5 MUST HAVES FOR IT INCIDENT RESPONSE PLAN.

DATA SECURITY
A UBDS GROUP COMPANY

An Incident Response Plan is your structured framework for identifying, managing, and recovering from technology-related disruptions – from ransomware and insider threats to outages and supply-chain compromises.

1 Defined Roles & Responsibilities

When an incident hits, there's no time to figure out "who does what."

The faster you mobilise the right people the less damage you will suffer.

Form a cross-functional Incident Response Team (IRT) with designated roles

- INCIDENT LEAD
- TECHNICAL LEAD
- LEGAL LIAISON
- COMMUNICATIONS MANAGER

Maintain up-to-date contact lists for

- INTERNAL TEAMS
- VENDORS
- REGULATORS

2x Conduct simulation exercises in a year to validate readiness and coordination.

Develop a RACI matrix for different incident categories.

RESPONSIBLE	ACCOUNTABLE
CONSULTED	INFORMED

2 Early Detection & Continuous Monitoring

If you don't detect the incident early, your response is delayed and the cost rises.

- Deploy SIEM and IDS to monitor security data across your IT environment.
- Set escalation thresholds and automated response triggers.
- Integrate threat intelligence feeds for proactive awareness.
- Regularly audit your detection systems and review logs for unusual activity.

3 Incident Classification & Prioritisation

Not all incidents are equal. Some are minor; others are catastrophic. You need to prioritise to allocate your resources effectively.

Establish severity tiers

Low ---> Critical

based on business impact.

- Define response time objectives for each tier.
- Link classification to escalation levels and executive involvement.
- Periodically review and adjust based on lessons learned from prior incidents.

4 Clear Communication Channels

In an incident you will need to coordinate among technical teams, business leadership, customers, regulators, and the public. Poor communication creates confusion, missed obligations (e.g., breach notification laws) and reputational harm.

- Prepare pre-approved communication templates for internal updates, regulatory notifications, and customer messages.
- Ensure clarity around who can authorise external statements.
- Maintain direct contact points with the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC).
- Run crisis communication drills simulating both internal and external scenarios.

5 Recovery & Continuous Improvement

The goal is not just to stop the incident, but to restore normal operations and learn to become stronger afterward. An IRP without recovery & review is incomplete.

- Define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical systems.
- Verify backup integrity and restoration processes through testing.
- Conduct post-incident reviews and document findings in a centralised incident register.
- Update your IRP based on evolving threats and technology trends.

DATA SECURITY
A UBDS GROUP COMPANY

+44 (0)1223 298333
+44 (0)1223 298338

Info@3BDataSecurity.com
IR@3BDataSecurity.com

Our Services

> Incident Response
> Penetration Testing
> Training Courses
> Information Security
> Digital Forensics
> Managed Services