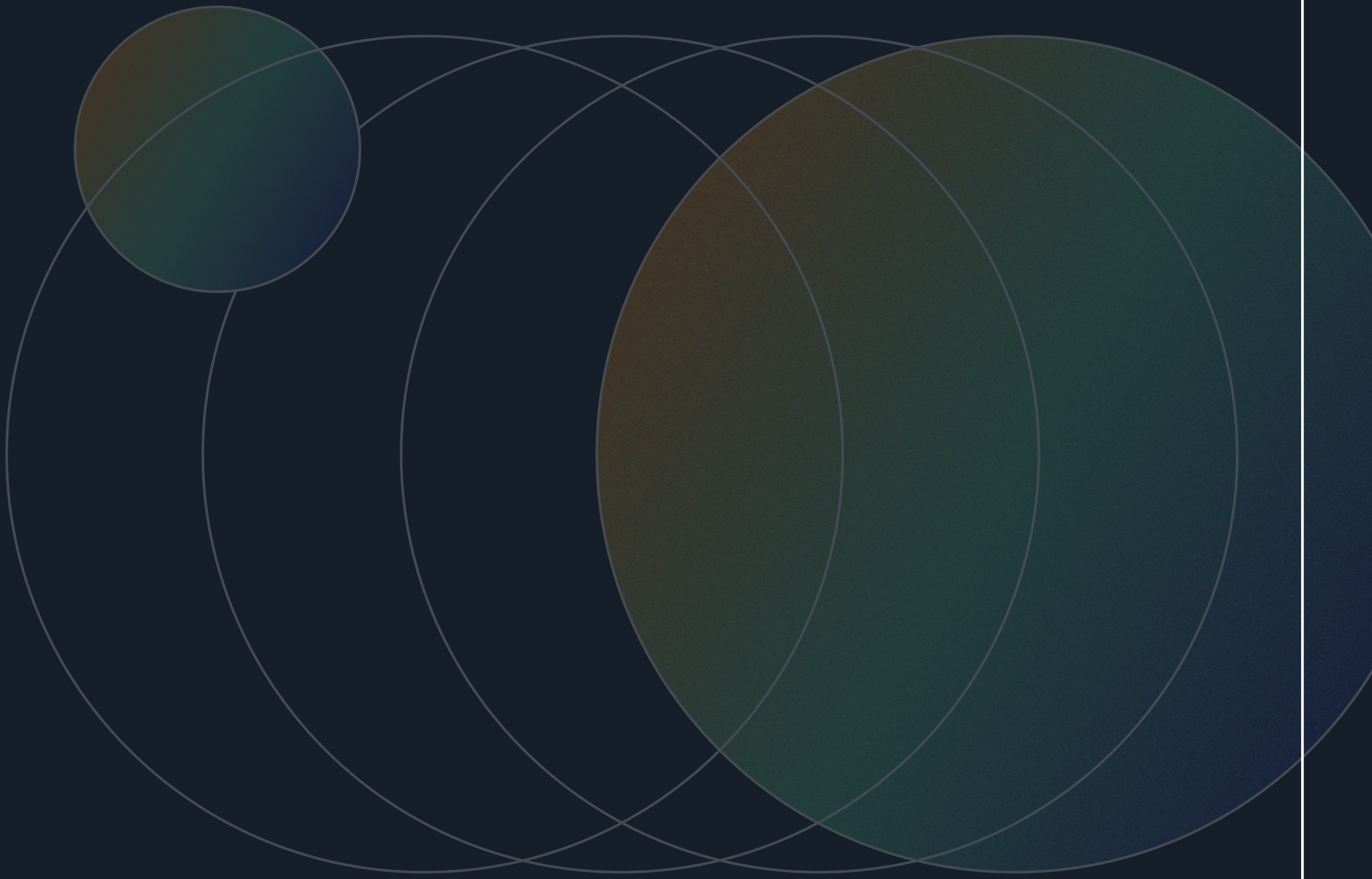
RSI | *Whitepaper*

Incident Response Services



858.999.3030 | info@rsisecurity.com
2022

TABLE OF CONTENTS

Incident Response Services

1. What is Incident Response Planning?
2. Seven Phases of Incident Response
3. Incident Response Tabletop Exercises
4. Use Cases for IR Tabletop Exercises
5. Holistic Incident Management (in Six Steps)

What is Incident Response Planning?

Incident Response is the area of cybersecurity that concerns what an organization does when an attack, breach, or other cybersecurity incident happens. It works in concert with preventive measures that make incidents less likely. But the real focus of Incident Response, and Incident Response Planning, is minimizing the negative impact of cybersecurity incidents that do occur.

