

Trace3's Incident Response Plan & Playbook Development service, a collaborative effort between our Incident Prevention & Response Team and Governance, Risk, and Compliance (GRC) practice, offers a comprehensive approach to crafting custom and effective incident response strategies. This service ensures your organization is prepared with actionable, scenario-specific plans and playbooks that guide your response efforts, minimizing the impact of cybersecurity incidents. By aligning with industry best practices and regulatory requirements, our artifacts empower your teams to respond confidently and efficiently to threats, safeguarding your operational continuity and reputation.



OVERVIEW

In the dynamic realm of cybersecurity, readiness, and rapid response are key to mitigating risks and preserving business integrity. Trace3's specialized service in developing Incident Response Plans & Playbooks is designed to equip your organization with tailored, actionable guides that prepare you for a wide range of cyber threats. Our combined expertise from the Incident Prevention & Response team and the GRC practice ensures that every artifact not only addresses technical response actions but also aligns with governance, risk management, and compliance standards, such as NIST 800-61. This dual focus guarantees a holistic approach to incident response, emphasizing not just immediate threat mitigation but also long-term resilience and regulatory adherence.

OFFERING DETAILS

Our Incident Response Plan and Playbook Development service is structured to provide your organization with a strategic framework tailored to your unique security landscape:

Collaborative Assessment: We begin with a comprehensive assessment of your current incident response capabilities, identifying gaps and opportunities for enhancement. This collaborative effort between your team and ours sets the stage for development that is both effective and aligned with your needs.

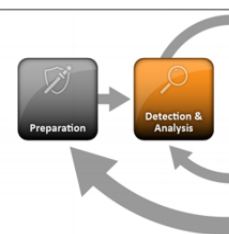
Customized Plan and Playbook Creation: Leveraging insights from the assessment phase, our experts craft detailed plans that document workflows and communication standards within the organization. Additionally, playbooks include step-by-step response actions, decision-making criteria, and communication plans, ensuring a coordinated and efficient response to threats.

Integration and Training: Beyond creation, we assist in integrating these plans and playbooks into your existing incident response processes. This phase includes training your team on effectively executing the plan and playbooks, ensuring readiness and confidence in handling incidents.

Continuous Improvement: Recognizing the evolving nature of cyber threats, we offer ongoing support to review and update the plan and playbooks in line with new threats, technological advancements, and changes in regulatory requirements.

Incident Response Plan

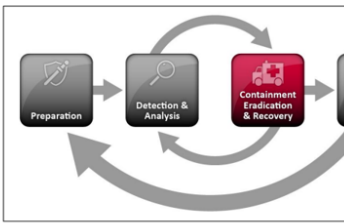
priority-setting based on data and system criticality and sensitivity, required collection and analysis of incident information, information preservation, documentation, and communication.



Upon the immediate identification of a suspected or confirmed data breach involving systems or data containing cardholder info, NPPI, or FedLine (NACHA) information, the IRT will follow escalation processes to ensure compliance with all notifications and legal responsibilities.

Refer to the organization's Crisis Communication Plan for more information on communication procedures.

3.6 CONTAINMENT, ERADICATION, AND RECOVERY



3.5.2 WHAT IS A SECURITY INCIDENT?

A security incident may involve any, or all, of the following:

- A violation of corporate computer security policies
- Unauthorized computer access,
- Loss of information confidentiality,
- Loss of information availability,
- Compromise of information integrity,
- A denial-of-service condition against data, network, or systems,
- Misuse of service, systems, or information, or
- Physical or logical damage to systems.

Security incident examples include:

- The presence of a malicious application, such as a virus or Trojan horse
- Establishment of an unauthorized account for a user
- Unauthorized network activity,
- Presence of unexpected/unusual programs, or
- Computer theft.

3.6.1 PLANNING

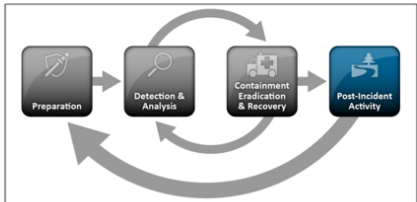
The IRT should collect and/or review the incident documentation and event reports verified as being factual (information may have been misreported or incorrectly documented) and re-consider its appropriateness if already assigned. The IRT of the IRT, needs to be notified of the incident, both internal and external to the organization.

If the incident requires computer forensic analysis, arrangements must be made for the collection and preservation of evidence. Information should be restricted on a need-to-know basis.

At this stage, thoroughness is more important than speed. The primary objective is to contain the incident and prevent further damage.

Every incident should be treated as if it will lead to a court case. Establish robust evidence, including the date and time of every entry in the incident log and signing of a robust body of evidence. Also, document each individual's time spent on the incident response costs.

3.7 POST-INCIDENT ACTIVITY



3.7.1 RESPONSIBILITIES

The Incident Manager initiates, and coordinates, remediation and post-incident activities as soon as basic risk mitigation activities have been taken to stabilize the environment. The Incident Manager keeps the Incident Owner informed of status and actions being taken throughout the remediation and post-incident review process, who in turn keeps executive leadership apprised of the situation.

Based on reviews of findings at the time, and an assessment of project size and complexity, the Incident Manager convenes one or more Remediation and Post-Incident Review Teams (PIRTs).

- The Incident Manager and PIRTs document findings and activities continuously throughout the review.
- Scopes of various PIRTs may be segmented by type of technical expertise required, and/or by required knowledge of policy or organizational issues, as appropriate for the particular situation.
- The Incident Manager may be a participating member of PIRTs or may delegate the work to other individuals. In any case, the Incident Manager maintains continuous, close communications with PIRTs, and over-all control of remediation and post incident review activities.
- PIRTs analyze conditions in the IT environment local to the incident, including technical, policy, and organizational aspects. Scope of review includes circumstances and activities before the incident as well as during the response.
- Throughout the process, the Incident Manager and PIRTs continue to analyze implications of local IT environment issues and assess scope of areas potentially affected, potentially including other IT environments throughout the organization.
- The IRT Coordinator and PIRTs prepare an action plan for recommended changes to improve the local environment going forward.
- PIRTs document lessons learned, including aspects that were good as well as those which were problematic.

VALUE

We ensure a strategic advantage in cybersecurity readiness and response by tailoring each plan and playbook to your organization while enhancing your team's ability to act decisively and mitigate risks effectively. Developing customized Incident Response Plans and Playbooks is a critical investment in your organization's cybersecurity and operational resilience. These playbooks serve as a roadmap for rapid and effective response, significantly reducing the time to contain and eradicate threats. By minimizing the impact of incidents, you not only protect your critical assets and customer data but also maintain trust and confidence among stakeholders. Furthermore, our emphasis on compliance and governance ensures that your response strategies meet regulatory standards, protecting your organization from potential fines and legal challenges.

As cyber threats continue to evolve, the value of having a customized, agile response strategy cannot be overstated. Investing in our Incident Response Plan and Playbook Development service is an investment in safeguarding your organization's future, reputation, and growth.

Enable your Security team's response to cyber threats with Trace3's Incident Response Plan and Playbook Development service. For more information, contact your Trace3 Security expert or visit us at Trace3.com. Strengthen your cyber defense today and turn your response strategy into a competitive advantage.