NHS Digital

Data Security Standard 7

Continuity Planning

The bigger picture and how the standard fits in

2019/20

Information and technology for better health and care

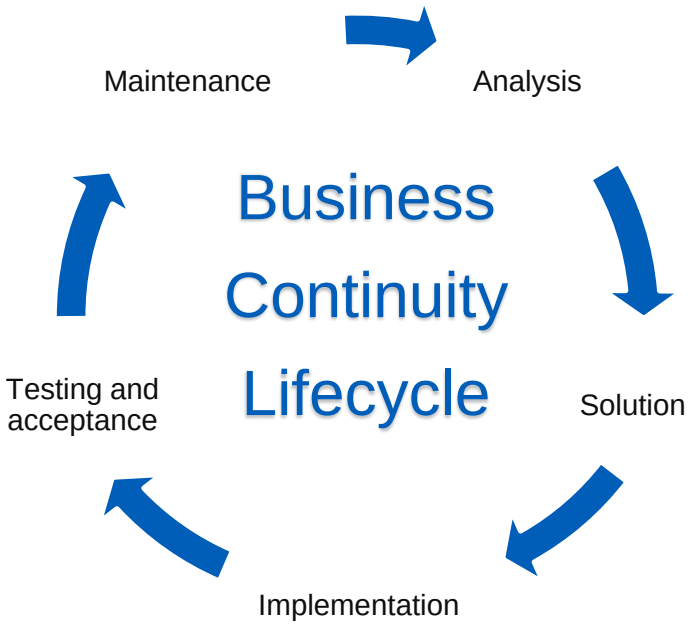
Contents

Overview

The National Data Guardian review's data standard 7 states that:

"A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management."

A business continuity exercise is run every year as a minimum, with guidance and templates available from the toolkit. Those in key roles will receive dedicated training, so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English.

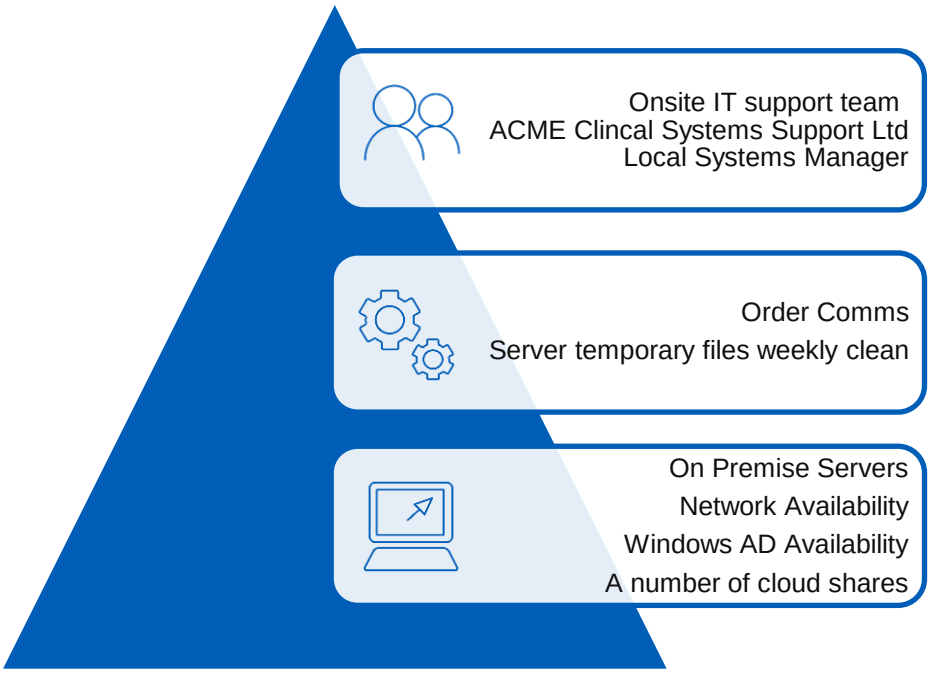


Know your services

In knowing your organisation from a continuity perspective is initially understanding and cataloguing the health and care services your organisation provides. For each of those catalogued services you should know:-

- What technology and services underpin that service in terms of availability and security
- Other dependencies such as power, cooling, data, people and other systems
- The impact of the system being unavailable

For example, looking at a generic clinical service that is underpinned / dependent upon people, processes and technology



Example Clinical Service

Organisations understand the health and care services they provide.

