International Journal of Scientific and Management Research
Volume 8 Issue 7 (July) 2025
ISSN: 2581-6888
Page: 145-157

An Incident Response Playbook Guide for Small and Medium Enterprises (SMEs)

Loveth A Odozor[1], Lynda Omini[1], Seth Nti Berko[2], Ufomba Precious[1], Yuval Nitzan[1], & Kofoworola Idowu[1]
[1]Yeshiva University Private University In New York City, **USA**
[2]A private technology and business consulting company based in Georgia Atlanta
DOI - http://doi.org/10.37502/IJSMR.2025.8712

Abstract

Small and medium enterprises (SMEs) are increasingly targeted by cyber threats ranging from ransomware and phishing attacks to insider misuse and supply chain compromises. Unlike large corporations, SMEs often lack dedicated security teams, mature processes, and adequate resources to respond effectively to incidents due to the high cost of security resources. This guide provides a practical, step-by-step response playbook tailored to the unique constraints and needs of SMEs. This playbook outlines the preparation, detection, analysis, containment, eradication, recovery, and post-incident review phases. By adopting structured incident response practices, SMEs can improve their resilience, minimize business disruption, and meet compliance requirements without the overhead of enterprise-level frameworks. This document serves as a hands-on reference to help SME leaders and IT staff respond to security incidents confidently and systematically.

Keywords: Cybersecurity, Incident Response, Small and Medium Enterprises, Playbook, Business Continuity, Cyber Threat Management, Preparedness, Resilience

Introduction

Cybersecurity incidents are no longer the exclusive concern of large enterprises. Small and medium enterprises (SMEs) have emerged as prime targets for cybercriminals due to their often-limited security budgets, under-resourced IT teams, and reliance on third-party services. According to recent industry reports, over 40% of cyberattacks globally now impact small businesses, with the average cost of a data breach in an SME exceeding $120,000. “While the true cost of a data breach varies, on average, small businesses can expect to pay $120,000 to $1.24M in 2025 to respond and resolve a security incident.” (Jason F, 2025). Such an outrageous loss can lead to business closure.

While many SMEs recognize the importance of cybersecurity, few have a documented incident response (IR) process in place. In practice, incidents are often handled reactively, with ad hoc decisions made under pressure. This lack of preparation increases the likelihood of operational downtime, regulatory penalties, and reputational harm.

Developing a clear, actionable incident response playbook can help SMEs bridge this gap. A playbook provides structured guidance before, during, and after an incident, outlining the roles, responsibilities, and procedures necessary to detect, contain, and recover from cyber threats

efficiently. Unlike complex enterprise frameworks that require specialized security operations teams, this guide is designed to be accessible and practical for smaller organizations with limited resources.

The purpose of this document is to equip SME leaders, IT managers, and designated incident handlers with an easy-to-follow roadmap for responding to cybersecurity incidents. By leveraging this playbook, SMEs can improve their readiness, reduce the impact of cyber events, and build confidence among customers, partners, and regulators.

