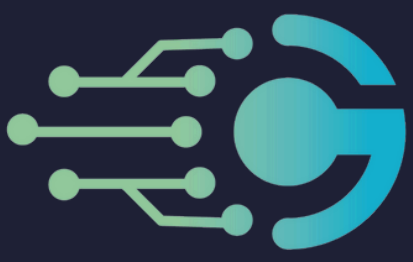
GUIDE

Incident Response Playbook Template

A Step-by-Step Guide for Financial Services, Law Firms, Accountants, and Estate Agents



Chapman Technology Partners

Why Every Regulated Firm Needs an Incident Response Playbook

When a cyber incident strikes - from a phishing attack to a ransomware breach - the first few hours are critical.
Without a clear, structured plan, chaos and confusion can quickly lead to data loss, reputational damage, and FCA compliance breaches.

An Incident Response Playbook gives your firm the confidence and control to act fast, contain damage, and recover operations safely.
At Chapman Technology Partners, we help firms across the UK design and test tailored response playbooks — ensuring readiness before disaster strikes.

> "Speed and structure make all the difference during an incident. A well-rehearsed playbook turns a crisis into a controlled process."
>
> Greg Chapman, MD Chapman Technology Partners

Section 1: What Is an Incident Response Playbook?

An Incident Response Playbook is a structured document outlining who does what, when, and how during a cyber incident.

It defines clear escalation paths, roles, and communication plans, enabling your team to respond decisively and in compliance with sector regulations.

Core objectives:

- Minimise damage and downtime
- Protect client data and business reputation
- Maintain FCA, SRA, or ICO compliance
- Restore systems and evidence for investigation

Section 2: The Six Phases of Incident Response

1 Preparation
Build the foundation: define your response team, establish contact lists, and conduct regular security training.

2 Identification
Detect and verify incidents using monitoring tools, threat detection, and user reports.

3 Containment
Isolate affected systems to stop the spread of malicious activity.

4 Eradication
Remove malware, revoke compromised credentials, and patch vulnerabilities.

5 Recovery
Restore clean backups, validate systems, and resume normal operations safely.

6 Lessons Learned
Conduct a post-incident review to strengthen your cyber resilience.

Section 3: Template Walkthrough

Use this structure to create your own playbook:

Section	Details
1. Incident Classification	Define severity levels (Low, Medium, Critical) and response triggers
2. Roles & Responsibilities	Identify team members (IT, Legal, HR, Management, PR)
3. Communication Plan	Outline internal/external notification protocols, including FCA/SRA timelines
4. Technical Procedures	Include system isolation, log preservation, and forensic steps
5. Recovery Checklist	List steps for restoring services and confirming system integrity
6. Post-Incident Review	Capture learnings, update controls, and schedule future tests

Section 4: Aligning Your Playbook with FCA Requirements

The FCA expects regulated firms to maintain robust operational resilience and report material cyber incidents promptly.

Your playbook should:

- Include clear FCA reporting procedures
- Record decision-making timelines
- Demonstrate proactive cyber risk management

Learn more via the Financial Conduct Authority (FCA) website.

Section 5: How Chapman Technology Partners Can Help

Our cyber security experts can:

- Assess your current incident readiness
- Design a tailored playbook aligned with your sector's regulations
- Conduct live tabletop exercises to test your team's response
- Provide ongoing monitoring and rapid response support

> "We've helped firms move from reactive firefighting to proactive cyber resilience."
>
> Greg Chapman, MD Chapman Technology Partners

Next Steps

Building cyber resilience takes more than a template — it takes practice. Chapman Technology Partners can help you review your IT setup, test your response plan, and strengthen your defences.

Book your free 15 minute intro call here and let's discuss how we can help ensure your business can respond fast and recover stronger.

www.chapmantechnologypartners.co.uk

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions for Regulated Firms

Strawberry Fields Digital Hub,
Chorley, PR7 1PS

enquiries@ctpartners.co.uk
01257 542388

CYBER ESSENTIALS CERTIFIED