

Cyber security incident: Checklist for data security and protection leads

Version 1 – October 2024

**Data security and protection leads can use the ten questions below to find out what’s happened during a** [**cyber security incident**](http://www.digitalcarehub.co.uk/cyber-security)**. It’s a starting point that you can use to gather vital information as soon as you suspect something has gone wrong.**

**It should be used in conjunction with your** [**business continuity plan**](https://www.digitalcarehub.co.uk/data-security-protecting-my-information/businesscontinuity/) **– it should not replace it.**

**Date completed:**

**Completed by:**

1. What problem has been reported, and by whom?
2. What services, programs and/or hardware are affected or aren’t working?
3. Are there any signs that data has been lost? For example, have you received ransom requests, or has your data been posted on the internet?
4. What information (if any) has been shared with unauthorised parties, deleted or corrupted?
5. Have your stakeholders (such as people who draw on care services or partner organisations) noticed any problems? Can they use your services?
6. Who designed the affected system(s), and who maintains it?
7. When did the problem occur or first come to your attention?
8. What is the scope of the problem, what areas of the organisation are affected?
9. Have there been any signs as to whether the problem has occurred internally within your organisation or externally through your IT supply chain?
10. What is the potential business impact of the incident?