FusionRed®

Cyber Incident Response Checklist

A complete guide of what you should do IMMEDIATELY after experiencing a cyberattack.

Downloading this document to your device is highly recommended

Table of Contents

I.

Introduction

FusionRed®

I. Introduction

What it looks like: First few hours of being attacked

When a cyberattack hits, confusion spreads faster than the breach itself. Systems go offline, teams scramble, and decisions must be made, fast! For small to mid-sized businesses (SMBs), this moment is often the difference between recovery and ruin.

Unlike large enterprises, SMBs often lack internal incident response teams or formal playbooks. That leaves business leaders in reactive mode, guessing what to do next, second-guessing every decision, and hoping they've contained the damage.

How this guide will help you

hope is not a strategy. That's why this checklist exists. It's a practical, no-fluff guide for what to do in the critical hours and days following a cyberattack. Whether it's ransomware, business email compromise, or a data breach—this resource is designed to help you move from panic to control.

Use this checklist to:

- Regain control quickly and efficiently
- Minimise business downtime and financial loss
- Preserve evidence for legal, regulatory, and insurance purposes
- Avoid common mistakes that worsen the damage

II.

Checklist: Complete incident response for SMBs

FusionRed®

II. Checklist: Complete incident response for SMBs

Phase 1: Immediate Containment

- [ ] **Activate Your Incident Response Plan (& Assign Response Leader)**

  Kickstart your documented plan and immediately assign who will lead the response. Ownership is critical from minute one.

- [ ] **Isolate Affected Systems**

  Disconnect infected devices and servers from your network. This will stop the attacker from causing further damage.

- [ ] **Identify the Type and Scope of Attack**

  Know whether it's ransomware, credential theft, etc. Your response steps depend on the kind of breach you're dealing with.

- [ ] **Engage IT or Your Cybersecurity Provider**

  Bring in your IT team or managed service provider immediately. The faster you escalate, the more you can control the spread.

- [ ] **Document Everything**

  Log what's been affected, when it was discovered, and who did what. You'll need this for insurance claims, &compliance reporting.

Phase 2: Stabilisation & Communication

- [ ] **Communicate Internally (Smartly)**

  Inform your team with calm, clear, need-to-know details. Avoid chaos and misinformation. Panic spreads faster than facts.

- [ ] **Notify Key Stakeholders**

  Depending on the attack, inform customers, partners, or legal counsel. Transparency builds trust, silence can destroy it.

- [ ] **Conduct a complete cybersecurity assessment**

  Let experts trace the breach, determine how it happened, and whether it's ongoing. Without this, you risk reopening the door to the same attacker.

Phase 3: Recovery & Learning

- [ ] **Reset Access Credentials**

  Update passwords, revoke compromised accounts, and implement MFA. Credentials are a hacker's golden key. Don't let them keep it.

- [ ] **Begin Recovery and Restoration**

  Use clean backups to restore critical systems, double-check configurations. Rushing recovery without verifying can reintroduce the breach.

- [ ] **Report the Breach (MUST)**

  Notify regulators, cyber insurers, or industry bodies per compliance laws. Failure to report can lead to legal trouble or insurance denials.

- [ ] **Conduct a Post-Incident Review**

  Debrief what happened, what went wrong, and how to improve. This is where prevention begins, by learning from failure.

III.

Taking Action

FusionRed®

III. Taking Action

Most SMBs Don’t Get a Second Chance

Here’s the truth: a cyberattack is rarely a one-time event. Many businesses get hit again (harder), because they never addressed the gaps that let the first one in.

The cost of getting it wrong? It goes beyond downtime. We’re talking lost clients, reputational damage, compliance penalties, insurance denials, and in some cases, complete shutdown.

That’s why FusionRed offers a free 1:1 consultation with cybersecurity experts. We’ll walk through your current response capability, identify your blind spots, and show you how to strengthen your defences, proactively.

Exclusive
FREE CONSULTATION

Schedule a free consultation today and take the first step toward securing your business.

Click the button below to schedule a call

Contact Us Now


FusionRed®