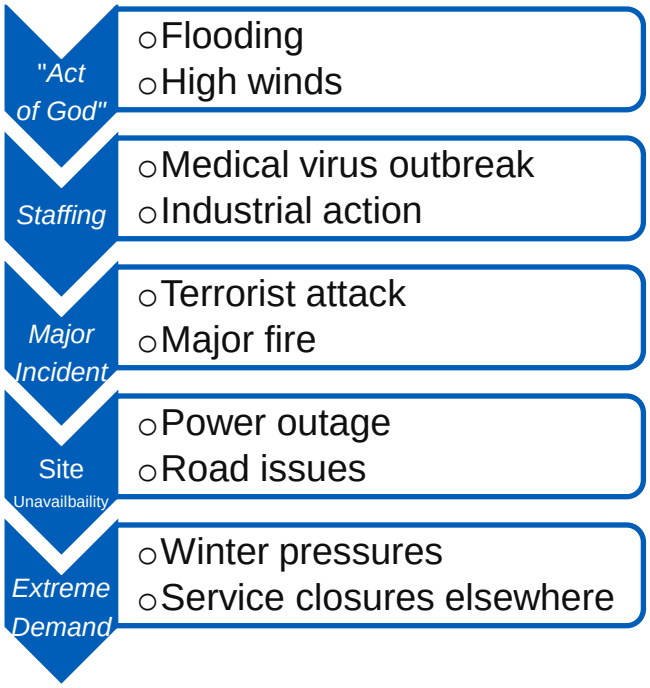
Data Security Standard 7.1.1

Business continuity and disaster recovery

Definition and background

The terms business continuity and disaster recovery are often interchanged and sometimes viewed as the same thing. A business continuity plan (BCP) is concerned with how you keep the organisation going and could involve relocation and reshaping services. Disaster recovery is effectively a plan of attack of how you fix the problem and return the organisation back to normality.

In the care system, organisation business continuity tends to focus on:



The global WannaCry cyber-attack in May 2017 has reaffirmed the potential for cyber incidents to impact directly on patient care and the need for our health and care system to act decisively to minimise the impact on essential frontline services.

