Start here today to help your business survive a Cyber Incident tomorrow:

Sources of help and further information

Autumn 2022

Also available online at https://neict.org/isnortheast/cyber-resilience-for-business-managers/

Version control; changes in addition to the document title since version 0.3 are highlighted

Helping you to respond to a Cyber Incident

Considering risks in 'peacetime' and planning how you might respond to a Cyber Incident in advance of it happening will help you keep your business going.

There are a number of key areas that can help.

- Being aware of the risk
- Pre-planning and making decisions in advance
- Developing a Cyber Incident Response Plan consisting of:
    - A Business Continuity Plan
    - A Communications Plan
    - An IT Disaster Recovery Plan

This document lists questions to consider for each of the three response Plans. **By answering the questions and recording your answers you'll create the bulk of your Cyber Incident Response Plan that should be helpful in the event of a Cyber Incident.** Ideally, you should then test this (as you would a Fire evacuation plan) and make amendments as necessary.

Sources of further information and guidance are also included as well as links to template document cover sheets for to other actions you can take to make your business more cyber resilient.

Contents

Notes:

This document was in part co-created at the Northumbrian Water Innovation Festival 2022 during a one-day 'daily dash' co-ordinated by CyberNorth and UKC3. Some content is based on a similar initiative for schools in North Tyneside and from the North East Cyber Incident Response Plan developed by Local Resilience Forum emergency planners. It also borrows from Lessons Learned from significant cyber incidents in the last few years.

The document prompts the reader to consider questions they may not have previously thought about; it should also be useful to those familiar with business cyber resilience, acting as a checklist and reminder of things to consider.

Compiled by Graham Jordan, for ISNorthEast Summer 2022.

Sources of help and further information

If you're new to the subject

Ten steps you can take now to lessen the impact of a Cyber Incident

Business advisers

Industry / sector / local networks

Your supply chain (and their security suppliers)

Small & medium sized organisations - NCSC.GOV.UK

NCSC_A5_Small_Business_Guide_v4_OCT20.pdf

Self-employed & sole traders - NCSC.GOV.UK

Cyber blogs | Business Resources | Institute of Directors (iod.com)

Legal Implications of a Cyber Incident: Awareness of key commercial and legal implications of a cyber incident. Who do you need to report to and by when?

Regional organisations of the National Cyber Resilience Centre Network such as the North East Business Resilience Centre

Action fraud

Regional Organised Crime Units such as NERSOU

Scottish Cyber Incident Response Pack including documents to help support your organisation plan your response to a cyber incident.

Once you've a bit of experience

Director GCHQ speaks at CyberUK 2022 - GCHQ.GOV.UK

CRCGM announces free cyber security resources for small businesses (brimcentre.com)

Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk)

CybercrimeSmallBusinesses.pdf (suffolk.police.uk)

Cyber insurance providers

The Business Continuity Institute

The Emergency Planning College

NCSC CIR service providers

Regional cyber Clusters e.g. Cybernorth.biz

BS 31111:2018 Cyber risk and resilience. Guidance for the governing body and executive management – this is a non-technical entry point for senior managers which emphasises organisational as well as technical aspects of cyber risk management.

CBEST Implementation Guide, V2 (Bank of England, 2016) A framework for organisations seeking to stay resilient during a cyber attack

The Civic Cyber Resilience Model (developed under the National Cyber Security Programme Think Cyber – Think Resilience initiative) provides wide ranging guidance on civic cyber resilience

Building Resilience Together briefings providing strategic briefing material for local leaders, policymakers and practitioners on collaborative working on the cyber agenda.

Sector-specific resources such as Resilience Direct for the Public Sector and Cyber Security for Legal and Accountancy Professionals. (Fraud Advisory Panel) An e-learning module jointly developed by the Government, the Law Society and Institute of Chartered Accountants

	Lego exercise via Regional Cyber Crime Unit or National Cyber Resilience Centre Network
For your IT colleagues Tools to see if you've already been hacked - Shodan, leakpeek, have i been pwned etc. Report a Cyber Attack | North Eastern ICT Partnership (neict.org) CiSP NCSC free ACD tools Local IT providers that offer Cyber Incident response services Cyber Essentials / Cyber Essentials+ NCSC exercise in a box via NCSC, Regional Cyber Crime Unit or National Cyber Resilience Centre Network Minimum Cyber Security Standard	**Template cover sheets for your Plans** https://neict.files.wordpress.com/2022/07/templates-for-cyber-resilience-starter-guide-v0.1.docx **'Answer Book' / Workbook to make notes, record your responses to the prompt questions and note any necessary actions to improve your readiness to respond.** https://neict.files.wordpress.com/2022/10/cyber-resilience-work-book-v0.1.docx