

# RESILIENTLY

Cybersecurity made clear.

## Post-Breach Lessons Learned

A structured template for conducting post-incident reviews, documenting findings, and tracking remediation.

## Incident Overview

Incident ID/Name

Incident Date(s)

Date Detected

Date Contained

Date Resolved

Incident Classification

Severity Level

## Review Participants

List all participants in this lessons learned review. Include representatives from all teams involved in the incident response.

Name	Role/Department	Involvement in Incident

## 1. Incident Summary

Brief description of what happened

Attack vector / Initial compromise method

Systems/Data affected

Business impact (operational, financial, reputational)

## 2. Timeline of Events

Document the key events in chronological order. Be as specific as possible with times.

### 3. Root Cause Analysis

Identify the underlying causes that allowed this incident to occur. Use techniques like '5 Whys' to get to root causes, not just symptoms.

## Technical root cause(s)

1. *What is the primary purpose of the study?*

### Process/procedural root cause(s)

1. **What is the primary purpose of the proposed legislation?**

Human factors

Contributing environmental factors

## 4. What Went Well

Document aspects of the response that were effective. These are practices to maintain and build upon.

### **Detection**

Effective detection practices

### **Response**

Effective response practices

### **Communication**

Effective communication practices

### **Recovery**

Effective recovery practices

## 5. Areas for Improvement

Document gaps, challenges, and areas where the response could have been more effective.

### **Detection Gaps**

**What detection capabilities were missing or delayed?**

### **Response Challenges**

**What response challenges were encountered?**

### **Communication Issues**

**What communication problems occurred?**

### **Resource/Tool Gaps**

**What resources or tools were needed but unavailable?**

## 6. Recommendations

Based on the analysis, document specific recommendations for improvement.

### **Immediate Actions (0-30 days)**

**Quick wins and critical fixes**

## **Short-term Actions (30-90 days)**

Important improvements requiring planning

## **Long-term Actions (90+ days)**

Strategic initiatives and investments

## **7. Action Item Tracker**

Track all remediation actions resulting from this review. Review progress regularly until all items are complete.

Action Item	Owner	Priority	Due Date	Status

## 8. Policy & Procedure Updates

Policies requiring update

Procedures requiring update

Incident response plan changes needed

Training requirements identified

## 9. Sign-Off

This lessons learned review has been completed and the findings/recommendations are accepted.

Security Lead Name & Signature

IT Lead Name & Signature

Executive Sponsor Name & Signature

Review Completion Date

Next Review/Follow-up Date