THE
SOUTH EAST
CYBER
RESILIENCE
CENTRE

Cyber Incident Response Plan

CYBER INCIDENT RESPONSE PLAN

A cyber security incident response plan provides a process that will help your business, charity or third sector organisation to respond effectively in the event of a cyber-attack.

How to use this template

- **You** are free to use, share, adapt and build upon this material, but you may not use this material for commercial purposes.
- **We** suggest reviewing the pack and editing names and numbers where necessary, before you distribute to your organisation.
- **Consider** printing appendix H to help staff with a clear reporting procedure in the beginning of any incident.
- **Use the** checklist to provide a prompt response that will limit the damage of any attack, whilst communicating effectively through your channels to keep suppliers, customers, and staff onside. The checklist will help to calmly guide a response through a time of heightened stress and confusion.

APPENDICES

At the end of this document, you will find several appendices in the index that form resources for you to use. They are titled:

- Appendix A - Contacts Directory
- Appendix B - Action Card for a manager receiving a report of cyber incident
- Appendix C - Incident Log to record initial actions
- Appendix D - Advice to give to staff reporting a Cyber Security Incident
- Appendix E - Tactical Manager Action Card
- Appendix F - Strategic Manager Action Card
- Appendix G - Lessons Learned Report
- Appendix H – Cyber Security Incident Plan
- Appendix I - Device out of action posters
- Appendix J - Cyber Action Wall staff Posters
- Appendix K –Version Control Information

WHAT IS A CYBER SECURITY INCIDENT?

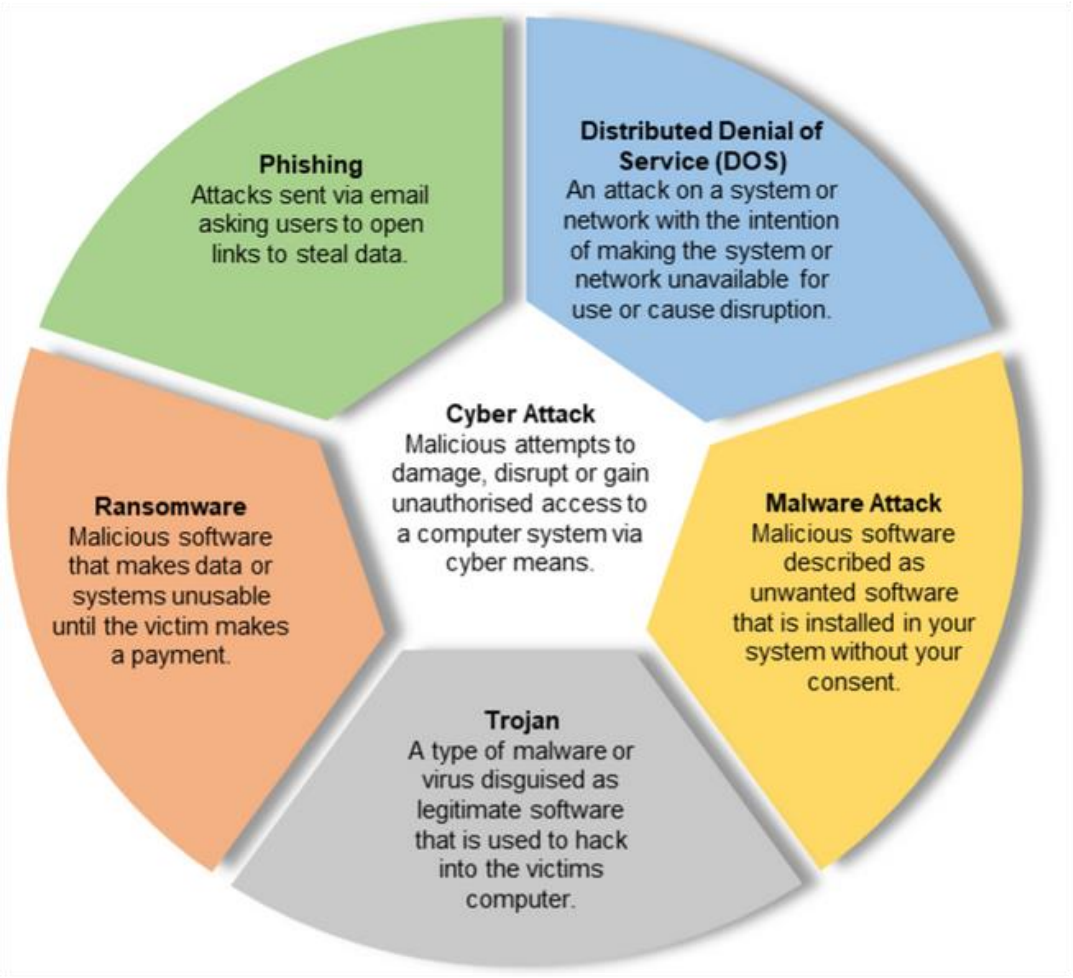
The National Cyber Security Centre (NCSC) defines a cyber security incident as:

- A breach of a computer system's security policy to affect its integrity or availability.
- The unauthorised access or attempted access to a computer system.

