

## The questions to ask your Incident Response Team

In order for an incident response (IR) team to identify, investigate and respond to a cyber incident effectively, it needs a formally approved Incident Response Policy supported by a documented Incident Response Plan and detailed playbooks or procedures. Like a fire drill, a predetermined plan can help cut through the chaos if the worst happens.


The following structured questions can be used to develop robust business-aligned incident response procedures and operational checklists.


- What types of events are considered incidents?
- Who identifies an incident?
- How is an incident identified?
- What is the acceptable interruption window?
- Who is the Incident Manager during an incident?
- What are the expectations for receiving and sending updates to and from the Incident Manager?
- Who are the organisation's primary IR team members?
- Who are the secondary IR team members?
- Who are the IR escalation contacts?
- What is the internal communication plan?
- What are the extended communication plans with providers?
- What is the alternative communication plan if the attack disables regular means of communication (email, phone, conference bridge availability)?
- What types of information does the company have and what are the disclosure requirements for each type?
- When should the legal team get involved and who makes that decision?
- Is there a plan to coordinate the internal IR team, partners, vendors and legal to a conference bridge in the event of an incident?

These questions are just the tip of the iceberg. For help implementing a **purpose-built incident response plan prepared with your business in mind**, contact the BAE Systems Incident Response team

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: [learn@baesystems.com](mailto:learn@baesystems.com) | W: [baesystems.com/digital](https://www.baesystems.com/digital)

 [linkedin.com/company/baesystemsdigital](https://www.linkedin.com/company/baesystemsdigital)

 @BAESystemsDigi



Assured Service Provider



In association with  
National Cyber  
Security Centre

**Victim of a cyber attack?**

**Contact our emergency response team on:**

UK & International: +44 330 158 5263

Email: [cyberresponse@baesystems.com](mailto:cyberresponse@baesystems.com)