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

Communications issues 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.

Communications

Do you have a Communication Plan for a Cyber Incident?

Think of this like a plan you would have for communicating if there had been a fire in your building. You should assume that during this time you could have severely limited or no access to phones and email. You should also consider how you communicate with staff, customers and the media during a Cyber Incident.

Questions to think about:

1. *What methods of communication do you still have available? How would you communicate with staff? Customers? It's useful to think about who, when (e.g. how long after the incident) and how (as you may not have phones or email) in advance.*
2. *How do you contact customers and protect the business?*
3. *How will you (securely) contact staff? - Do they all use WhatsApp for example? Do you already have a staff WhatsApp or Facebook group?*
4. *Do you have emergency contact numbers? Staff? Suppliers? Key customers? Landlord? Caretaker? Compliance, ICO (!) Action Fraud (!) Police (!), sources of help, people that have been through something similar? (ICO), key suppliers that integrate with your IT systems, your Board, etc.*
5. *Do you have 'company' mobile phones that you can give out the numbers for to customers?*
6. *Do you have standby arrangements in place for website and social media? Do you know the passwords to your website and social media accounts? Can you access them from outside of work?*
7. *Do you have multiple / spare social media accounts (that customers know they can trust) in case you get locked out?*
8. *What would you tell the media?*
9. *Do you have a media policy?*
10. *Have you got a pre-prepared statement? What would it say?*
11. *Has anyone had media training?*
12. *Who is going to communicate?*
13. *Who needs to know what? Is it the same message to all? Do you have a prioritised list? Is it up to date?*
14. *When is it right to communicate?*
15. *What can you say and can't say? Who 'signs it off'?*
16. *How do you stop the bad guys finding out they've been successful?*
17. *You could be unlucky and get hit by a mass 'attack' or you could be targeted – would anyone have reason to target you? Is there a chance you, your friends, family or employees overshare information that could be used against you?*