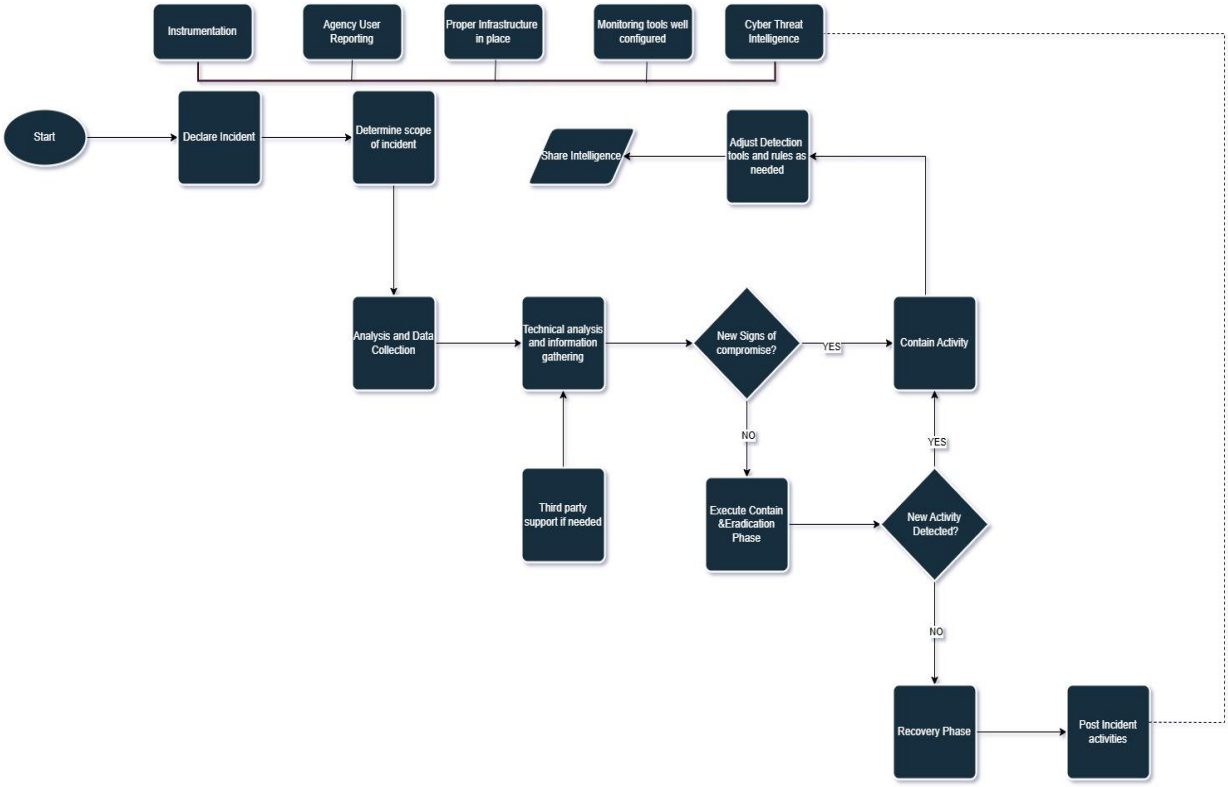

Fig.1 General Incident Response Playbook Workflow for SMEs

Why are playbooks necessary for SMEs?

Reduces Response Time:

- A playbook provides predefined steps and checklists, enabling your team to react quickly when an incident occurs
- Faster action limits damage, containing threats before they spread further into your systems.

Minimize Business Disruption

- With clear recovery procedures, SMEs can restore operations faster, reducing costly downtime and revenue loss.
- Ensures continuity of critical services, even during crises.

Improves Consistency and Accountability

- Standardizes how incidents are detected, reported, and managed across the organization.
- Defines roles and responsibilities so everyone knows exactly what to do and who to inform.

Supports Regulatory Compliance

- Many regulations (e.g., GDPR, HIPAA, CCPA) require documented incident response processes.
- A playbook demonstrates due diligence and helps meet legal and contractual obligations.

Protects Reputation and Customer Trust

- Structured response and timely communication show customers, partners, and stakeholders that you take security seriously.
- Reduces reputational harm by preventing chaotic or delayed responses.

Strengthens Organizational Preparedness

- Regularly reviewing and practicing the playbook raises awareness and improves readiness across staff.
- Helps identify security gaps and drive continuous improvement of defense.

Organizations use incident response strategies to tackle cyberattacks and cybersecurity incidents, reducing recovery time and costs and minimizing damage caused by breaches. The following are the phases of the Playbook.

Preparation Phase

A standard incident response methodology focuses on preparation, not just developing the capability to respond effectively, but also making sure that systems and networks are properly equipped and ready to handle potential incidents. This phase ensures readiness to handle cybersecurity incidents effectively, fostering resilience and reducing response time.

Preparing to handle Incidents:

Identifying key assets during preparation phase involves determining the systems, data, and resources that are critical to an organization's operations. This includes pinpointing assets like servers, databases, intellectual property, and sensitive customer information that, if compromised, could significantly impact the business. By prioritizing and categorizing these assets, the organization can allocate appropriate protections and ensure they are included in the incident response plan. Next is to ensure adequate configurations, which means setting up systems and devices securely with proper settings to reduce vulnerabilities. Ensuring system backups and recovery involves creating regular backups and testing restoration processes to guarantee data can be recovered quickly in case of an incident. Network segmentation is another important factor to consider in the planning phase; it is the process of dividing the entire network into smaller areas. This is done to reduce the attack surfaces, especially in the case of an incident, to protect systems and sensitive information. Preventive measures such as system hardening are part of the planning phase of the IR, such System hardening techniques like patches, regular updates, and risk assessments are aimed at keeping software up to date,

fixing known vulnerabilities, and regularly assessing potential risks in a bid to strengthen defenses against security attacks.

The Incident Response team is selected during this phase of the IR, preparing tabletop exercise, and maintaining sufficient staffing by assigning roles and responsibilities. It is important to note that the IR team should not be only the Information Security department/unit. Accordingly, incident response teams often manage the organization's incident information sharing efforts, incident record keeping, such as aggregating information related to incidents and effectively communicating with other relevant stakeholders, as well as ensuring sensitive information is not leaked to the public in this process.

Continuous monitoring in the preparation phase involves consistently tracking network traffic, system activities, and security logs to detect potential threats before they escalate. It ensures real-time visibility into the environment, allowing early identification of vulnerabilities or suspicious behavior that may indicate future incidents. Ensuring that every necessary step is well covered during the planning phase will make it very easy for cybersecurity to be detected as soon as they happen, which will make the detection phase run smoothly.