Your Data: Better Security, Better Choice, Better Care

Government Response

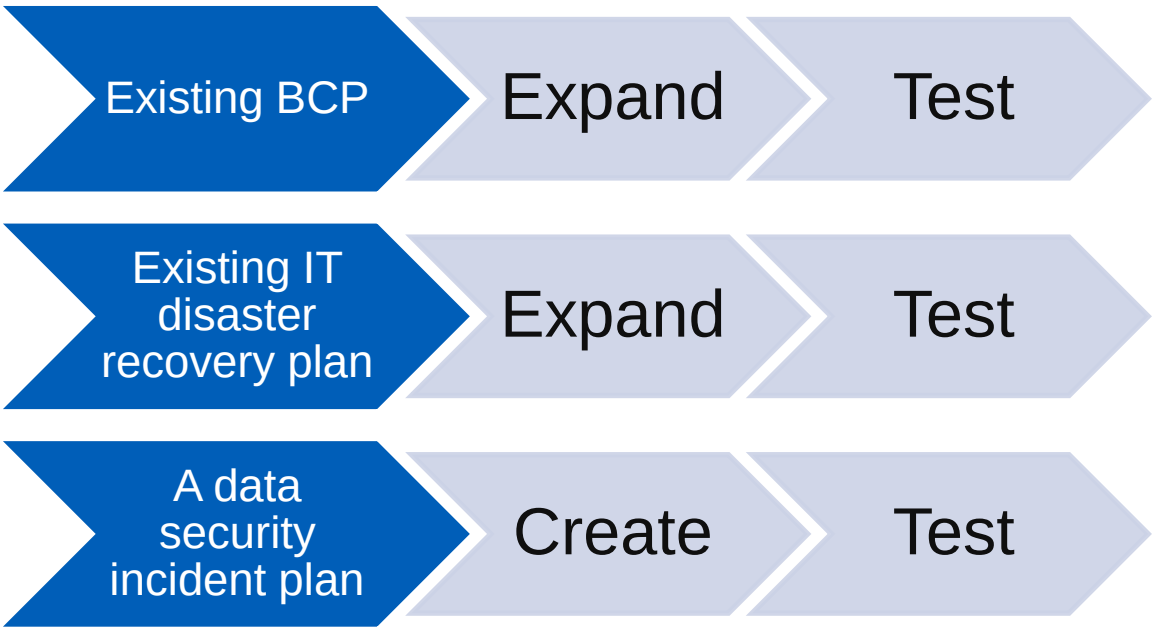
Whereas the IT tends to focus on disaster recovery. With a focus on:

- Identifying IT objectives and timescales
- Priority of recovery
- The recovery team
- Actions for recovery

Planning against common risksWhere plans exist in small organisations, there would tend to be one plan.

A continuity plan for data security incidents

There are three routes to implementing:



You can expand an all-encompassing BCP to include data security content, alternatively expand your IT disaster recovery plan. However, where possible we would recommend you have a separate data security incident plan.

Whichever route you choose data security should be included in any plan, even those not related to cyber incidents. For example, where a restored system that may have the full set of access rights in place.

Expanding your existing BCP

Generally, this is for smaller organisations that already have an all-encompassing business continuity plan. You should include sections on data security including what to do, what to avoid and scenarios.

A smaller organisation business continuity plan (a generalised version of the pharmacy BCP in Appendix 2) is contained in full in Appendix 3.

Expanding existing IT disaster recovery plan

Generally, this is for organisations that have an existing IT disaster recovery plan. The team responsible is a small set of people who would respond to data security incidents as well as the more traditional IT ones. This approach can be useful in dealing with an incident where the initial cause may not be known, such as network problem that could be caused by faulty equipment or a denial of service attack.

It is important data security is featured as prominently as the more traditional causes of incidents and includes as a minimum what to do, what to avoid and scenarios.

Good practice guideline for business and IT security plans are referenced in Appendix 2.

A set of suggested scenarios for data security testing are contained in Appendix 4.

Creating a data security incident plan

For organisations with granularity of roles and sufficient size, we would recommend a separate data security incident plan.

This will allow you to really focus on data security incidents, the actors, attack surface basic and sophisticated attacks, the phases of the attack and the response.

There are two examples in Appendix 2, the Cyber Security Incident Response Guide by Crest (The Council for Registered Ethical Security Testers) and the Computer Security Incident Handling Guide by National Institute of Standards and Technology (NIST) U.S. Department of Commerce.

Whilst both examples are very useful, it is important to note the CREST document is written from a point of view of those wishing to augment their data security response with external help. The NIST guidance in parts can be quite US centric.

Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?

Data Security Standard 7.1.2

Know what you need

The length of time it takes to resolve an incident can be prolonged by a lack of knowledge of the resources needed and their availability.

This can be compounded by treating each incident in isolation and in a bespoke way rather than using lessons learned and shared resources

The resources can be people and one widely used method is to formally set up an incident response team. This will generally be a multidisciplinary IT team which can tackle a range of incidents ranging from hardware / network failure to a large-scale malware outbreak.