To that effect, an Incident Response Plan (IRP) is a strategic approach to handling an incident when it happens. IRPs differ for every organization, but most share the same priorities:

IRP Priority 1

Protect human life and safety, as they relate to stored information.

IRP Priority 2

Protect critical business operations and any relevant sensitive data.

IRP Priority 3

Protect other information and prevent exploitation across all systems.

IRP Priority 4

Prevent damage to all systems and data, including non-sensitive data.

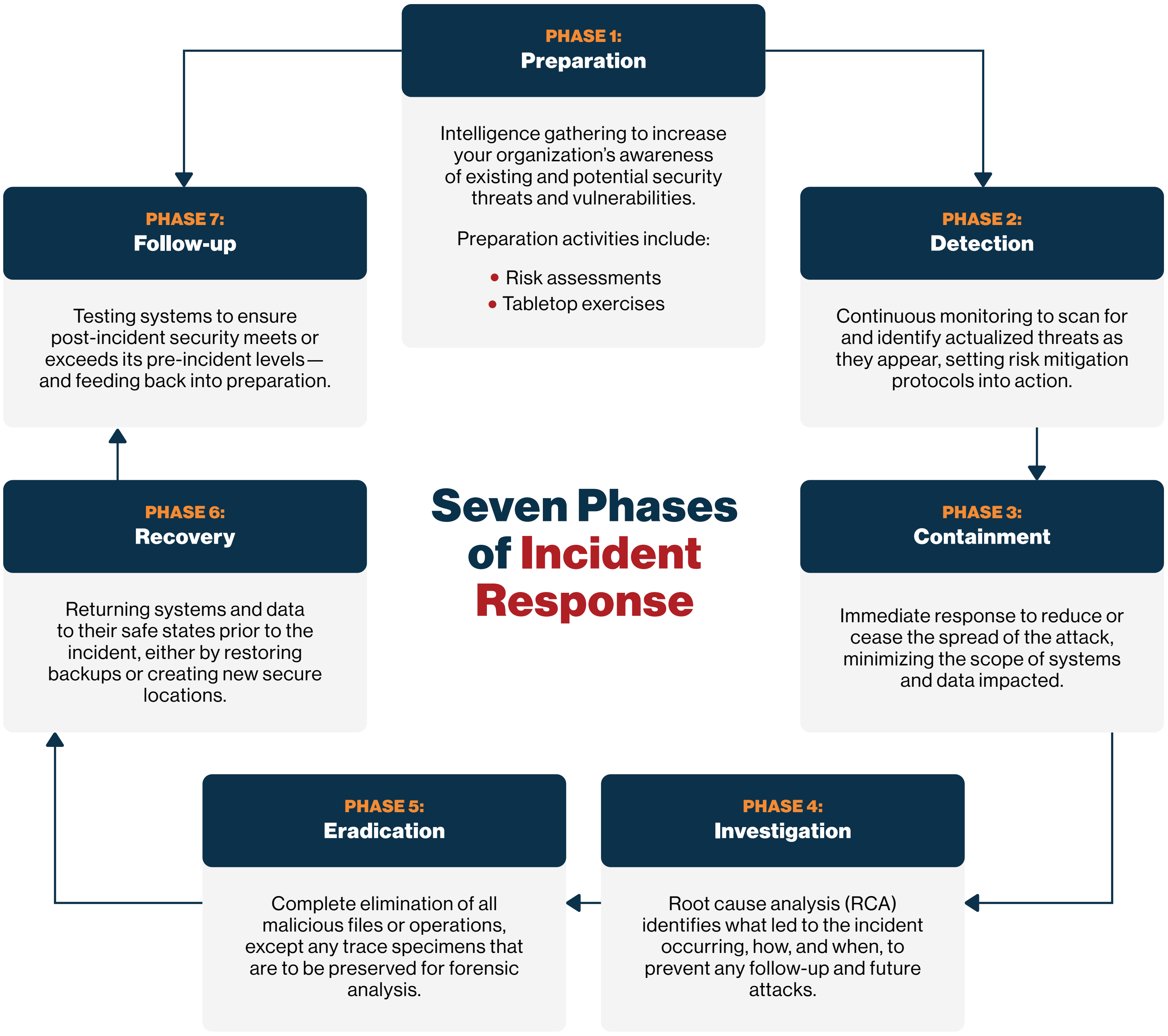
IRP Priority 5

Minimize disruption of computing resources, including all processes.

