

10 Steps to an Effective Cyber Breach Response for Large Organisations



1. Appoint a member of senior management who can agree key decisions up front, before they need to be made
2. Appoint a triage officer who will evaluate suspected incidents, decide the scale of response required, and appoint an incident lead
3. Create a set of step by step guidelines for dealing with different types and severities of breaches
4. Appoint a multi-functional Incident Response Team (IRT) including people from finance, legal, HR and marketing, as well as security and IT
5. Share the contact details of the IRT (and their deputies) with the triage officer and the senior management representative
6. Create a call list of external specialists including legal advisors, PR advisors, and technical and cyber forensics specialists
7. Identify the most likely scenarios for breaches and mitigate them by reducing their likelihood or likely impact
8. Pre-plan your responses to the most likely breaches by creating template internal and external communications
9. Regularly train the members of your IRT in the use of the step by step guidelines by running realistic breach scenarios
10. Agree a process for learning from breaches that will feedback into and improve the step by step guidelines

For an in-depth exploration of cyber breach responses and to experience a cyber breach simulation, consider attending our [Cyber breach response workshops](#) which take place regularly throughout the year.