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

Understanding Cyber risk

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.

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?*