These priorities filter into other security initiatives an organization has implemented, whether for regulatory compliance or other reasons. They inform every aspect of Incident Response, such as the roles and responsibilities each stakeholder assumes and the specific tactics used to identify, quarantine, eliminate, and recover from an attack or other incident in real-time.

Seven Phases of Incident Response

Just as every IRP will target a unique set of priorities catering to an organization's needs, the same goes for how Incident Response plays out in action. Nevertheless, most effective Incident Response programs follow a similar structure. RSI Security uses a seven-phase approach:



Seven Phases of Incident Response

PHASE 1:
Preparation

Intelligence gathering to increase your organization's awareness of existing and potential security threats and vulnerabilities.

Preparation activities include:

- Risk assessments
- Tabletop exercises

PHASE 2:
Detection

Continuous monitoring to scan for and identify actualized threats as they appear, setting risk mitigation protocols into action.

PHASE 3:
Containment

Immediate response to reduce or cease the spread of the attack, minimizing the scope of systems and data impacted.

PHASE 4:
Investigation

Root cause analysis (RCA) identifies what led to the incident occurring, how, and when, to prevent any follow-up and future attacks.

PHASE 5:
Eradication

Complete elimination of all malicious files or operations, except any trace specimens that are to be preserved for forensic analysis.

PHASE 6:
Recovery

Returning systems and data to their safe states prior to the incident, either by restoring backups or creating new secure locations.

PHASE 7:
Follow-up

Testing systems to ensure post-incident security meets or exceeds its pre-incident levels—and feeding back into preparation.

Other organizations may use a simpler or more complex model. For example, the National Institute for Standards and Technology (NIST) recommends a four-phase protocol that collapses detection and investigation into one phase, and containment, eradication, and recovery into another consolidated phase. We find that treating each process as distinct is the most effective approach.

Incident Response Tabletop Exercises

The most effective Incident Response Planning and Incident Management programs have one thing in common: they all integrate Incident Response into employee awareness training.

All incoming staff should be apprised of their roles and responsibilities in the event of an attack, breach, or other cybersecurity incident. Beyond onboarding, all staff should be subject to regular training modules and assessments that gauge their readiness and preparedness for an event.

One of the best approaches to test readiness involves Incident Response Tabletop Exercises.

IR Tabletop Exercises are controlled, live simulations that allow employees to practice their communication, logging, analysis, mitigation, and other Incident Response tactics. They allow for near-infinite repetition of an entire scenario or individual parts within it, for granular insights.

Use Cases for IR Tabletop Exercises

IR Tabletop exercises are closely related to penetration testing, which simulates a full-scale attack on your organization. They operate on a smaller scale for greater volume and variety. And, like penetration tests, these exercises can be implemented on any system or asset.

Three common IR Tabletop Exercise scenarios every organization should run regularly are:

Malware Attack Scenarios

Malware and related attacks (ransomware, etc.) are among the most common cybersecurity incidents faced by all organizations. Tabletop exercises can help employees identify and respond to targeted campaigns effectively.

Cloud Vulnerability Scenarios

As more organizations migrate more of their data storage and processing into the cloud, new threats and weaknesses become apparent every day. Tabletop exercises test secure behavior across the cloud and edge devices.

Network Breach Scenarios

When cybercriminals gain illegitimate access to your network, they can compromise any asset connected to it. Tabletop exercises can help employees understand what a breach looks like and how to respond to it in real-time.

