

NOT IF, BUT **WHEN** **CYBER RESOURCE**

Practical Tips & Advice to Protect You &
Your Organisation from A Cyber Attack



Modern cyber attacks are **professionalised**. You are an **opportunistic** target - you can't predict what or when it's going to happen".

Jordan M. Schroeder
Managing Chief Information Security Officer, Barrier Networks

- Understand the risks & ensure the correct controls are in place. Ask:
- What **threats** do we face?
 - What **impact** will fall on our customers, stakeholders and staff?
 - What's the **plan** to mitigate the impact of each threat?
 - Have we **tested** the plan?
 - What **board support** do we need?

Lee Cramp
Deputy Director and Data Protection Officer, Department of Health and Social Care

Cyber security is an ever increasing global issue and has been for many years. Whilst working from home brings new opportunities for employers and staff alike, it also carries an increased online risk to malicious attacks seeking to expose, manipulate and exploit organisations and individuals' confidential data.

This resource has been designed by ACOSVO to help voluntary sector organisations be better informed about cyber security and attacks. It has been produced in partnership with CyberScotland and supported by Scottish Government.

It guides you along your cyber resilience journey by introducing a checklist (prioritised into high, medium, low) which your organisation can take to achieve maximum cyber protection. By working through this, you will

Most attacks that are going on all of the time are generally **automated**. They look for a **flaw** so they can get through with the **least amount** of effort".

minimise the impact of future cyber attacks on your organisation and best protect all your stakeholders.

Simple instructions are combined with more strategic-level questions to consider. You will also find signposting to further useful resources, such as articles, videos, blogs & infographics.

Individuals can download, save and edit the resource to keep track of personal or team progress with the various cyber areas over the coming days, weeks and months.

Consider appointing a cyber champion within your organisation to engage board and operational team members and to lead on cyber resilience improvements throughout your organisation.

- Enter Name
- Follow Journey
- Click Links
- Mark as Ticked


CYBER RESILIENCE JOURNEY: PRIORITIES



OWNER:
REVIEWER:
DATE:

Checklist

<p>Wi-Fi</p> <p>Never send or receive private information when using public Wi-Fi.</p> <p>Get Safe Online · Watch</p>	<p>Updates</p> <p>Take a minute to enable auto-updates on all mobile devices.</p> <p>NCSC Blog · Watch</p>	<p>Passwords</p> <p>Incorporate the NCSC method (link below). Use a password manager to store securely.</p> <p>NCSC Tips · Password Managers</p>
<p>Risk register</p> <p>Include cyber-related topics on your risk register and discuss regularly.</p>	<p>e-Bulletins</p> <p>Sign up to receive regular updates on cyber security from trusted sources straight to your inbox.</p> <p>CyberScotland · NCSC · SCVO</p>	<p>Privileges</p> <p>Ensure your access to network is extended only as far as one's role requires. Protects from insider threat.</p>
<p>Ransomware</p> <p>Set out a basic principle for negotiation - see pointers on page 4.</p> <p>NCSC Guidance · Poster</p>	<p>Accreditation</p> <p>Become cyber-security accredited. Includes cyber essentials & cyber essentials plus.</p> <p>Self Assessment · SBRC Video</p>	<p>Priority Legend:</p> <ul style="list-style-type: none"> High Priority Medium Priority Low Priority

<p>Authentication</p> <p>Ensure to set up 2 Factor Authentication on all devices and platforms used for work.</p> <p>ISAME Info · NCSC Blog · Watch</p>	<p>Data back-up</p> <p>Identify and ensure all important data is stored on the cloud or offline on a portable hard-drive.</p> <p>NCSC Blog · Watch</p>	<p>Software</p> <p>Consider installing a mobile device management software as a way of remotely controlling devices.</p> <p>NCSC Guidance · Comparison</p>
<p>Supply chain</p> <p>Assess other organisations whose cyber insecurity may directly affect your own i.e. through an imposter attack - see pointers on page 4.</p> <p>NCSC 12 Principles · Assessment</p>	<p>Av software</p> <p>Ensure an anti-virus software is installed on all devices. Ensure staff know how to keep enabled.</p> <p>NCSC Guidance · Blog</p>	<p>Phishing</p> <p>Document instances and educate members of staff on how to report low-medium & high threats.</p> <p>SBRC Exerise in a Box</p>
<p>"Cyber is one of many strategic business risks and must be considered at the board level".</p> <p></p>		
<p>Incident management</p> <p>Have a policy which can be analysed and learned from post-incident - see pointers on page 4.</p> <p>NCSC Guidance · Timelines</p>	<p>Incident response</p> <p>Consider keeping an incident response company on retainer for when an issue occurs.</p> <p>CyberScotland · NCSC Guidance</p>	

Further Support

Resources

Webpages

NCSC Glossary
NCSC Active Cyber Defence
STOic Table Top Exercise

Applications

SBRC App

Check-ups

SCVO Digital Check up

For Boards

NCSC Toolkit
Ransomware
Resources

How to Report

Access the Free SBRC Cyber
Incident Helpline on 01786
437 472

Forward spam emails to
report@phishing.gov.uk

Report spam text messages
directly to your mobile phone

provider by forwarding them to
7726 free of charge

Check to notify OSCR or the
Information Commissioners Office
where necessary

Pointers

Supply chain

- 1) Whose cyber security are you
reliant on & how might your
cyber insecurity be used against
others?
- 2) Ask your supply chain if they
are carrying out an incident
response plan?
- 3) Are they cyber accredited &
if so, which one?

Ransomware

- 1) What sensitive information

may be used to force
negotiations?

- 2) Will you enter negotiation &
if so, where will you find the
necessary experience?
- 3) How will you obtain and pay
ransom in the digital currency
required?

Incident management

- 1) When does an incident
become an incident?
- 2) What does a high, medium
or low level incident look like?
- 3) How many machines are
affected?

Where do you keep your
plan? Is its location
known throughout the team
& can it be accessed outside
your network"?

Remember – no one becomes
an expert at this overnight.
The only way forward is to
identify, plan, test – repeat".

Keith McDevitt

Cyber Security Integrator, Scottish
Government

Not If, But When

