AdverseMonitor

INCIDENT RESPONSE GUIDE

Data Breach Response Playbook

A step-by-step framework for detecting, containing, eradicating, and recovering from data breaches—plus regulatory compliance guidance.

Version 2.0 | December 2025

Table of Contents

Executive Summary

> When you discover a data breach, the first hours and days are critical. How you respond determines whether the incident becomes a contained security event or a catastrophic business failure.

$4.88M

Average cost of a data breach in 2024 (IBM)

$1.5M

Savings with IR team & tested plan

277

Average days to identify & contain

The 6-Phase Framework

This playbook follows the industry-standard incident response lifecycle:

Phase	Objective	Timeline
1. Detection	Confirm incident, assemble team, preserve evidence	Hours 0-4
2. Containment	Stop the bleeding, prevent spread	Hours 4-24
3. Eradication	Remove attacker presence completely	Days 1-7
4. Recovery	Restore operations safely	Days 7-30
5. Legal/Regulatory	Meet compliance obligations	Per regulation
6. Post-Incident	Learn and improve	Days 30-60

Key Insight: Organizations that detect breaches within 200 days save an average of $1.02 million compared to those taking longer. Early detection through dark web monitoring can cut detection time to minutes.

1 Phase 1: Detection & Initial Assessment

1 Confirm the Breach

Not every security alert is a breach. Before activating full incident response:

- □ Verify the legitimacy of the alert or report
- □ Gather initial evidence (logs, screenshots, alerts)
- □ Determine if this is a false positive or actual compromise
- □ Document the discovery time and method
- □ Classify severity: Critical / High / Medium / Low

2 Assemble the Incident Response Team

Immediately notify and convene your IR team:

Role	Responsibility
Incident Commander	Overall decision authority and coordination
IT/Security Lead	Technical investigation and remediation
Legal Counsel	Regulatory compliance and legal exposure
Communications	Internal and external messaging
Executive Sponsor	Business decisions and resources
HR (if needed)	Insider threat or employee notification

3 Preserve Evidence

Before making any changes to systems:

- □ Capture memory dumps from affected systems
- □ Export and preserve logs before rotation/deletion
- □ Take forensic images of compromised systems
- □ Document all actions taken (chain of custody)
- □ Screenshot dark web postings or threat actor communications

> **Critical:** Evidence preservation must happen BEFORE containment actions. Shutting down or reformatting systems destroys valuable forensic evidence.

2 Phase 2: Containment

4 Implement Short-Term Containment

Limit damage while maintaining evidence and business operations:

- □ Isolate affected systems from the network (don't power off yet)
- □ Block attacker IP addresses and C2 domains at firewall
- □ Disable compromised user accounts
- □ Force credential resets for affected accounts
- □ Increase monitoring and logging across all systems
- □ Implement emergency firewall rules if needed

5 Assess the Scope

Determine what was compromised by answering these questions:

- □ Which systems were accessed?
- □ What data was stolen, encrypted, or modified?
- □ How many records/users are affected?
- □ What was the initial entry point?
- □ How long did attackers have access?
- □ Are there additional persistence mechanisms or backdoors?
- □ Is data appearing on dark web leak sites?

6 Implement Long-Term Containment

Establish sustained defensive posture:

- □ Apply emergency patches to exploited vulnerabilities
- □ Force password resets for potentially compromised accounts
- □ Implement additional access controls and monitoring
- □ Segment network to prevent lateral movement
- □ Review and harden security configurations
- □ Deploy additional endpoint detection tools

Balance Speed with Thoroughness: Rushed containment without understanding scope often leads to incomplete remediation and re-infection.

3 Phase 3: Eradication

7 Remove Attacker Presence

Eliminate all attacker access and persistence mechanisms:

- □ Remove malware, ransomware, and hacking tools
- □ Delete unauthorized user accounts and backdoors
- □ Close exploited vulnerabilities through patching
- □ Reset all potentially compromised credentials
- □ Rebuild severely compromised systems from known-good backups
- □ Update endpoint protection signatures
- □ Block newly identified malicious indicators

8 Verify Complete Remediation

Ensure attackers cannot return:

- □ Conduct full security scans across environment
- □ Review logs for any remaining malicious activity
- □ Verify all backdoors and persistence mechanisms removed
- □ Test security controls are functioning properly
- □ Validate patches were applied correctly
- □ Confirm no unauthorized accounts remain

> **Don't Restore Yet:** Restoring from backups before completing eradication risks re-introducing the attacker's tools or restoring compromised data.