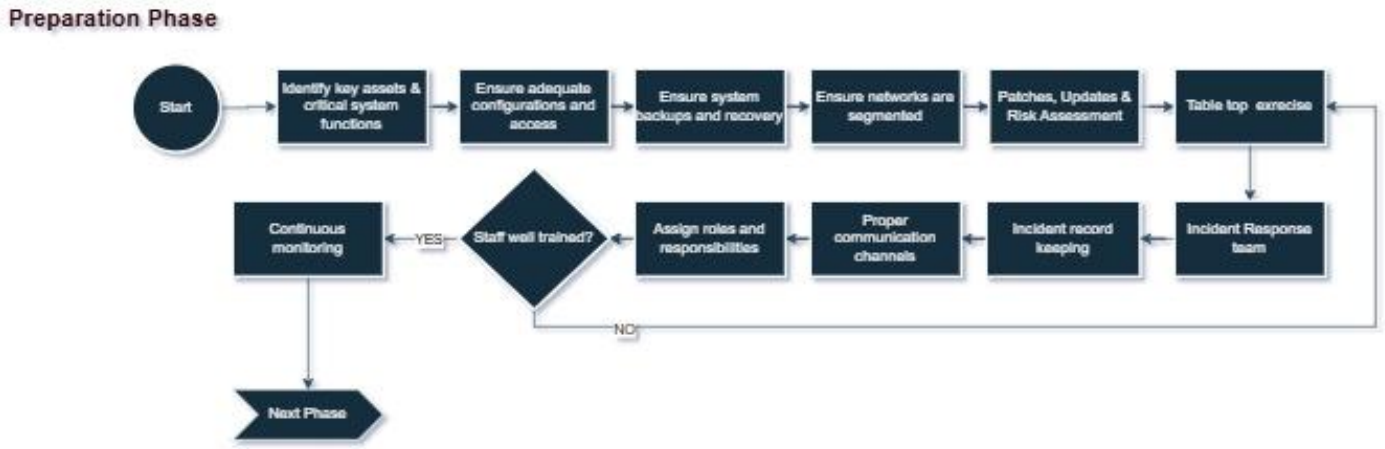

Fig.2 Preparation Phase of the Incident Response playbook for SMEs

Detection Phase

The detection phase of an incident response playbook is critical for identifying potential security incidents as early as possible to minimize damage. This phase involves recognizing, analyzing, and confirming anomalous activity that may indicate a cybersecurity incident. One of the most crucial aspect of the incident response process is to correctly detect and assess the entire incident, accessing whether an incident has occurred, to what extent is its occurrence, what type of incident, what information could the threat actors be after, and magnitude of the compromise within cloud, operational technology (OT), hybrid, host, and network systems, all based on the SMEs environment in question.

Activities involved in the Detection Phase

Threat monitoring involves deploying and configuring tools such as SIEM systems, IDS/IPS, firewalls, and endpoint detection tools to ensure continuous monitoring and anomaly detection. Security logs from servers, applications, firewalls, user activity, and third-party threat

intelligence feeds are analyzed to identify suspicious activities. Automated alerts are generated by security tools when rule violations or unusual patterns, like failed logins or malware signatures, are detected. Additionally, employees or users can manually report suspicious behaviors, such as phishing attempts or abnormal system activity.

Alerts are initially triaged by classifying them based on severity, potential impact, and the systems affected. High-priority alerts concerning sensitive data or critical assets are addressed promptly, while low-priority ones, often involving minimal risk, are deprioritized. The completion of the detection phase leads to the next phase of the IR, which is to properly Analyze

