Breach Response Plan Template for Small & Medium Businesses

A ready-to-use framework for faster, smarter incident handling.

First 30 Minutes of Cyber Breach

The first half hour of a breach often feels chaotic—phones ringing, Slack blowing up, people shouting “Pull the plug!” That’s exactly when mistakes can make things worse. Here’s how to stay grounded:

- **Pause Before Acting:** Don’t panic, shut down servers or wipe machines. Quick reactions can destroy critical evidence.
- **Isolate Calmly:** Disconnect only the affected system from the network (not the whole office Wi-Fi), so attackers can’t move further.
- **Escalate to the Right Person:** Immediately notify your designated incident lead (not “everyone in the company”). Having one point of contact avoids rumor-storms.
- **Capture the Moment:** Take screenshots, preserve logs, and write down what’s happening. These raw details are gold for investigators.
- **Controlled Communication:** Inform senior management that *“a potential breach is under review”*—short, factual, and no blame. Avoid mass announcements until facts are confirmed.

The first 30 minutes are about *stopping the chaos from spreading faster than the breach itself*. Calm isolation, clean evidence, and clear escalation set the tone for the entire response.

Template Sections

1. Preparation

- Define key contacts:
    - ☐ Security lead: [Name/Contact]
    - ☐ IT team: [Name/Contact]

- ☐ Legal advisor: [Name/Contact]
- ☐ PR/Communications: [Name/Contact]

Ensure vendor contracts require **breach notifications** within [X hours].

2. Detection & Identification

- ☐ How was the breach detected (tool, vendor alert, employee report)?
- ☐ What systems/data are potentially affected?
- ☐ Confirm severity level: Low / Medium / High / Critical

3. Containment

- ☐ Isolate compromised systems immediately.
- ☐ Disable affected vendor accounts or integrations.
- ☐ Preserve logs and forensic data for investigation.

4. Eradication & Recovery

- ☐ Remove malware, unauthorized access, or faulty API connections.
- ☐ Patch exploited vulnerabilities.
- ☐ Restore systems from backups.
- ☐ Monitor for recurrence.

5. Post-Incident Review

- ☐ Document the timeline of events.
- ☐ Identify root cause (vendor failure, internal misconfig, etc.).
- ☐ Update security policies and vendor requirements.
- ☐ Conduct a lessons-learned workshop within 7 days of breach closure.

Communication Plan

- **Vendors/Partners:**
  "We have identified a potential security incident. While investigations are ongoing, we are taking precautionary steps. We will update you within [X] hours."

- **Customers:**
  "Your security is our priority. We recently detected suspicious activity affecting [describe system minimally]. At this time, no [or specify] customer data is confirmed to be impacted. We are working with security experts and will provide updates every [X] hours."

- **Internal Stakeholders & Managers:**
  "A security incident has been detected on [system]. Investigation is underway, evidence preserved, and containment in progress. Next update at [time]. Please do not share externally until official communication is released."

- **Regulators (if required):**
  Short compliance-focused message including: incident detected, scope, actions taken, and following update timeline.