4 Phase 4: Recovery

9 Restore Operations

Safely return systems to production:

- □ Verify backups are not compromised before restoration
- □ Restore from clean backups or rebuild systems
- □ Implement additional monitoring on restored systems
- □ Gradually bring systems back online with validation
- □ Monitor closely for signs of re-infection (48-72 hours minimum)
- □ Validate business operations are functional

Restoration Priority Order:

1. Critical infrastructure (authentication, DNS, network)
2. Business-critical applications
3. Customer-facing services
4. Internal productivity tools
5. Non-essential systems

10 Implement Enhanced Security

Don't just return to the previous state—improve defenses:

- □ Address vulnerabilities that enabled the breach
- □ Implement recommendations from IR investigation
- □ Deploy additional security controls and monitoring
- □ Update incident response procedures based on lessons
- □ Consider additional security investments (EDR, SIEM, etc.)
- □ Implement dark web monitoring for early threat detection

5 Phase 5: Regulatory & Legal Response

11 Determine Notification Requirements

Work with legal counsel to understand your obligations:

Regulation	Notification Window	Triggers
GDPR	72 hours	EU personal data affected
HIPAA	60 days / Immediately if 500+	PHI breach
PCI DSS	Immediately	Cardholder data compromised
US State Laws	Varies (24 hrs - 90 days)	State resident PII
SEC Rules	4 business days (Form 8-K)	Material incident

12 Notify Affected Parties

When required, notify promptly and transparently:

- □ Regulatory authorities within required timeframes
- □ Affected customers/users with clear, honest communication
- □ Credit monitoring services if financial data compromised
- □ Law enforcement (FBI IC3, local cybercrime units)
- □ Cyber insurance provider (required for claim)
- □ Business partners if their data was affected

13 Manage External Communications

Control the narrative and maintain trust:

- □ Prepare holding statement for media inquiries
- □ Update website with incident information (if required)
- □ Designate single spokesperson for all media contacts
- □ Monitor social media and news coverage
- □ Provide regular updates as investigation progresses

6 Phase 6: Post-Incident Activities

14 Conduct Post-Incident Review

Within 2-4 weeks after containment, hold a blameless retrospective:

- □ Document complete timeline of events
- □ Identify what happened and how it happened
- □ Analyze why existing controls didn't prevent/detect it
- □ Identify what worked well in the response
- □ Identify what didn't work or caused delays
- □ Create prioritized remediation roadmap
- □ Update incident response plan based on lessons

15 Implement Long-Term Improvements

Turn the incident into organizational resilience:

- □ Address root causes identified in post-incident review
- □ Implement approved security improvements
- □ Update security policies and procedures
- □ Provide additional training to staff
- □ Conduct penetration testing to validate improvements
- □ Schedule tabletop exercises quarterly
- □ Review and update cyber insurance coverage

Continuous Improvement: Every breach is a learning opportunity. Organizations that conduct thorough post-incident reviews become significantly more resilient.

Quick Reference: First 24 Hours

Hour 0-1

- □ Confirm breach is real (not false positive)
- □ Activate incident response team
- □ Begin evidence preservation
- □ Notify IT/Security leadership

Hours 1-4

- □ Complete initial evidence collection
- □ Begin short-term containment
- □ Isolate affected systems
- □ Block known malicious indicators
- □ Notify legal counsel

Hours 4-12

- □ Complete scope assessment
- □ Identify affected data types and volume
- □ Determine regulatory notification requirements
- □ Engage external IR firm if needed
- □ Brief executive leadership

Hours 12-24

- □ Implement long-term containment
- □ Begin eradication planning
- □ Prepare customer/regulatory notifications
- □ Contact cyber insurance provider
- □ Prepare external communications

Critical Mistakes to Avoid

Don't Delete Evidence — Shutting down or reformatting systems before forensics destroys critical evidence needed for investigation and legal proceedings.

Don't Go Dark — Failing to communicate with stakeholders creates speculation, erodes trust, and can make the situation worse.

Don't Pay Ransoms Without Consultation — Payment doesn't guarantee data return, may violate OFAC sanctions, and funds criminal enterprises.

Don't Miss Notification Deadlines — Regulatory penalties for late notification can exceed the cost of the breach itself.

IR Contact Information Template

Complete this template **BEFORE** an incident occurs:

Internal Team

Role	Name	Phone
Incident Commander		
IT/Security Lead		
IT/Security Backup		
Legal Counsel		
Communications/PR		
CEO/Executive Sponsor		
CFO		
HR Director		

External Partners

Organization	Contact	Phone/Email
Cyber Insurance		
IR/Forensics Firm		
Outside Legal Counsel		
PR/Crisis Communications		
FBI Cyber Division	ic3.gov	
Local FBI Field Office		

Early Detection Saves Millions

AdverseMonitor alerts you within minutes when your organization appears on dark web leak sites—giving you critical early warning to contain breaches faster.

platform.adversemonitor.com/signup

AdverseMonitor

This playbook is provided for educational purposes. Consult with qualified professionals for your specific situation.