It can be obvious when you need data security and protection resources to tackle a malware outbreak as it is seen as cyber issue. However, some issues not readily seen as data security and protection due to their nature e.g. server hardware failure could bring about data security and protection challenges in their resolution.

For example, when commissioning a new server to replace the failed one, the understandable emphasis is to return the service back online with expediency and perhaps take a few short cuts (such as minimum patching, hardening and open file rights). Or it may be tempting to temporarily store file shares in the cloud during remediation, however no assessment may have been made of any legal data protection and contractual obligations before doing so.

The right tools for the job

Just like any repair, having the right physical and digital tools at your disposal in a timely fashion can make all the difference. Having a “grab bag” containing items such as switch, networks, diagnostic laptop (with server / network analysis software), usb drives with boot diagnostic software etc can be useful.

Careful consideration on how many grab bags are required and where they should be located. i.e. storing them all on your main site which may have restricted access during an emergency would not be wise.

Public cloud can be a very useful resource (given its high availability and location independence) for machine images, restoration data and diagnostic software.

You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.

Data Security Standard 7.1.3

Whatever method you use to store your restoration resources, remember it is important that you are licensed for the software, that any data stored is secured and processed in a safe manner and that it is as up to date as it needs to be.

An Intelligence lead security posture

You should be horizon scanning via the CareCERT portal, the Cyber Associates Network (CAN) and other sources in order to make temporary changes to your security posture.

For example, a developing situation with a widespread convincing phishing campaign that delivers a highly disruptive piece of malware could temporarily trigger: -

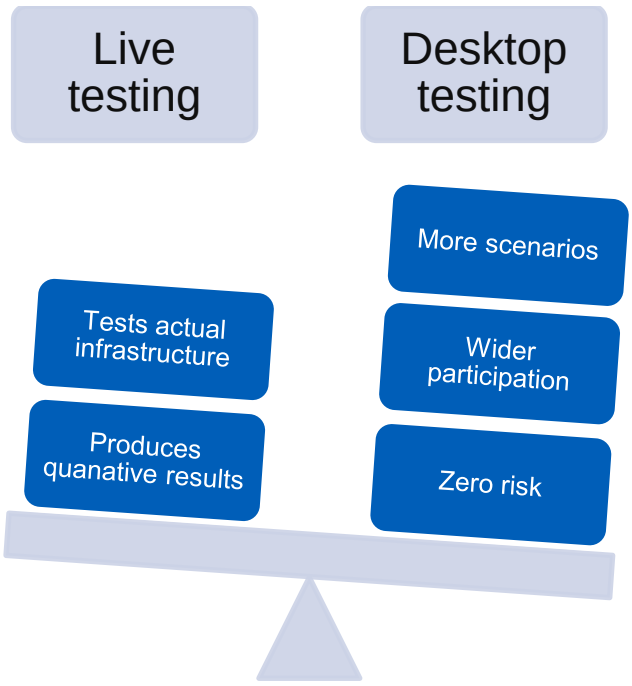
- A targeted awareness campaign
- A temporary freeze on optional updating
- Blocking certain categories of websites
- Elevated rights being restricted to a small cohort
- Certain network segments with at risk systems (medical devices etc) being completely separated from the corporate network

Once the event has passed these, more draconian measures would be repelled.

> You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.
>
> Data Security Standard 7.1.4

Testing the plan

Testing the plan can generally be done in two ways - through live testing (simulation / active testing) or through desktop-based scenarios.



Live testing

This can take the form of more active penetration test with a threat actor with a defined target, e.g. bring down a system.

The testing can take place in a live environment or sand pit. It is important that if undertaking the testing in a live environment that you are confident the live environment will not be negatively affected. Conversely, if using a simulated / sand pit environment, it is important that it is a true reflection of a live environment to be representative.

The person undertaking the role of the threat actor should not be the person who would normally be on the incident response team and would normally not have “insider knowledge”. Unless the scenario is of a disgruntled former employee.

