National Cyber Security Centre
a part of GCHQ

Response & Recovery
Small Business Guide

This advice helps small-to-medium sized organisations prepare their response to and plan their recovery from a cyber incident. The 5 steps covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/response** .

1. Prepare for incidents

It's impractical to develop detailed instructions to manage *every* type of incident (the list could be endless), so develop plans to handle those incidents most likely to occur.

Identify critical electronic information such as contact details, emails, calendars, and essential documents. Find out where this information is stored. Identify the key systems and processes necessary to keep your organisation running. Record how they are accessed.

Make a regular daily/weekly back up copy of essential information. Regularly test that the backup is working to ensure you can restore information from it.

Make a list of the key partners (customers, suppliers, third parties, etc) that you would need to contact as a result of different types of incident.

Assign joint (or shared) responsibility amongst staff members to ensure there's cover when people aren't available. Ensure key documents are made available and are up to date.

Put risk on the agenda. What you value, and what you are doing to protect it, should be part pf your business-as-usual discussions at management meetings or weekly catch-ups.

Make an incident plan, and keep it safe so you can use it if your equipment is stolen or damaged by a cyber attack. Assign roles to members of staff, and document how and when they can be contacted.

Test your staff's understanding of what's required during an incident through exercising. Consider using the NCSC's free 'Exercise in a Box' product to test your organisation's resilience and preparedness.

Document contact details of external people who can help you identify an incident (such as your web hosting provider), and read contracts to know what's covered. Ensuring that all relevant details are accessible and up to date will be invaluable during 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**

These 10 questions can help you identify what occurred:
- **What problem has been reported, and by who?**
- **What services, programs and/or hardware aren't working?**
- **Are there any signs that data has been lost?**
- **What information has been disclosed, deleted or corrupted?**
- **Have your customers noticed any problems? Can they use your services?**
- **Who designed the affected system, and who maintains it?**
- **When did the problem occur or first come to your attention?**
- **What areas of the organisation are affected?**
- **Is your external supply chain the cause/affected?**
- **What is the potential business impact of the incident?**

Analyse antivirus/audit logs to help identify the cause of the incident. Use antivirus software to complete a full scan, and research any findings using trusted sources (such as police/security websites).

3. Resolve the incident

These actions will help your organisation get back up-and-running. You'll also need to check that everything is functioning normally, and fix any problems.

If your IT is managed externally, contact the right people to help (identified in Step 1). 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 website to find out which incidents qualify.

ico. Information Commissioner's Office

Report to law enforcement via Action Fraud or Police Scotland's 101 call centre. The more who report, the more likely it is that criminals will be arrested, charged and convicted.

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

After the incident, it's important to review what has happened, learn from any mistakes, and take action 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 (from Step 1) to reflect the lessons learned.

Reassess your risk and make any necessary changes to your defences.