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

# Business continuity questions to consider

Summer 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 0.2 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.

# Business Continuity

**Do you have a Business Continuity Plan for a Cyber Incident?**

A response to a Cyber Incident could require long hours of sustained effort for a prolonged period (in some cases months. For example, a ransomware attack). Your plan should also include how you plan to manage and support your staff during this time. Both those responding to the Incident and those not directly involved in the response but could be affected by the Incident as these can often cause huge amounts of stress to staff who can no longer do their job.

*Questions to think about:*

1. *What's the worst that could happen? How long can you operate without IT?*
2. *Do you rely on technology for the safety of your staff or customers? What health & safety systems rely on IT? eg, fire alarms, CCTV, BMS, etc as they should be considered first to keep everyone safe.*
3. *Do you have any safety-critical processes / manufacturing / monitoring / treatment systems that might be affected?*
4. *Do you have a Business Continuity Plan and can you get to it? What if you can't get to your electronic files?*
5. *Have you considered other emergency situations such as a flood or fire? What Plans do you have in place for those? How much can you apply from these to a Cyber Incident?*
6. *What are your 'crown jewels'? – data, systems, business processes, key historic data, people? Do you have any single points of failure? Could you rate them by importance - e.g. platinum, gold, silver and bronze?*
7. *What are your priorities for recovery? How long can you manage without them? What gets recovered first (e.g. platinum)? How long will it take to recover them?*
8. *Do you process any sensitive data? Might you have also suffered a data breach?*
9. *What can you put in place for your customers?*
10. *If your workaround involves writing things down on paper, how will you keep that secure?*
11. *Where would you recover your data from? What's your next best source?*
12. *Can you rely on your data? How will you know if your data has been corrupted?*
13. *Who looks after your payments in and out? What arrangements do you have with suppliers and customers if payment systems go down?*
14. *How will you manage and support your staff? Can you pay them?*
15. *During an Incident you may need to buy a laptop / printer / mobile phone or even expensive Incident response services. Who can spend money? How?*
16. *What about your 'non-IT' suppliers – THEIR cyber resilience? (Your supply chain). What if THEY have a Cyber Incident? Include your landlords in your thinking – you might get locked out or have no electricity or internet.*

17. *How would you accept stock deliveries into your warehouse or fulfil orders?*

18. *What do your (different) stakeholders really value and can you continue to provide that?*

19. *What 3rd party services do you rely upon being in place? Don't just think IT, e.g. logistics partners*

20. *What contractual obligations do you have to others?*

21. *Who is going to examine lessons learned after the Incident? What will they need to know? Is that being captured?*

22. *Who will manage any offers of help? How will you understand what they can offer?*

23. *Many high-profile Incidents have happened 'out of hours'. What if key staff members are on holiday / jury service / maternity? Is your business usually affected by seasonal factors that would raise additional concerns?*

24. *Will you convene a 'recovery board' to direct your response to the Incident?*

25. *Do you have emergency staffing protocols in place?*
    - *What are your business-critical roles / tasks?*
    - *Who is going to be responsible for what?*
    - *Is that the same as their usual role?*
    - *Who is going to keep a log of key decisions made during the Incident response?*
    - *What's the chain of command?*
    - *Where do staff get reliable information from?*
    - *Are colleagues aware of this in advance of an Incident?*
    - *Consider holding on to staff about to leave and brining new starters in sooner. Any recent retirees that might be able to help*

26. *How will you know if your Incident response is working?*