Any live test does have many limitations it must occur at a known time when the response team is already gathered, and the effect would have to be detected by the team. In a real scenario the time of the event will be unknown, and effects may not be flagged.

Desktop testing

This should form a realistic scenario and a frank and honest appraisal of your response. The goal of desktop testing if to identify gaps in your response in terms of people, processes and technology. These gaps should inform improvement actions that help your future response to any data security incidents.

These test(s) need to occur at least annually and have board level representation.

It is highly recommended that you utilise National Cyber Security Centre (NCSC)' Exercise in a Box' for desktop testing.

Exercise in a Box is an online tool from the NCSC that helps organisations test and practise their response to a cyber attack.

- It is completely free and you don't have to be an expert to use it.
- The service provides exercises, based around the main cyber threats, which an organisation undertake in its own time, in a safe environment, as many times as it needs to.
- It includes everything you need for setting up, planning, delivery, and post-exercise activity, all in one place.
- To use Exercise in a Box you need to register for an account, which enables the provision of a tailored report, helping organisations identify their next steps and pointing toward guidance that is most relevant for the organisation.

https://www.ncsc.gov.uk/information/exercise-in-a-box

Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.

Data Security Standard 7.2.1

Which scenario/s were tested during the business continuity exercise, why, and when?

Data Security Standard 7.2.2

Membership of the testing group

It is recognised that the exact makeup will vary and be dependent on the size and nature of the organisation. The table below makes some recommendations of the type of roles, with an understanding that some roles may be merged.

Role	Description
Board level member	Mandatory, allows board to be informed
External chair / adjudicator	Someone independent from your organisation who is not involved in the incident response. They would have some experience in this area (such as your counterparts from a neighbouring organisation). They would deliver the scenario, respond to queries and develop the scenario based on the answers
Information / data security / IG	Specialist in data security and protection
Head / director IT	The person responsible for IT in your organisation
CCIO (Chief Clinical Information Officer)	To understand the clinical impact of incidents
Network manager	Specialist responsible for network infrastructure
Server manager	Specialist responsible for server infrastructure
Service desk manager	Responsible for the help desk service
Desktop manager	Responsible for team of desktop technicians

An example of an attendance sheet is shown in Appendix 5

Scanned copy of meeting registration sheet with attendee signatures and roles held.

Data Security Standard 7.2.3

The type and volume of scenarios

The type of scenarios should be related to the most likely data security incidents. Some suggestions for the type of incidents are included in Appendix 4. Three of the most likely scenarios should be undertaken.

During the testing

During the test, the scenario should be explained to the incident team with replies and queries logged. The chair should probe the answer and develop the scenario. The intention like any testing is to identify areas for improvement. An example of a log of test is shown in Appendix 5.

Where you find gaps, you should log them (together with a name to look at them), however the exercise should not be overtaken by solutions analysis. The primary purpose is to identify a gap and then move on.

Post testing

Post testing a full action plan should be drawn up with allocated names and dates. This should be followed up. An example action plan is contained in Appendix 5.

From the business continuity exercise, which issues and actions were documented, with names of actionees listed against each item.

Data Security Standard 7.2.4

You are not alone

Data security incidents when discovered can be daunting and it can be tempting to implement blanket controls. Your immediate response can either help remediate or worsen the situation.

It is important that you engage with NHS Digital (for an NHS body) or a Cyber Incident Response company where appropriate. They will have experience and a pool of resources and intelligence not at your disposal.

> On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.
>
> Data Security Standard 7.3.1

Roles and responsibilities

In the event of invoking the plan, it is essential that team members are able get hold of contacts to assemble the response team.

Therefore, there is a mandate that a hard copy of the contacts for the response team is kept securely and kept up to date. It is important that it is also known when it was last updated and printed.