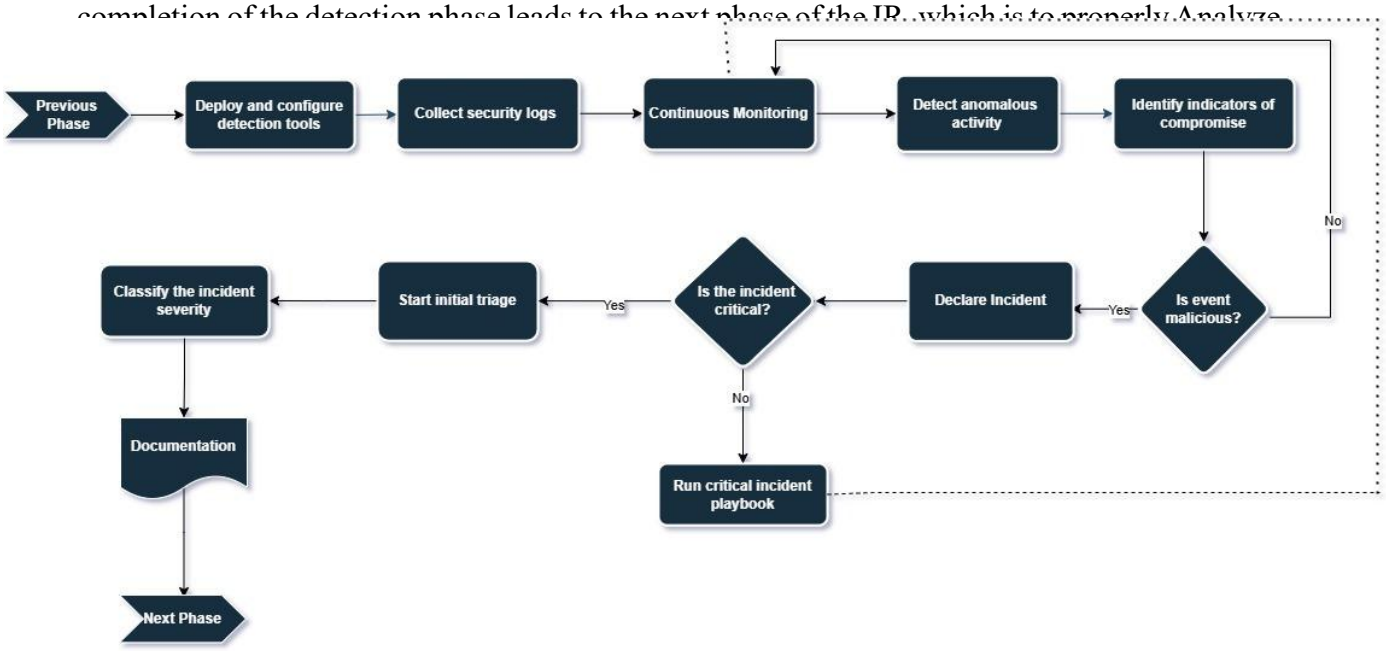

Fig.3 Detection Phase of the Incident Response Playbook for SMEs

Analysis Phase

The Analysis phase aims to systematically understand the scope, impact, and potential risks of the incident, enabling an informed and effective response. This also involves gathering and examining all relevant data and evidence related to a detected activity to understand its nature, scope and potential impact.

Activities in the Analysis Phase:

Verify previously collected data by cross-checking its accuracy and relevance to the incident while identifying any information gaps. Ensure that all affected systems and endpoints are accounted for in the preliminary findings. Scope validation involves assessing verified data to ensure all endpoints and affected systems have been identified. If the scope is incomplete, it is updated with additional data before proceeding; otherwise, the process moves to the next step.

Identify and collect indicators of compromise (IOCs) such as malicious files, IP addresses, and URLs across affected systems using tools like endpoint detection and response (EDR) and system logs. Consolidate these IOCs to facilitate correlation and further analysis.

Perform technical analysis by conducting in-depth forensic analysis of affected systems, networks, and data by examining file systems, memory dumps, and network traffic for

malicious activity. Identify the attacker's tactics, techniques, and procedures (TTPs) to understand the nature of the threat.

Threat intelligence involves matching discovered indicators of compromise (IOCs) with threat intelligence feeds to determine if an incident aligns with known attack patterns or threat actors.

Damage assessment evaluates the impact on data, systems, and operations, quantifying losses and identifying potential exfiltration or modification of sensitive information. During risk identification, gaps in security controls and potential vulnerabilities are pinpointed, along with mitigation strategies to address them. Incident analysis is completed by verifying all systems and data involved, ensuring findings are actionable, and deciding whether additional data collection is needed before proceeding. Finally, a summary report is prepared and shared with the incident response team, leadership, and stakeholders, transitioning to the next response phase with clear action steps.

The Goal is to enable an informed and structured approach to mitigating the incident, ensuring a comprehensive understanding of its impact and residual risks. After the incident has been properly analyzed, we can go further to contain the affected systems and eradicate the threat from the environment.

