SCVO CyberScotland

Responding to a cyber incident:

If a cyber incident is happening you might notice things like:

- Computers running slowly
- Users being locked out of their accounts
- Users being unable to access documents
- Redirected internet searches
- Unusual account activity
- Messages demanding a ransom for the release of your files
- People informing you of strange emails coming from your email addresses
- Requests for unauthorised payments

If you think there's been a cyber incident

Don't panic!

Try to work out what's happening

Work with your IT owner or provider to:

→ categorise the problem.

→ work out how severe it is.

→ understand the impact of it.

→ Analyse the problem to work out what is happening and how it can be contained or fixed, then prioritise these tasks.

STEP 1

□ Report it

If you confirm there's been a cyber incident, report it to Police Scotland by calling 101.

Report the incident to OSCR using their concern form – https://www.oscr.org.uk/raise-a-concern

If there has been a personal data breach, your Data Protection Officer should report it to the Information Commissioner's Office within 72 hours – **https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach**

STEP 2

□ Gather your team

Use the contacts list on page 2, assign responsibilities and engage external support where needed.

Getting support

Contact the Cyber Incident Response & Recovery Helpline: **0800 1670 623** (Weekdays 9am-5pm) for support during an incident.

Go to **www.cyberscotland.com/organisations/third-sector** for a supporting guide on how to respond to an incident.

You can also contact your insurance provider if you have cover that includes cyber support.

STEP 3

□ Manage the incident

Incident management should continue throughout the incident response process, until the incident is resolved.

Track the response
Track what happens and what you do - particularly in cases that might need to be reviewed by regulators or the police.

Keep everyone updated
Regularly report on the issue and how the incident response is going. Maintain regular comms with key contacts and those affected. You might also want to contact the media or send a press release out about the incident.

Make sure it's being properly responded to
Ensure the full incident response plan is followed, co-ordinating response actions and supporting where required.

STEP 4

□ Respond to the incident

1 Contain the problem
If it's safe to do so, take steps identified to contain the incident, reduce its impact and stop things getting worse.

2 Solve the problem
Fully remove the threat from your network and systems. This might mean monitoring the problem for a while before you move on to the next stage.

3 Recover your systems and data
Once you're sure the problem is resolved, return everything to business as usual. Put systems back online (make sure they're not compromised) and recover any data.

You did it! Here's what to do next

→ Review what you learned from the incident itself with your key contacts and anyone else who worked on the problem, as well as how the response went.

→ Use what you learn when reviewing the incident to update your plan if needed, and make changes at your organisation to stop similar issues happening again.

SCVO CyberScotland

Preparing for a cyber incident:

Work together to complete in advance. Maintain and test this plan regularly, and store it securely.

Your contacts

Depending on your organisation, one person might be responsible for multiple areas, and some of your contacts could be external providers.

Your CEO

Responsibilities

→ Preparing for a cyber incident
→ Leading and managing incident response

Name

Phone

Deputy's name

Deputy's phone

Your Insurance provider

Responsibilities

→ Supporting incident response (depending on your policy)

Name

Phone

Deputy's name

Deputy's phone

Your IT owner

Responsibilities

→ Supporting incident preparation and identification
→ Containing and solving the problem
→ Recovering systems and data

Name

Phone

Deputy's name

Deputy's phone

People responsible for supporting incident response and preparation

Your Comms owner

Name

Phone

Deputy's name

Deputy's phone

Your Legal owner

Name

Phone

Deputy's name

Deputy's phone

Your HR owner

Name

Phone

Deputy's name

Deputy's phone

Your Finance owner

Name

Phone

Deputy's name

Deputy's phone

Have you considered...

- □ What is covered in your insurance policy and IT contracts?
- □ How you would run your business offline?
- □ Do staff and volunteers understand their responsibilities?
- □ Whether you're protected against common cyber threats?
- □ What your incident response comms might look like?
- □ What's important to your business?
- □ How you would respond to an incident offline?
- □ How you would communicate offline?
- □ Who you might have to communicate to?

Notes