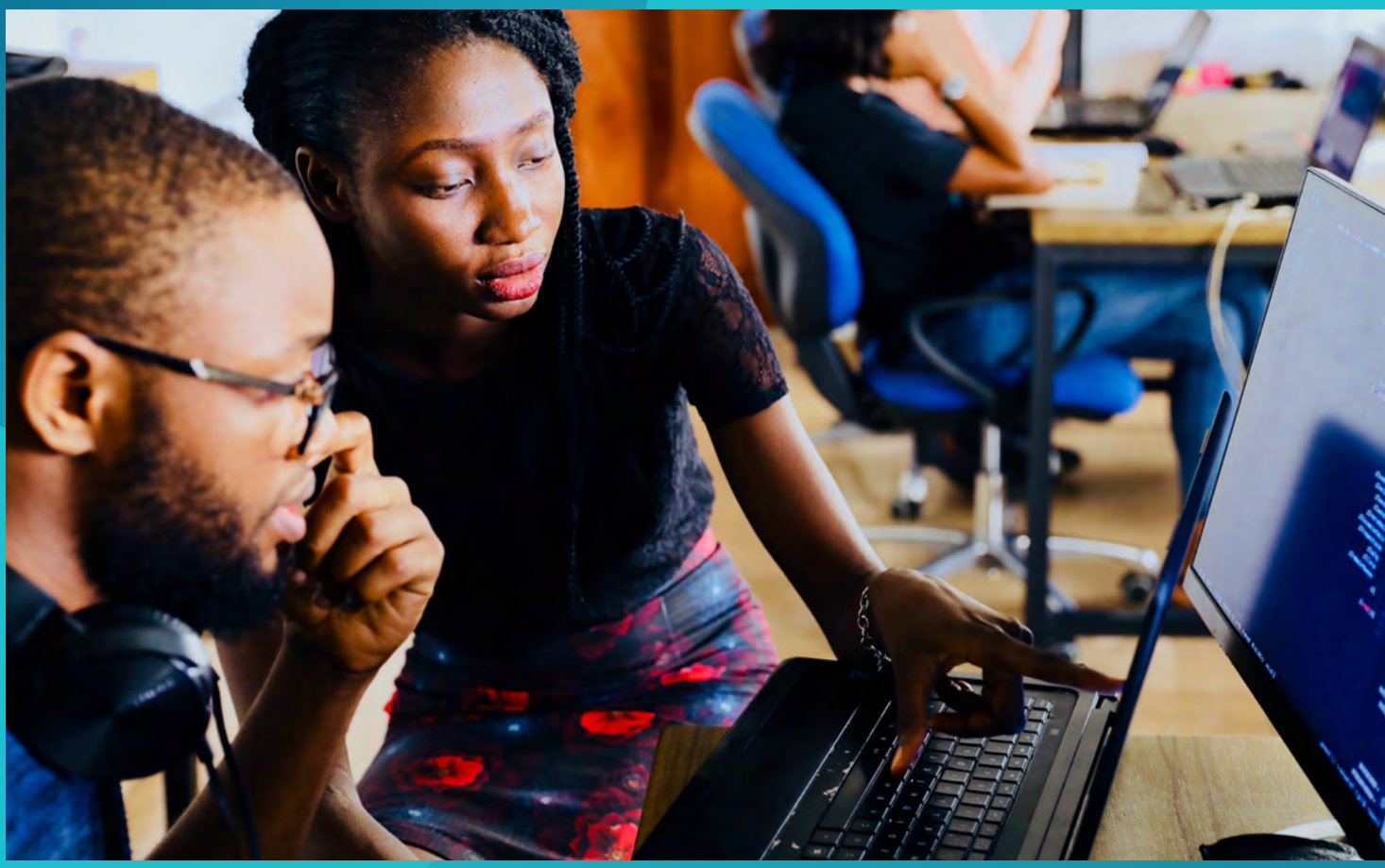
THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST



Prepare Your Business: Checklist

In partnership with

Scottish Business Resilience Centre

NORTH WEST REGIONAL ORGANISED CRIME UNIT

nwcrc.co.uk

Prepare your business: Checklist

Use this checklist to help prepare for, respond to and recover from cyber incidents. For more information visit: www.nwcrc.co.uk/incidentresponse/

Plan ahead: What could you do to protect your business?	Notes
Identify and prioritise your most valuable assets ○ What do you care about most? ○ What are your 'Crown Jewels'? **When an incident occurs:** ○ Consider your order of system recovery and prioritise these areas. ○ Review at the time of invocation of the incident – your recovery order will depend on the current needs of the business at that time.	
Understanding your IT service contracts ○ Check what support is included by any outsourced SAAS (Software as a Service) providers within your contract. This might include email accounts, calendars, and file storage. ○ Give clear and detailed instructions on what security controls you want your IT provider to implement. **For each external provider write down:** ○ What data are they responsible for? ○ Are back-ups included in your package? Are they turned on? ○ Are there other security features you could add on or turn on?	
Create a Cyber Security Incident Response Team ○ Create a team who will handle the response to an incident. This step may involve input from your outsourced IT managed service provider.	

Plan ahead: What could you do to protect your business?	Notes
Ensure staff understand Cyber Incident Team roles ○ Allocate deputies to cover for absences.	
Consider what equipment may be required to run your business offline ○ What would a manual process look like? ○ Have a back-up communication channel e.g phone numbers, social media, intranet.	
Capture business emergency contacts ○ Create an emergency contact document. Include staff names and contact details, emergency contacts, customers and suppliers. ○ Make a digital copy of the document available in a place you can access easily. ○ Print a hard copy of the document and keep it in a safe place. ○ Consider keeping another copy of this document somewhere offsite. ○ Update this document regularly (for example every 3 months).	
Share resilience plans with staff ○ Train staff who feature within the Incident Response Team on what is expected of them in their roles. ○ Ensure they have a delegated deputy in case of staff absences. ○ Implement staff training for policies and procedures and reporting incidents.	
Understand the role of social media and communications in cyber incident response ○ Create a crisis communication plan. ○ Create a public relations plan. ○ Draft responses for a variety of scenarios and timeframes, including information to get you through the first 48 hours. ○ Draft content for your company website – pre-upload a draft web-page with information including FAQs and / or a hotline for customers or stakeholders to call.	

Prepare your business: Checklist

Plan ahead: What could you do to protect your business?	Notes
Make copies of your incident response plan ◯ Ensure you can still access your plan should computer equipment become unavailable.	
Undertake weekly IT security checks ◯ Undertake weekly security updates. ◯ Regularly check you can restore your information from a back-up copy. Make sure that data is copying in a condition where it can be restored from. ◯ Do you need to replace or restore any technology?	
Regularly (daily / weekly) back-up computers and key documents ◯ Keep copies safe / offsite. ◯ Ensure you can restore the information from it. ◯ https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data	
Test your Cyber Incident Response plan ◯ NCSC Exercise in a Box lets you test your incident response plan, ensuring staff know how to respond during an incident. It contains material for setting up, planning, delivery, and post-exercise activity. ◯ Regularly test and check key elements of the plan. ◯ Consider creating your own bespoke cyber exercises. This allows you to tailor these to reflect your organisation's values and threats you face.	

Designed by

Agent.

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Cyber Resilience Centre
Manchester Technology Centre
Oxford Rd
Manchester
M1 7ED

0161 706 0940

info@nwcrc.co.uk

nwcrc.co.uk

@northwestcrc