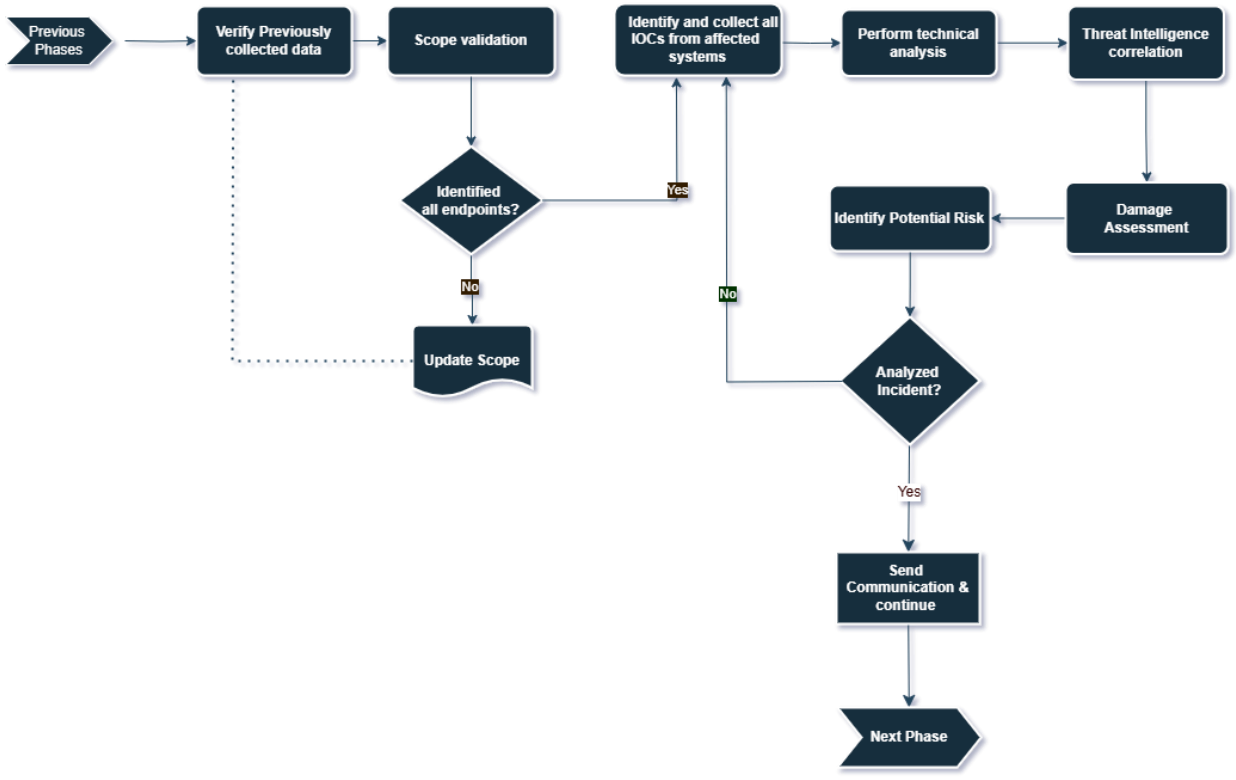

Fig.4 Analysis Phase of the Incident Response Playbook for SMEs

Containment and Eradication Phases

Containment is a critical focus during incident response, particularly in major incidents, to prevent further harm and minimize immediate impact by cutting off the adversary's access. The type of containment strategy depends on the specific nature of the threat, such as the approach to handling fileless malware differing from that for ransomware. The goal for Eradication is to restore normal operations by removing any traces of the attack, such as malicious code, and

addressing the vulnerabilities exploited by the attacker. Before proceeding to eradication, it's essential to ensure that all potential access points have been secured, adversary activities are fully contained, and all relevant evidence has been gathered, often requiring several iterations.

Actions to be taken as soon as there's a new sign of compromise.

Identify the affected systems impacted by the incident by determining which endpoints, servers, or network segments are compromised. Review logs from IDS, IPS, and EDR tools to analyze and understand the nature of the attack.

Isolate affected systems by disconnecting them from the network, such by removing network cables or disabling wireless connections.

Temporarily enforce least privilege on all critical systems to ensure only authorized users have access. Implement network segmentation to prevent the spread of threats, such as by isolating affected subnets, VLANs, or servers. Additionally, update firewall filters and perform network scans to enhance security and detect potential threats.

If new signs of compromise are detected, revisit the technical analysis step to reassess the incident. Once the containment is successful and no new signs are found, preserve evidence for potential legal investigation, update detection tools, and proceed to the eradication phase.

During the incident response, capturing forensic analysis involves reviewing logs, malware, and affected systems to determine the root cause, such as the exploited vulnerability or attack vector, while updating detection tools. For high-risk systems, re-imaging may be necessary to fully remove anomalies, using standard Operating System templates to rebuild the affected systems.

Restore impacted systems and files from backups that are confirmed to be clean and secure. Ensure the backups haven't been compromised by the ransomware, using offline or cloud-based backups whenever possible. At the end of the containment stage, the Incident responders move forward to recover the affected systems and incorporate them back into the network, this is called the Recovery Phase of IR

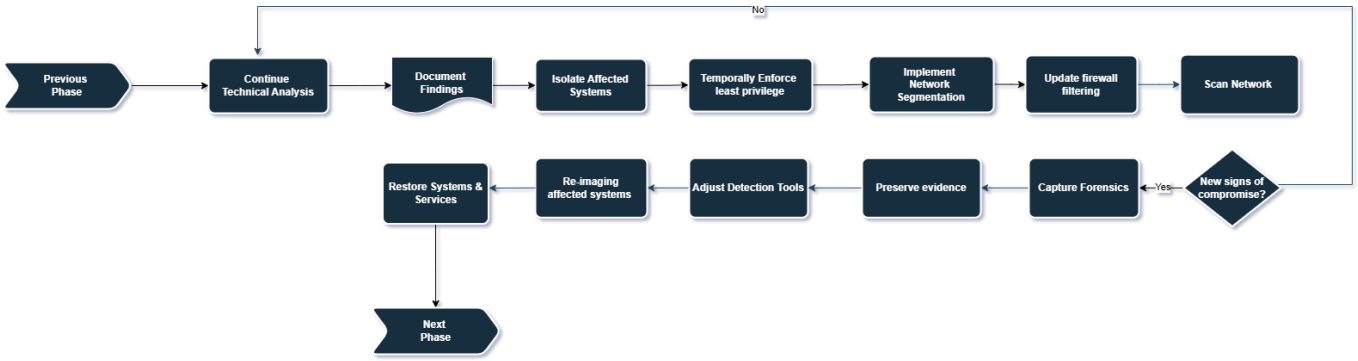

Fig.5 Containment and Eradication Phases of the Incident Response Playbook for SMEs

Recovery Phase

A key requirement for a successful recovery is enhanced vigilance and controls to ensure the recovery plan has been successfully executed and that threat actors are not actively operating. As soon as data has been restored from backup sources, verify data integrity, test to ensure all

backups are incident-free, and then develop methods to detect lingering threats and re-infection signs.