Consideration should be given to where the copy contact list is located, especially in a scenario that affects access to the site (i.e. the same list used for IT disaster recovery).

The contact list should be reviewed and updated at intervals. When updated the contact list should be reprinted.

> All emergency contacts are kept securely, in hardcopy and are up-to-date.
>
> Data Security Standard 7.3.2

Digital contact list

It is recognised that not every incident will require accessing a “last resort” hardcopy contact list. Storing on a source outside your network (such as NHS Mail / Cloud) which is accessed from any device can seem attractive. You will need to ensure the location / security of the service is compatible with trust and national guidance. However, digital storage should be additional and not a replacement for hard copy storage.

Press material

A draft press statement(s) should be drawn up in conjunction with your communications team to speed up the press response and ensure consistency.

There is a commercial sector link on how to handle the media following a cyber-attack in Appendix 2. This provides some key points to consider when crafting skeleton statements.

These should be reviewed and updated on a regular basis.

Are draft press materials for data security incidents ready?

Data Security Standard 7.3.3

If I could turn back time

Backing up to a different source has been a standard method of recovery for decades. However, when needed during an incident some organisations have found that restoring a backup has proven difficult and this has prolonged the time to return to business as usual.

This can be for a variety of reasons:-

- Overused / old media
- Corrupt catalogue
- Bad image files
- Multiple complex restores required (full and then a large number incrementals)
- Backup didn't occur / backed up the wrong system
- Nowhere to store the restore
- Networked disk-based storage being unavailable due to the nature of the incident

For all these reasons and more, it is important that you can have confidence in the recovery of essential service through testing, documenting and routinely reviewing.

The testing should be representative of the service / system in focus and not based on routine smaller scale requests or an old live incident. For example, a routine restore of single mailbox for a returning member of staff would not be considered as enough confidence to restore a whole email system.

Whether to use live or test systems should be determined on risk and whether the test system is sufficiently representative of the live system to make the testing valid.

Just as important as the tests themselves is documenting how to restore the system as well as any issues found during the test and the plan to rectify them.

The testing frequency should be routinely periodic especially after any major change in the system / service.

Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.

Data Security Standard 7.3.4

When did you last successfully restore from backup?

Data Security Standard 7.3.5

Appendix 1 -
Table of data security level 7 assertions

Assertion	Sub Assertion	Evidence
7.1 Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.	7.1.1	Organisations understand the health and care services they provide.
	7.1.2	Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?
	7.1.3	You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.
	7.1.4	You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.
7.2 There is an effective test of the continuity plan and disaster recovery plan for data security incidents.	7.2.1	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.
	7.2.2	Which scenario/s were tested during the business continuity exercise, why, and when?
	7.2.3	Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held.
	7.2.4	From the business continuity exercise, which issues and actions were documented, with names of actionees listed against each item.
7.3 There is an effective test of the continuity plan and disaster recovery plan for data security incidents.	7.3.1	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.

	7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.
	7.3.3	Are draft press materials for data security incidents ready?
	7.3.4	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.
	7.3.5	When did you last successfully restore from backup?

Appendix 2 -
Useful resources

Emergency Preparedness, Resilience and Response (EPRR) business continuity toolkit: NHS England

https://www.england.nhs.uk/ourwork/eprr/bc/

Emergency Planning / Business Continuity: Pharmaceutical Services Negotiating Committee (PSNC)

PSNC has produced a business continuity template to meet the requirements of community pharmacy service providers.

https://psnc.org.uk/contract-it/essential-service-clinical-governance/emergency-planning/

Response and recovery planning (CAF) : NCSC

Putting suitable incident management and mitigation processes in place. There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-1-response-and-recovery-planning

CareCERT Information Sharing Portal: NHS Digital

A home for the latest intelligence and guidance with:

- threat articles
- whitepapers
- best practices.

https://nww.carecertisp.digital.nhs.uk/

How to handle the media following a cyber-attack: Mediafirst

Example from the commercial sector consideration when handling the press.