Activities commonly recognised as security policy breaches are:

- Attempts to gain unauthorised access to a computer system and/or to data.
- The unauthorised use of computer systems and/or data.
- Modification of a computer system's firmware, software, or hardware without the computer system owner's consent.
- Malicious disruption and/or denial of service.

The attack methodology for a cyber security incident varies greatly, as will the associated response. The scale of a cyber security incident will not always be determined or obvious from the outset. The nature of cyber-attacks evolves very quickly, some typical cyber-attack methods are outlined below.



CYBER SECURITY CONSEQUENCES

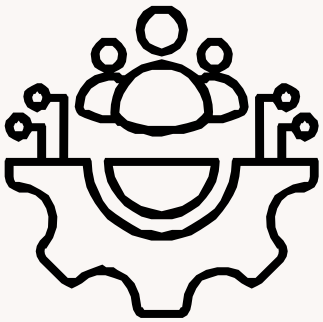
You should keep your organisation's computer systems and data safe and functional whilst maintaining a service provision. There are many ways in which cyber security incidents can negatively impact your organisation. The main impacts can be broadly categorised into 5 areas:

1. Physical/Digital - infection of your computer systems and that of your supply chain, or loss of personal or private information leading to regulatory consequences.
2. Economic - the asset is compromised and must be replaced or repaired incurring a financial cost.
3. Psychological - confusion and disarray while the organisation regroups to work around the attack.
4. Reputational - unfavourable scrutiny, loss of confidence and goodwill or business.
5. Social/societal - negative changes in public perception and an adverse change in how the public engages with the organisation.

IT FAILURES OR CYBER-ATTACKS?

Cyber-attacks may initially present as computer system failures, glitches, or smaller losses of IT service. Only IT, Information Security, or a member of the senior leadership team can declare a cyber security incident. However, where there is a loss of operational IT functionality, Business Continuity (BC) plans can and should be invoked by any member of staff.

BC plans contain initial actions to address IT loss, including actions to isolate potentially compromised computers and reporting of the incident to the IT service desk. BC plans should be held in paper copy as well as electronically, so they are independent of IT access and easily found when required.



CYBER SECURITY INCIDENT ASSESSMENT PROCESS

Cyber security incidents should be assessed on its severity at an early stage. This assessment will also be completed by other organisations who may have more of an informed view of what is occurring regionally and nationally.

It is important to understand how the assessment process works so you know when to activate your Cyber Security Incident Plan. Once a cyber security incident is declared the following roles should be established to deal effectively with the incident:

- **Duty Manager** will initiate this plan if information is received, or you are contacted by other departments telling you that a response should be activated.
- **IT** are key in both the recovery of systems as well as the recovery of evidence. IT should have a very comprehensive emergency response plan to deal with a cyber security incident. IT deal with cyber threats daily and it is important to recognise their knowledge and experience in dealing with this incident type.
- **Information Security** is part of the wider Information Management department, it deals with the data that is held on IT systems. This role has a data security plan that can be implemented in the event of an incident.
- **Data Protection Officer** is responsible for the assessment of an incident's impact on the rights and freedoms of data subjects. This role is responsible for reporting data losses or compromises to the Information Commissioner's Office (ICO) within a 72-hour timeframe, as well as briefing the Senior Information Risk Owner.
- **Operational/Business Impact** of a cyber security incident is likely to have an operational or business impact on services. It will be necessary to appoint departmental leads to manage this impact by the activation of business continuity plans. The number of people allocated to this role will be dependent on the scale of the impact.
- **Communications** is important that communications are maintained with staff to prevent the potential spread of a cyber security incident. It is also vital to keep partners and the media informed; any large-scale cyber security incident is likely to be of significant national media interest.
- **Tactical Manager/Senior Leadership Team/Duty Manager** is someone that exists at both tactical and strategic levels which is crucial to a successful outcome. The establishment of an internal coordination meeting at an early stage is strongly advised.