Activities involved:

Reconnect systems to the network and ensure the restored data is from a clean source using tightened perimeter security while testing systems thoroughly to ensure there are no traces of threats. To confirm that normal operations have resumed, perform an independent test or review compromise/response-related activities.

The goal of the recovery stage is to recover affected systems, detect related attacks, review cyber threat intelligence, and closely monitor the environment for signs of threats. Further analysis of the incident will be carried out to fully understand what happened, what could be done better, and find the gaps existing in the network, this is called the Post-Incident Review phase. Organizations learn great lessons through this phase.

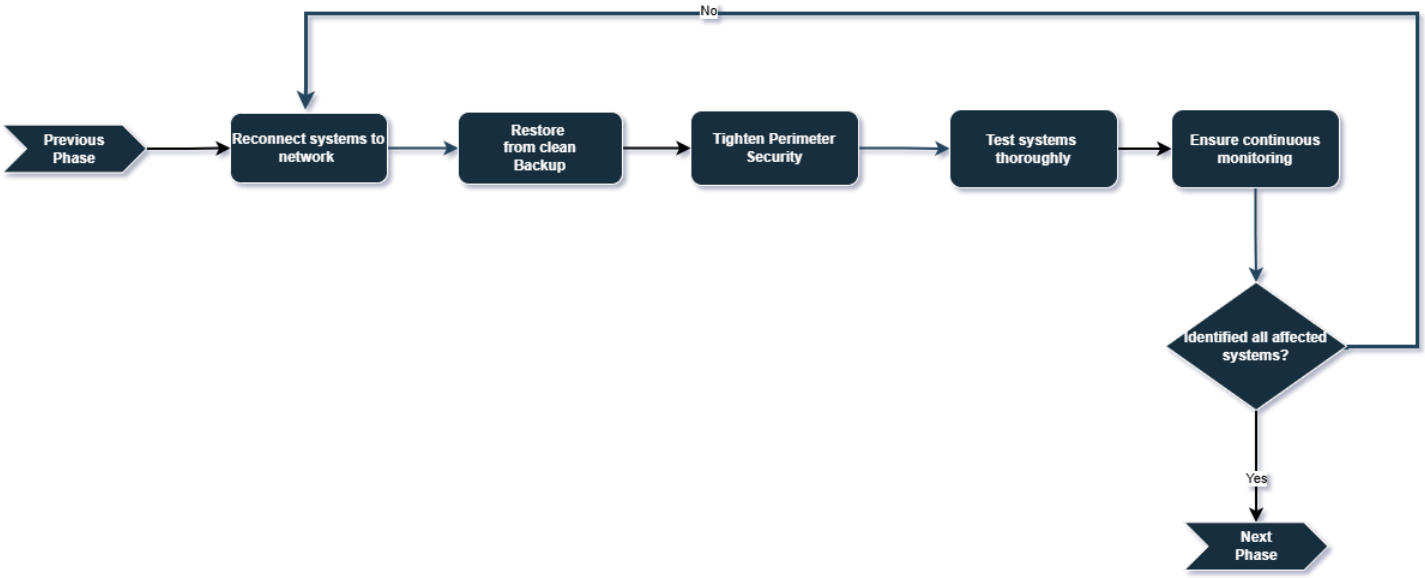

Fig.6 Recovery Phases of the Incident Response Playbook for SMEs

Post-Incident review Phase

This phase focuses on evaluating the response of incidents, identifying areas for improvement, and integrating lessons learned into organizational practices to prevent future occurrences.

Activities Involved:

Conducting incident review consists of a team with representatives from IT, security, legal, and management to review the incident, analyzing the timeline and effectiveness of response actions. Identify any delays, gaps, or communication issues, and gather feedback from all team members involved in the response.

Identifying and documenting lessons learned involves organizing a workshop with stakeholders to discuss challenges, solutions, and opportunities for improvement.

Reviewing and updating the Incident Response Plan (IRP) involves comparing the IRP against findings from the incident review and updating protocols, checklists, and procedures to address identified gaps.

Sharing insights with relevant teams involves conducting a debriefing meeting to present key findings, summarize the incident, and discuss its impact on operations, reputation, and financials.

Implementing prevention measures involves introducing new protocols to prevent future incidents, while testing these measures ensures their effectiveness. Integrating new measures includes incorporating them into existing systems and processes to enhance overall security and preparedness.

Conducting employee training involves developing materials based on lessons learned and organizing regular sessions to cover update policies and preventive measures. It also includes using real-world scenarios for engagement, ensuring role-specific training, and tracking participation and knowledge retention through assessments and simulations.

In the post-incident phase of an incident response, officially closing the incident involves finalizing all documentation, signing off on the closure report, and notifying stakeholders that the incident has been resolved. It also includes securely storing incident documentation for future reference and compliance audits.