Sign up for security threat bulletins and emergency notifications.

http://www.mediafirst.co.uk/our-thinking/how-to-handle-the-media-following-a-cyber-attack/

Appendix 3 –
Data security scenarios

It is highly recommended that you utilise NCSC exercise in a box for desktop testing

https://www.ncsc.gov.uk/information/exercise-in-a-box

However, scenarios from the previous version are included in case you wish to retest last year's response.

Example A: Stand and deliver!

A member of your staff opens up an email attachment which looks legitimate. Sometime after they notice they are unable to open up their work documents. On investigation the damage is not limited to the one person - work all the organisation's network shared documents have been encrypted. The member of staff receives a ransom mail detailing where to transfer money to rectify the issue. When trying to mitigate via a backup you run into a problem with the backup tape and creating an inventory.

How do you proceed?

Example B: *makes you want to cry*

Your helpdesk receives an influx of calls reporting from staff stating they have static screen displaying a message asking for payment in bitcoins to unencrypt the PC.

How do you proceed?

Example C: *Not so fast, not so furious*

Your network monitor system starts to alert you of high traffic volumes and helpdesk receives calls from staff reporting sluggish response on networked applications. You manage to trace the IP address (which changes) but is within a range for an eastern European country.

How do you proceed?

Example D: *Pass me the remote*

You notice a trend of calls being received by your helpdesk that the pointer on the screen is moving by itself and opening and closing tiles and files.

How do you proceed?

Example E: *Not my problem?*

A third party to your organisation (a data processor) reports that it has been subjected to an unspecified cyber-attack. It believes there is a potential for hundreds of your staff records to have been accessed (but cannot prove they have).

How do you proceed?

Example F: *A modern classic?*

A USB stick is found in the staff car park and handed in to reception. It contains a large data set of sensitive patient data. You are initially surprised as you have an endpoint protection system in place preventing unencrypted devices.

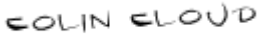
How do you proceed?

Example G: *Which way?*

You discover large amounts of your active directory structure has been deleted. In recent weeks as part of cost improvement plans, you have not renewed a number of senior IT contractors' contracts. You remain suspicious.

How do you proceed?

Appendix 4 –
Example of results of a test

Attendance sheet			
Desktop test	Your network monitor system starts to alert you of high traffic volumes and helpdesk receives call from staff reporting sluggish response on networked applications. You manage to trace the IP address (which changes) but is within a range for the same eastern European country.		
Review venue	A meeting room	Date / Time	dd/mm/yy @ hh:mm
Attendees role Board member	Mrs Patricia Personnel	HR Director	
Head of IT	Mr Colin Cloud	IT Manager	
CCIO	Miss Susan Septum	Lead Consultant	
IG/ data security	Mr Lee Privilege	IG / IS Manager	
IT networks	Miss Cat Five	Network Manager	
IT servers	Mr Stan Bye	IT Server Manager	
Adjudicator	Mr Aton Detail	External Audit Service	

Log of responses			
Process review	Your network monitor system starts to alert you of high traffic volumes and helpdesk receives call from staff reporting sluggish response on networked applications. You manage to trace the IP address (which changes) but is within a range for the same eastern European country.		
Review venue	A meeting room	Date / time	dd/mm/yy @ hh:mm

Notes the scenario is not known to the group beforehand.

AD Delivers the scenario.

CF & CC Respond with a discussion on blocking a blanket range of addresses from the Eastern European country.

SS Ask if this will affect a high profile clinical trial running jointly between the organisation and a university hospital in that country as its was one of the Chief Exec top priorities. The group wasn't aware of the trial and data / systems being shared.

Action 1: SS / LP Revisit data flow mapping exercise

AD asked why during the initial stages why the disaster recovery plan wasn't mentioned or invoked (e.g. war room, disaster team, sitreps, press statement etc).

