e.g., registry files) that necessitate forensic collection (Skulkin, 2022).	Establishes baselines for regular activity to identify better future anomalies (Salim et al., 2023).

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
Conduct regular mock drills.	Develops scenario-based drills to evaluate the response plan (Ellis, 2025; Burrell, 2024).	Participates in practice required executive-level notifications during a crisis (Ellis, 2025).	Translates IR simulation orders into executable technical instructions for IT staff (Skulkin, 2022).	Test collection tools like FTK Imager during simulations to ensure rapid response (Skulkin, 2022).	Participates in drills to refine real-time detection of indicators of compromise (Ellis, 2025).
Identification					
Discover the point of entry.	Oversees the investigation to ensure all leads are prioritized	Informs leadership whether the entry point was a	Requests specific network and application logs to pinpoint the	Analyzes forensic artifacts (e.g., email headers) to	Provides initial detection data from proactive 24/7 monitoring

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
	based on severity (Ellis, 2025).	social engineering tactic such as spear-phishing (Burrell, 2024).	entry host (Mat et al., 2024).	identify the trustworthy source of the attack (Skulkin, 2022).	systems (Ellis, 2025; Salim et al., 2023).
Perform event triage	Determines if the event meets the criteria for a formal incident declaration (Ellis, 2025).	Notifies stakeholders immediately upon confirmation of a verified breach (Ellis, 2025).	Shares technical triage results with IT teams to heighten organizational awareness (Skulkin, 2022).	Evaluates the maliciousness of artifacts to determine the threat level (Skulkin, 2022).	Sifts through network traffic data to differentiate between routine events and actual incidents (Salim

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
					et al., 2023).
Containment					
Isolate the workstation	Authorizes network segmentation to prevent lateral movement (Salim et al., 2023).	Informs management of the business impact caused by isolating critical systems (Ellis, 2025).	Coordinates workstation isolation with IT administrators (Skulkin, 2022).	Secures a volatile memory dump before isolation to preserve fileless malware traces (Skulkin, 2022).	Monitors for lateral movement attempts targeting other network segments (Malik et al., 2024).
Disconnect affected devices	Balances the timeline of	Notifies external stakeholders of	Issue logical or physical	Verifies that disconnection	Identifies additional

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
	disconnection against essential business operational needs (Ellis, 2025).	any service disruptions caused by disconnection (Ellis, 2025).	instructions for disconnecting the system (Skulkin, 2022).	does not violate the chain of custody for evidence (Skulkin, 2022).	compromised devices requiring disconnection based on traffic patterns (Salim et al., 2023).
Eradication					
Securely remove all malware.	Ensures the root cause is addressed to prevent an	Confirms to leadership that the primary threat has been	Provides specific remediation steps for the IT staff to execute	Identifies persistence mechanisms, such as registry	Performs environment-wide scans for remaining

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
	immediate re-infection loop (Ellis, 2025).	neutralized (Ellis, 2025).	(Skulkin, 2022).	run keys or malicious services (Skulkin, 2022).	malicious signatures or "fileless" code (Salim et al., 2023).
Disable unauthorized accounts	Audits all identity and access management (IAM) changes made during the breach	Reports the extent of account compromises to stakeholders and legal teams (Ellis, 2025).	Directs administrators to disable rogue service accounts or unauthorized users (Skulkin,	Identifies which accounts were used by the attacker for privilege escalation	Monitors for new unauthorized account creation attempts post-eradication (Salim et al.,

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
	(Skulkin, 2022).		2022).	(Skulkin, 2022).	2023).
Recovery					
Restore from trusted backups.	Ensures all restoration efforts follow strict change management protocols (Skulkin, 2022).	Coordinates with the board to decide the timing for production re-entry (Ellis, 2025).	Manages the restoration process alongside the IT operations department (Skulkin, 2022).	Validates that backup images were not previously compromised or infected (Skulkin, 2022).	Monitors the restored network traffic for any unusual outgoing connections (Salim et al., 2023).

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
Verify the systems are clean.	Reviews final reports to confirm all clean-up criteria have been met (Ellis, 2025).	Updates leadership that systems are secure and working as intended (Ellis, 2025).	Confirms that technical staff have patched and hardened the restored hosts (Skulkin, 2022).	Performs integrity testing to ensure no malicious code fragments remain (Skulkin, 2022).	Monitors recovered systems for a set duration to detect signs of recurrence (Ellis, 2025).
Lessons Learned					
Hold an after-action meeting.	Leads the formal meeting to analyze response	Presents a business impact summary and receives	Facilitates a technical debrief on the remediation	Submits documented findings on the attacker's TTPs	Shares detection time metrics and alert accuracy data for the team

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
	successes and plan failures (Ellis, 2025; Burrell, 2024).	executive feedback (Ellis, 2025).	actions taken (Skulkin, 2022).	for the final report (Skulkin, 2022).	to analyze (Salim et al., 2023).

Phases/Tasks	Incident Response Team Leader	Management Communication Liaison	Technical Personnel Communication Liaison	Computer Forensics Specialist	Active Monitoring Personnel
Update the incident response plan.	Updates IR protocols based on the weaknesses identified during the postmortem (Ellis, 2025).	Communicates future funding needs for security improvements to management (Ellis, 2025).	Communicates new requirements for technical training or infrastructure upgrades to IT (Skulkin, 2022).	Recommends new digital forensic tools or collection methods (Skulkin, 2022).	Adjusts monitoring rules and filters to detect similar future attacks faster (Salim et al., 2023)

Real-Life Incident

In 2008, while working at a university, I inadvertently triggered a bulk deletion script in the production environment instead of a test folder, erasing approximately 50% of the student body's accounts before I could halt the operation. In the immediate aftermath, I assumed the technical recovery role, tasked with restoring the deleted objects, while my manager, the only other person directly involved in the response, acted as the liaison to communicate the timeline and status to the organization. The incident was resolved through a coordinated effort where I focused on the technical restoration of the data while my manager handled the administrative fallout, resulting in the successful recovery of all accounts.

References

- Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. *PeerJ Computer Science*, 10, e2487. <https://doi.org/10.7717/peerj-cs.2487>
- Burrell, D. N. (2024). Exploring the cyberpsychology and criminal psychology of whaling and spear fishing online attacks. *RAIS Conference Proceedings*.
<https://doi.org/10.5281/zenodo.14514640>
- Ellis, D. (2025). 6 phases in an incident response plan. *SecurityMetrics*.
<https://www.securitymetrics.com/blog/6-phases-incident-response-plan>
- Malik, V., Khanna, A., Sharma, N., & Nalluri, S. (2024). Advanced Persistent Threats (APTs): Detection techniques and mitigation strategies. *International Journal of Global Innovations and Solutions (IJGIS)*, 2. <https://doi.org/10.21428/e90189c8.91e89a3e>
- Mat, N. I. C., Jamil, N., Yusoff, Y., & Kiah, M. L. M. (2024). A systematic literature review on advanced persistent threat behaviors and their detection strategy. *Journal of Cybersecurity*, 10(1), tyad023. <https://doi.org/10.1093/cybsec/tyad023>
- Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and the Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*, 9(7), e17156. <https://doi.org/10.1016/j.heliyon.2023.e17156>
- Skulkin, O. (2022). Incident response techniques for ransomware attacks. Packt Publishing.
<https://usd.vitalsource.com/books/9781803233994>