CYBER SECURITY INCIDENT ASSESSMENT PROCESS

- **Strategic Manager/Senior Leadership Team/Chief Executive/Business Owner** will set a strategy for the CIRT to work to. There are often competing demands between the swift recovery of IT systems compared to the recovery and investigation of the cyber security incident. It is the Strategic (Gold) Commander's responsibility to balance these demands.
- **Computer Incident Response Team** is responsible for responding to security breaches, viruses, equipment failures, ransomware, data theft, intrusions, and other incidents in businesses. In addition to technical specialists capable of dealing with specific threats, it should include experts who can guide businesses on appropriate communication during an incident.

EARLY HELP

Appendix J is a template wall poster to use in offices to assist staff in the reporting of a cyber incident and providing early guidance. Consider editing and affixing these in common areas.

ALERT STANDBY AND ACTIVATION TRIGGERS

The notification of a cyber security incident may come from several possible sources:

- Self-identification by IT, Information Security, or other internal user.
- Notification via the national structures of the National Cyber Security Centre (NCSC), or intelligence from another partner organisation.

INITIAL ACTIONS - ASSESSMENT

A cyber security incident can only be declared by a member of IT, an Information Security Officer, or the Strategic Manager. Although you may (correctly) suspect a cyber security incident is taking place, you must get the incident declared formally by an authorised person.

TASKS

The initial responder should refer to Appendix B – Action Card for a manager receiving a report of cyber incident.

COMMUNICATIONS

During a cyber security incident either targeting your systems or directed towards an external partner / supply chain, careful consideration should be had surrounding communication capabilities.

There may be a diminished capacity for those affected partners because of the impact from the cyber security incident. Resilient communication options should be considered such as alternative phones. Internally, a successful cyber-attack can affect multiple communication methods. Intranet and internet websites alongside communication avenues such as online contact, or email communication may be lost; effectively isolating the public from accessing your services and the service from using internal communications.

Voice Over Internet Telephony (VoIP) and Microsoft Teams are all telecommunications systems which could be lost or compromised.

RECOVERY

The key principles of recovery should be considered if the activation of this plan results in a major incident or disruptive event. The following elements of recovery should be considered:

- Humanitarian considerations
- Infrastructure
- Environmental considerations
- Finance

STAND DOWN AND INCIDENT CLOSE

This plan will stand down when the cyber security incident has been investigated to the satisfaction of the Strategic Manager. Relevant partner agencies must be notified of a stand down.

POST INCIDENT EVALUATION

Where possible the senior leadership team at all levels should seek to hold a hot debrief as soon as practicable after the incident has closed, making a formal record of the outcome. Formal debriefs maybe held at a later stage and should include the outcome from any hot debrief.

Identified best practice should be collated and disseminated. An after-action review of this plan will be carried out by the senior leadership team as soon as reasonably practical.

A template to report the use of this plan is included in Appendix G of this document. This review will identify learning points to improve the plan and the subsequent response.

Where possible the senior leadership team at all levels should seek to hold a hot debrief as soon as practicable after the incident has closed, making a formal record of the outcome. Formal debriefs maybe held at a later stage and should include the outcome from any hot debrief.

