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

Questions to ask whoever supports your IT

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.

IT Disaster Recovery

Do you have an ICT Disaster Recovery Plan for a Cyber Incident?

Think of this as your playbook with all instructions on how you would recover from a Cyber Incident. It should include all network and system documentation, detail of IT systems/applications and detail of any backups. If you have external suppliers, this should also include them and any contractual arrangements you have in place with them for responding to a Cyber Incident.

Questions to think about (and discuss with your IT colleagues/suppliers):

1. *Who looks after your IT? Do you have multiple suppliers?*
2. *How will you know you have a Cyber Incident and not just something that's 'business as usual' for your IT colleagues? (a glitch versus a disaster?)*
3. *What do you already have in place to mitigate the impact of a Cyber Incident?*
4. *If you had an Incident, what is your IT recovery strategy (does that fit what the business needs)?*
5. *Do you have enough IT resource to recover your systems? Who could help?*
6. *When was the last time you tested recovering your systems? Was that successful?*
7. *Do you have any failover technical capacity? Is it sufficient to keep the business going?*
8. *What IT systems do you rely on? Who provides them? Do you have their contact details?*
9. *What support arrangements do you have in place with your systems suppliers?*
10. *Are any of the systems you use 'out of support' from the 'manufacturer' e.g. Windows XP*
11. *What copies of data (back-ups) do you keep? How? Where? Are they separate from the network (air-gapped)? How up to date are they?*
12. *Do you have spare/reserve IT equipment?*
13. *How do you connect to the internet? What options do you have if that wasn't available?*
14. *Would your printers and photocopiers still work?*
15. *How might you need to preserve evidence for any criminal investigation?*
16. *What 3rd party organisations or systems are you connected to / do you rely on? Does anyone rely on you? Do any of your own systems rely on other systems you have?*
17. *Can systems / data / networks be accessed remotely? By whom? Using what equipment? Using what credentials?*
18. *What can 3rd parties do to help? What doesn't need specific knowledge of how you do things?*
19. *How will you know if the bad guys are still there / determine how long the Incident might last? (How would you know it's over?)* "are they still there?"

20. *How would you convince yourself the attacker was no longer present before you start to recover in full?*