Original version 0.1 released Summer 2022. This version 0.4 Autumn 2022

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

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

Helping you to respond to a Cyber Incident 2

What's the risk? 3

Business Continuity 5

Communications 7

IT Disaster Recovery 8

Sources of help and further information 10

Acknowledgements 12

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.

What's the risk?

Have you considered the risk to your business of a Cyber Incident? The Government has identified cyber as one of its top four risks to the UK, alongside terrorism, pandemic and environmental risks.

Unfortunately, commentators are now talking in terms of 'when' you might experience a Cyber Incident, rather than 'if'. There's also been a focus shift from defending and protecting to preparing to respond and recover from Cyber Incidents.

- One in five businesses (20%) and charities (19%) experienced a negative outcome as a direct consequence of a cyber attack[1]
- 4 in 10 had a cyber incident last year, rising 10% year on year; £2.4bn was lost
- Attacks can cause business to close down or production to relocate with an associated loss of employment
- Many SMEs don't think it will happen to them and only invest in cyber when it's a condition of winning a contract
- Only 19% of businesses have a formal Incident management plan

Likely business impacts of a Cyber Incident include:

- *Loss of sales, orders, income*
- *Loss of reputation, trust, customer confidence*
- *The need to evacuate premises / 'close shop'*
- *Inability to get stock into or out of your warehouse*
- *Having to do things manually; not being able to find what you need*
- *Inability to deliver services*
- *Not being able to keep customer appointments*
- *Loss of internal or external telephones, email, fax, internet, fire alarms and building systems - you could be locked out of your building*
- *Inability to communicate with staff, customers, suppliers, shareholders*
- *Incurring costs to investigate and fix problems*
- *Increased security risks due to staff using paper, personal IT, own phones etc.*
- *Potential theft of data, regulatory fines (ICO, PCI etc.) and increased regulatory scrutiny after the event*
- *Inability to monitor key activities including safety critical systems*
- *Stressed staff*
- *Inability to take or make payments, including paying staff*
- *An increased need to invest in IT systems and services after the event*
- *An increased chance of being a repeat victim of crime*
- *Potential loss of life, depending on the nature of your business*

The UK Government National Cyber Security Centre (NCSC) defines a Cyber Incident as *"a breach of a system's security policy in order to affect its integrity or availability and / or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990).*

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

In general, types of activity that are commonly recognised as being breaches of a typical security policy are:

1. *Attempts to gain unauthorised access to a system and / or to data*
2. *The unauthorised use of systems for the processing or storing of data*
3. *Changes to a system's firmware, software or hardware without the system owner's consent*
4. *Malicious disruption and / or denial of service"*

The upshot of this is that your systems or data will either not be available or will have been corrupted to the extent you cannot rely upon them. Additionally, as it the current trend with ransomware, data will have been locked so you cannot access it and it is likely that the perpetrators will release sensitive data to the outside world to pressure you into responding to ransom demands.

Likely Causes of a Cyber Incident

Cyber Criminals	Individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data and generating profit.
Physical Threats	Fires, floods, power outages, natural disasters, datacentre congestion, non-criminal
Accidental	It is worth noting that accidental Incidents may have similar implications (e.g., underground cable cut by a digger etc).
Hacktivists	Issue-orientated groups / individuals who want publicity to draw attention to their cause / grievance
Script Kiddies	Less skilled individuals who use cyber scripts or programmes developed by others – generally just playing around and not a threat to society
Insiders	Someone who exploits their legitimate access to an organisation's digital assets for unauthorised purposes.
Terrorism	Using malware to attack critical UK networks, e.g., government systems, utilities infrastructure
State sponsored threats / espionage	Attempts by states and state-sponsored groups to penetrate UK networks for political / technological / commercial / strategic advantage
Hacking for hire services	Laypersons with motivation but lacking the technical skills can now turn to online services to undertake / aid them to undertake cyber-crime including email hacking, website hacking, ransomware and DDOS.

Things to think about:

1. *Could you keep your business going?*

2. *Do you have someone responsible for risk? Someone at Board level? Or is it just you?*

3. *Have you discussed cyber risks within your organisation? With your Board? Your employees? Your insurers?*

4. *If you have cyber insurance, what does it cover?*

5. *How would you know if what you're experiencing is a computer outage or a cyber-attack? How much does that matter – are the impacts the same?*

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?*

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?*

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?*

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

Acknowledgements

Attendees at the Northumbrian Water CyberNorth/UKC3 Innovation Festival daily dash:

- Richard Snell, Celerity Ltd
- Gavin Bewsher, Cleveland Emergency Planning Unit
- Stuart Marshall, Cleveland Emergency Planning Unit
- Tim Shurmer, Cleveland Emergency Planning Unit
- Phil Jackman, CyberNorth
- Robert Campbell, Ecommnet Technologies Limited
- Andrew Fisk, Fisk Consulting
- Thea Scott, Footprints Consulting
- Adam Pickering, Fujitsu
- Hannah McGarrell, Fujitsu
- Jason Bishop, Fujitsu
- Lynsey Pickering, Fujitsu UK
- Laura Atkinson, Hicomply
- Nancy Gemski, Kyndryl
- Nathan Dale, Mott MacDonald
- Stephen Leach, North East Business Resilience Centre
- Rebecca Chapman, North East Business Resilience Centre Ltd
- Paul Armstrong, North Tyneside Council
- Simon Corbett, Northumbria University
- Emily Tomlinson, Northumbrian Water
- Louise Patterson, Northumbrian Water
- Graeme Cowie, NWL
- Gerard Kerrigan, Pen Test Partners
- Janine Marshall, RTC North Ltd
- Dominic Button, University of Sunderland
- Shaun Allan, XR Therapeutics

Cleveland Local Resilience Forum

Durham Local Resilience Forum

Northumbria Local Resilience Forum

CyberNorth

Dynamo North East

North Eastern ICT Partnership

North Tyneside Council IT Section

Northumbrian Water

Redcar and Cleveland Council

Copeland Borough Council

Newcastle University