Action 2: CC Inform team of plan

There followed a discussion on whether IDS/IPS protection / firewall was dynamic enough to cope with a scenario like this. PP suggested could we contact the support organisation for help and advice. It emerged the firewall was out of maintenance support and the supplier was ceasing firmware upgrade support next year. There was a discussion on why a business case / budget hadn't been identified for a replacement.

Action 3: CF Options appraisal

AD asked who you would need to alert if the situation went on over an hour and started to affect business critical and clinical systems. The group suggested the local CCG and NHS England but were unsure of others.

Action 4: CC/SS

AD said after an hour the network traffic dies down but access logs on a financial server are reported as red on the same service. Users to the service are reporting they are unable to log in due to no available licenses.

SB suggested restarting the server, LP suggested a more nuanced approach would be warranted and taking the server off the network to investigate forensically.

AD asked who would undertake such a forensic investigation and what plan would they follow?

The group was unsure due to resourcing constraints and current capabilities.

Action 5: CC/SS/LP

AD Asked in a scenario where the financial server is now off network. What would you do now as there is no apparent activity.

The group suggested that it would be good to go through various logs on the network and server infrastructure to try to identify any patterns, attack vectors and source. During the course of the conversation it was identified that there is a server SIEM logging system by XYZ for server infrastructure and a different instance and brand (ABC) for network infrastructure. It was discovered you couldn't query across both instances.

Action 6: CC/CF/SB

Improvement notes for next meeting

Useful to bring copies of the BCP, whiteboard for sketching ideas and more role play and time lapsed to give a sense of urgency.

Next scenario scheduled dd/mm/yy hh:mm @ 123 Room followed by follow up action meeting

Action plan					
Process Review	Your network monitor system starts to alert you of high traffic volumes and helpdesk receives call from staff reporting sluggish response on networked applications. You manage to trace the IP address (which changes) but is within a range for the same eastern European country.				
Review venue	A Meeting Room	Date / time	dd/mm/yy @ hh:mm		
	Agenda item	Action	Due	Allocated	Status
Agenda / actions 1)	Data flows	Revisit data flows works and particularly offshoring *Actions some flows identified however issues with lack of cooperation, escalated to SIRO*	dd/mm/yy	SS/LP	Unresolved
2)	Inform team of plan	Redistribute copies to team asking for improvements and have a follow up workshop *Action complete*	dd/mm/yy	CC	Resolved
3)	Produce an options appraisal for firewall / IPS / IDS	Produce an option paper for boundary protection *Actions: Report completed with CC & SIRO*	dd/mm/yy	CF	Resolved
4)	Who to inform	Produce a list of who / how to inform and update plan Actions: Plan updated	dd/mm/yy	CC/SS	Resolved
5)	Forensic investigations	Identify suitable course and external expertise Actions: Training and / or call off contract identified however no budget exists. Escalated to SIRO	dd/mm/yy	CC/SS/LP	Unresolved
6)	Unified SIEM	Identify a course of action for a unified SIEM. Actions: Report produced recommending extending ABC SIEM to cover both sides, enough licenses exist plan produced to rollout	dd/mm/yy	CC/CF/SB	Resolved
New items					
7)	Remote centres	Producing the actions prompted a question whether remote locations within other org estates are covered by the plan or the other estate. Actions: CC to confirm with counterparts	dd/mm/yy	CC	New
	Items 1 & 5 to be included in next SIRO meeting – on dd/mm/yy @ Board Room 1				

Appendix 5 –
The National Data Guardian reports

The NDG report

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent and Opt-Outs

The government response

‘Your Data: Better Security, Better Choice, Better Care’ is the government’s response to:

- the National Data Guardian for Health and Care’s ‘Review of Data Security, Consent and Opt-Outs’
- the public consultation on that review
- the Care Quality Commission’s review ‘Safe Data, Safe Care’

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.