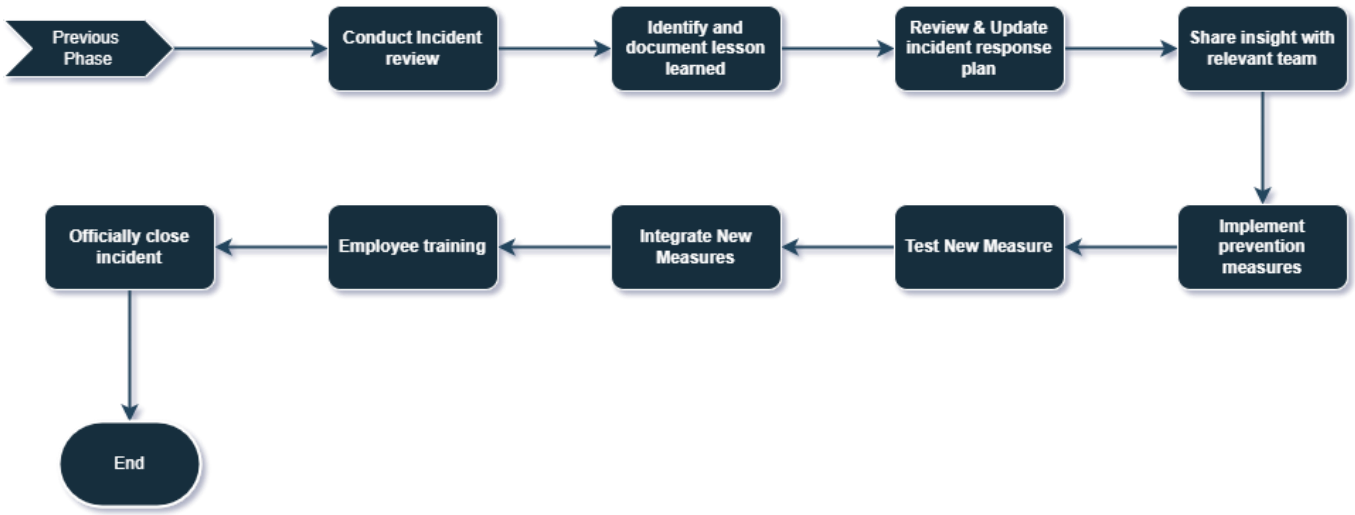

Fig.7 Post-Incident Phases of the Incident Response Playbook for SMEs

A case study of Cyberattacks on SMEs

SMEs, as well as larger organizations, face an increasing number of cyberattacks. Accenture's Cybercrime study reported that 43% of all cyberattacks are on SMEs, with about 95% of them resulting from human error. This study shows the need for SMEs to properly equip themselves with the knowledge on how to follow and implement Incident Response playbooks to ensure that they can recover from incidents as soon as possible. One outstanding case study is the Efficient Escrow, a California-based Escrow company, which faced a great deal of cyberattacks, resulting in the loss of $1.5 million from their bank account. The attackers gained access through malware, using a Trojan horse to infiltrate the organization's systems. The attackers sent $432,215 to Moscow, and a subsequent $1.1. million to China. The impact of this attack was very heavy on Efficient Escrow, from financial loss to legal fees, to loss of customers, bad reputation, and eventually, the business was shut down.

In cases like this, adequate planning could have helped the organization to properly plan for such the occurrence of a cyberattack. There is never enough security, hence it is always a question of when this attack will happen, and not will this attack happen?. This is why SMES need to have standard guidelines and a playbook on how to respond to Cyberattacks. SMEs can use playbooks as well as checklists to ensure they meet a good baseline for their incident response plan.

Below is expanded guidance with simple templates for incident reporting and documentation, aligned with industry best practices such as NIST SP 800-61 and SANS Incident Handler's Handbook, and simplified for SMEs:

Initial Incident Report Template

Purpose: Quickly capture essential details during the early stages of an incident.

Template:

Field	Details Example
Date/Time Detected	2025-07-21 09:34 AM
Reported By	Jane Doe (IT Support)
Affected System(s)	Finance Server -FS-01
Description of Incident	Unusual login activity from a foreign IP address
Detection Method	SIEM alert (Brute-force attempt detected)
Initial Severity Rating | Medium	Potential unauthorized access
Actions Taken	Account locked, log collected
Assigned Responder	John Smith (Security Analyst)
Communication Initiated	[ ] Yes [ ] No
Escalation Required	[ ] Yes [ ] No

Table 1. Initial Incident Report Template for SMEs

Incident Assessment Checklist

Purpose: Helps responders make consistent evaluations during triage.

Checklist:

- ✓ Confirm the incident (not a false positive)
- ✓ Identify affected systems/users
- ✓ Classify the type of incident (e.g., phishing, malware, data breach)
- ✓ Determine business impact (data loss, downtime, etc.)
- ✓ Capture volatile data if needed (e.g., active processes)
- ✓ Determine the need for isolation or containment
- ✓ Assign severity level (Low, Medium, High, Critical)
- ✓ Document assessment in the incident log

Escalation Matrix Template

Purpose: Define when and how incidents are escalated.