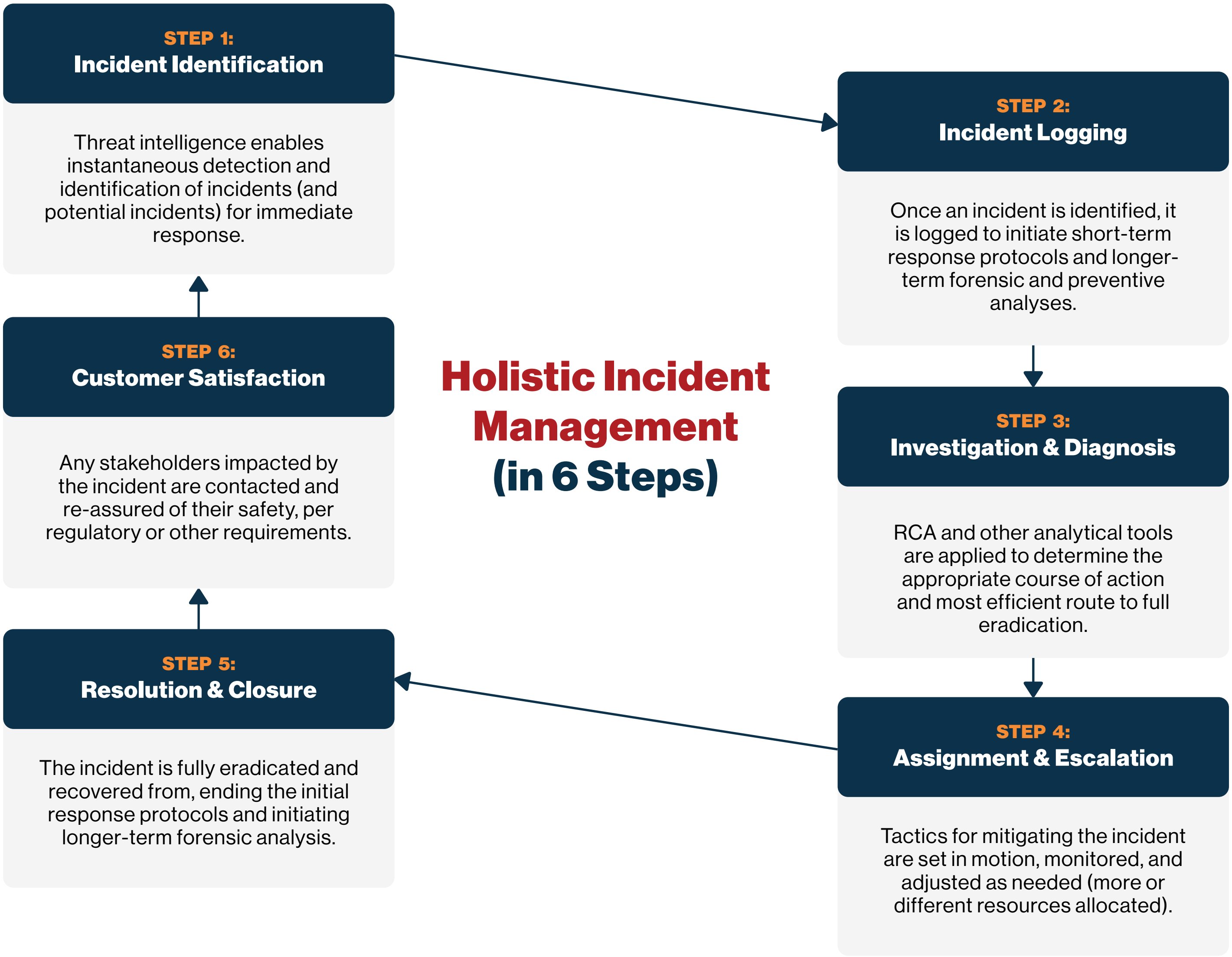
NOTE: These are not the only kinds of incidents organizations should test for; other critical ones include physical breaches and internal threat actors such as disgruntled current or former staff.

To get the most out of an IR Tabletop Exercise, consider partnering with a service provider like RSI Security, who will tailor the scenario to the specifications of your IRP and IT environment.

Holistic Incident Management (in Six Steps)

Incident Response is primarily focused on dealing with incidents in real-time as they occur. But a broader area of cybersecurity program development is Incident Management, which takes a longer-term view and emphasizes pre-incident prevention and post-incident remediation.

The most effective Incident Management programs follow a six-step approach:



Holistic Incident Management (in 6 Steps)

STEP 1:
Incident Identification

Threat intelligence enables instantaneous detection and identification of incidents (and potential incidents) for immediate response.

STEP 2:
Incident Logging

Once an incident is identified, it is logged to initiate short-term response protocols and longer-term forensic and preventive analyses.

STEP 3:
Investigation & Diagnosis

RCA and other analytical tools are applied to determine the appropriate course of action and most efficient route to full eradication.

STEP 4:
Assignment & Escalation

Tactics for mitigating the incident are set in motion, monitored, and adjusted as needed (more or different resources allocated).

STEP 5:
Resolution & Closure

The incident is fully eradicated and recovered from, ending the initial response protocols and initiating longer-term forensic analysis.

STEP 6:
Customer Satisfaction

Any stakeholders impacted by the incident are contacted and re-assured of their safety, per regulatory or other requirements.

RSI Security offers robust Incident Response Planning, IR Tabletop Exercises, and holistic Incident Management services to organizations of all sizes and across all industries.

RSI Security’s Incident Response and Incident Management Services

The experts at RSI Security have amassed decades of experience identifying, reacting to, and mitigating all kinds of cybersecurity incidents. Our suite of Incident Response services will streamline every part of the process, reducing the likelihood that an attack happens and minimizing the potential damage it can do to your organization and its reputation. We’ll help you rethink your Incident Response—and Management—and optimize your cyberdefenses.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com