# Activity sheet 3.27: What to do after an attack

*Learning outcome B: Cyber security*

*B3: Policy*

You work at a marketing agency. Your office has recently experienced several cyberattacks.

For each scenario below:

* identify the type of attack
* assess the severity of the attack on a scale of 1 to 5 (1 = low impact, 5 = high impact); give reasons for your assessment
* explain which services or processes within the agency will be affected
* explain which stakeholders should be informed of the attack
* explain what action the agency should take to recover from the attack.

1. A hacker has gained unauthorised access to files you created for a high-profile client’s launch of a new product.
   1. Type of attack:
   2. Severity of the attack (1 to 5):
   3. Reason:
   4. Affected services:

* 1. Stakeholders to be informed:

* 1. Actions the agency should take:

1. A remote server has bombarded the agency’s websites with data requests that has caused the website to crash.
   1. Type of attack:
   2. Severity of the attack (1 to 5):
   3. Reason:
   4. Affected services:

* 1. Stakeholders to be informed:

* 1. Actions the agency should take:

1. A member of staff has responded to an email that asked them to provide their username and password. The staff member thought the email was from the IT manager but it appears that the email account used was not one controlled by an agency employee.
   1. Type of attack:
   2. Severity of the attack (1 to 5):
   3. Reason:
   4. Affected services:

* 1. Stakeholders to be informed:

* 1. Actions the agency should take:

1. A security sweep carried out by the IT manager has discovered key-logging software installed on a computer used by the agency’s finance officer. The finance officer uses the computer to log into and manage the agency’s bank accounts.
   1. Type of attack:
   2. Severity of the attack (1 to 5):
   3. Reason:
   4. Affected services:

* 1. Stakeholders to be informed:

* 1. Actions the agency should take:

**Take it further**

Review a recent cyberattack and the response of the organisation affected.

To what extent did the organisation respond appropriately and effectively?

Suggest improvements to how the organisation responded.