Template

Severity Level	Escalate To	Response Time	Communication Required
Low	IT Support Lead	Within 24 hrs.	Internal only
Medium	Security Team / Manager	4 hours	Internal + Management
High	CISO / Executive Sponsor	1 hour	Full IR team + Execs
Critical	External Legal/Authorities	Immediate	All Stakeholders

Table 2. Escalation Matrix Template

Communication Log Template

Purpose: Track who was informed, when, and what was shared

Template

Date/Time	Stakeholder Contacted	Method	Summary of Communication
2025-07-21 10AM	**IT Director**	**Email**	**Informed of breach signs**
2025-07-21 11AM	**Legal Counsel**	**Phone Call**	**Possible PII exposure**
2025-07-21 1PM	**Affected Users**	**Email**	**Password reset initiated**

Table 3. Communication Log Template

Post-Incident Review Template

Purpose: Document lessons learned and improve processes.

Template

Field	Details Example
Incident Summary	**Unauthorized login attempt on the finance server**
Root Cause Identified	**Weak password + no MFA**

Containment Actions	**Account disabled, IP blocked, password reset**
Recovery Actions	**System monitored, patched, and reenabled after 48 hrs.**
Lessons Learned	**Enforce MFA, review password policy**
Improvements Suggested	**Add an alert for multiple failed logins**
Final Severity Rating	**Medium**
Closed By/Date	**Jane Doe / 2025-07-23**

Table 4. Post-Incident Review Template

Increasing Security in SMEs with Minimum costs

Small and medium-sized enterprises (SMEs) can increase their incident response (IR) abilities despite having resource constraints by adopting adaptive and agile strategies listed below:

1. Start Small, Prioritize Critical Assets: They can begin by identifying their most valuable digital assets, which is achieved through categorization and classification, then more focus can be placed on these assets during initial IR planning. A simple, actionable playbook for high-impact incidents like ransomware or phishing is a good way to start.
2. Use Agile Sprints: Rather than build a full IR program all at once, SMEs can consider taking an agile approach by implementing one small component at a time. For example, establishing roles, creating communication templates, or setting up logging to capture all logs. Regular review and iteration help refine processes based on lessons learned.
3. Leverage Existing Tools: Many SMEs already have basic tools like antivirus, firewalls, or Microsoft 365; they can reduce costs by leveraging the built-in alerting and log features that these tools offer, which can be used for basic detection and response without extra cost.
4. Train Staff: IR maturity doesn't require full-time security staff. SMEs can cross-train existing IT or operations personnel through affordable online platforms, tabletop exercises, or community initiatives like ISACA or local InfraGard chapters.
5. Adopt Frameworks Lightly: Rather than adopting an entire standard (like NIST 800-61) all at once, SMEs can selectively implement key elements most relevant to their current risk profile, thereby gradually expanding coverage.

By being adaptive, iterative, and resource-aware, SMEs can build a resilient incident response capability that improves over time without overwhelming their capacity.

Conclusion

Cybersecurity incidents present a growing and costly threat to small and medium enterprises, which often lack extensive resources and specialized personnel available to larger organizations. This practical incident response playbook provides SMEs with a clear, structured, and actionable roadmap to prepare for, detect, analyze, contain, eradicate, and recover from cyber threats effectively. By adopting these tailored procedures, SMEs can significantly reduce the impact of security incidents, maintain business continuity, and demonstrate due diligence to regulators and customers, and all stakeholders.

However, we acknowledge that implementing this playbook is not a one-time effort but an ongoing commitment to ensure resilience. Regularly reviewing, updating, and practicing the steps outlined here will help organizations strengthen their defenses, build a culture of preparedness, and respond confidently to evolving threats. Ultimately, a well-developed and consistently applied incident response process empowers SMEs to protect their assets, safeguard stakeholder trust, and thrive in an increasingly digital and interconnected business landscape.

Declaration

Acknowledgement

We acknowledge the editors and reviewers of this paper; your advice and insights have been of immense help.

Funding

Not applicable

Availability of data and materials

Not applicable

References

1) Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. Computer Security Incident Handling Guide, 2(2). https://doi.org/10.6028/nist.sp.800-61r2
2) Cybersecurity and Infrastructure Security Agency (CISA), 2021. Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. Available at: <https://www.cisa.gov/sites/default/files/2023-01/federal_government_cybersecurity_incident_and_vulnerability_response_playbooks_508c_5.pdf>
3) Firch, J., 2025. The true cost of a data breach to small business. Reviewed by J. Selvidge. [online] Available at: <https://purplesec.us/learn/data-breach-cost-for-small-businesses/?utm_source=chatgpt.com>
4) Palatty, N. J. (2025, June 16). 51 small business cyber attack statistics 2025 (and what you can do about them). WebsiteBuilderExpert. Available at: < https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/#:~:text=face%20cyber%20attacks.-,Accenture's%20Cybercrime%20Study%20reveals%20that%20nearly%2043,cyber%2Dattacks%20are%20on%20SMBs.>
5) https://security.cms.gov/policy-guidance/risk-management-handbook-chapter-8-incident-response-ir
6) https://www.group-ib.com/resources/knowledge-hub/network-segmentation
7) https://graniteharbor.com/learning-center/articles/business-continuity-planning-for-entrepreneurs
8) https://security.cms.gov/policy-guidance/risk-management-handbook-chapter-8-incident-response-ir
9) https://www.group-ib.com/resources/knowledge-hub/network-segmentation