A BRIEF GUIDE TO
RESPONSE & RECOVERY
FOR SMALL BUSINESSES

1 Prepare for Incidents

To develop detailed instructions to manage every type of incident would be highly impractical.

Develop plans to handle incidents that are likely to occur.

The following considerations will assist in the development of robust incident plans:

- Identify critical electronic information.
- Make a regular daily/weekly backup copy of essential information.
- Make a list of key staff and stakeholders.
- Assign joint (or shared) responsibility.
- Put risk on the agenda.
- Make an incident plan.
- Test your staff's understanding of recognising incidents.
- Document contact details of external people who can help you identify or assist with an incident.

2 Identify What's Happening

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

The following may indicate a cyber-incident:

- Computers running slowly.
- Users locked out/unable to access documents.
- Messages demanding a ransom.
- Strange emails coming out of your domain.
- Redirected internet searches.
- Requests for unauthorised payments.
- Unusual account activity.

After an incident has been identified initial actions may include:

- Analysing anti-virus/audit logs to help identify the cause of the incident.
- Using anti-virus software to complete a full scan, and research any findings using trusted sources (such as police/security websites).

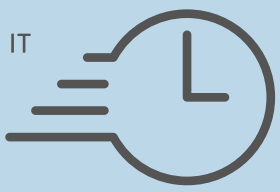
These 10 questions can help you identify what has occured:

1. What problem has been reported, and by who?
2. What services, programs and/or hardware aren't working?
3. Are there any signs that data has been lost?
4. What information has been disclosed, deleted or corrupted?
5. Have your customers noticed any problems? Can they use your services?
6. Who designed the affected system, and who maintains it?
7. When did the problem occur or first come to your attention?
8. What areas of the organisation are affected?
9. Is your external supply chain the cause and/or affected?
10. What is the potential business impact of the incident?

3 Resolve the Incident

It's important to take action as quickly as possible in order to mitigate and/or eradicate issues caused by the incident.

If your IT is managed externally, contact your IT advisers. If you manage your own IT, activate your incident plan.



This may involve:

- Replacing infected hardware.
- Restoring services through backups.
- Patching software.
- Cleaning infected machines.
- Changing passwords.

4 Report the Incident to Wider Stakeholders

You are legally obliged to report certain incidents to the ICO. Check their websites to find out which incidents qualify.

- Report to the Office of Cyber-Security and Information Assurance (OCSIA) and the Police using our cyber concern online reporting form found on www.gov.im/ocsia or by calling 686060.
- Keep your staff and customers informed of anything that might affect them (for example, if their personal data has been compromised by a breach).
- Consider seeking legal advice if the incident has had a significant impact on your business/customers. If you have cyber insurance, they will be able to provide you with more advice.

5 Learn from the Incident

Reviewing an incident after it has happened is important to learn from any mistakes and take actions to reduce the likelihood of it happening again.

- Review actions taken during response. Make a list of things that went well and things that could be improved.
- Review and update your incident plan to reflect the lessons learnt.
- Reassess your risk and make any necessary changes to your defences.

Office of Cyber-Security & Information Assurance
Ort son Shickyrys Lectraneagh as Sauyhys Fysseree

www.gov.im/ocsia
@cyberiom
IOM Government Office of Cyber-Security & Information Assurance

AWARE SECURE RESILIENT