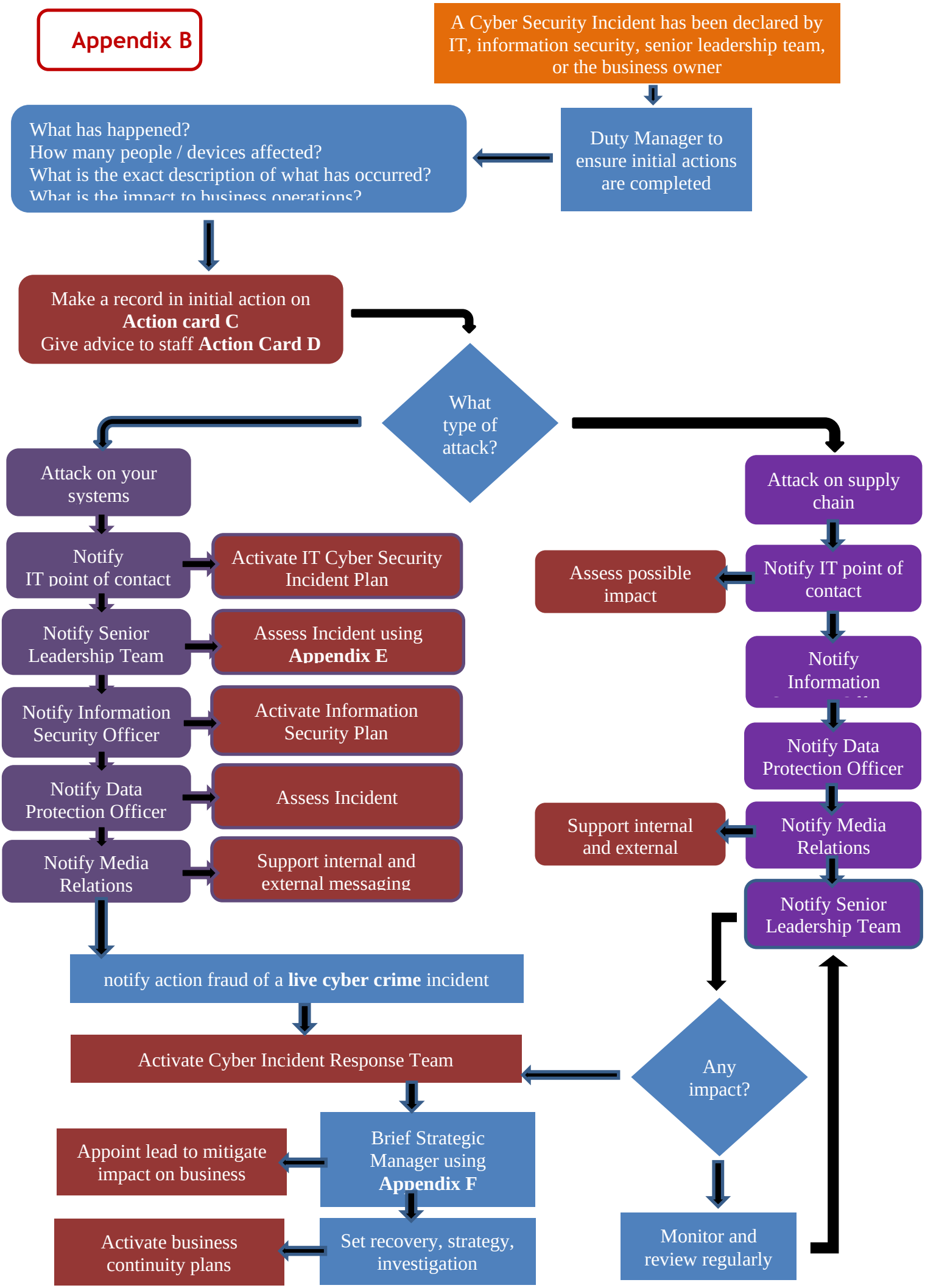
Identified best practice should be collated and disseminated. An after-action review of this plan will be carried out by the senior leadership team as soon as reasonably practical. A template to report the use of this plan is included in Appendix G of this document. This review will identify learning points to improve the plan and the subsequent response.

Appendix A Contacts Directory

Complete the blanks with relevant information to your organisation

Organisation	Notes	Contact Details
Internal Agencies		
IT point of contact	office hours emergency out of hours	
Information Security Officer		
Data Protection Officer		
External Agencies		
Action Fraud	Provides the central point of contact for the reporting of fraud & cybercrime. Will forward details of the cyber security incident to the National Fraud Intelligence Bureau who analyses and then notifies the National Crime Agency. Neither Action Fraud nor the National Fraud Intelligence Bureau is responsible for the investigation of offences but record all Live cyber-attacks.	0300 1232040
Information Commissioners Office (ICO)	Data Protection Officer to make contact. Bear in mind a 72-hour deadline for any data breaches.	0303 1231113
National Cyber Security Centre (NCSC)	In the event of a serious cyber security incident the NCSC will provide further specialist advice and support to assist with the response and mitigate potential impacts. https://report.ncsc.gov.uk/	0300 0200964
National Crime Agency (NCA)	Investigate the most serious and complex attacks hitting the UK. The NCA will co-ordinate and support the entire UK policing response as well as providing specialist high-end technical support. The NCA will assess the cyber security incident via the NCCU and allocate the appropriate agency to investigate.	
Regional Cyber Crime Unit (RCCU)	When tasked by the NCA may provide support to: •Support the investigation into the cyber security incident. •Assist during a cyber specific incident by providing cyber tactical representatives and advisors. •Provide specialist knowledge and assistance in and out of hours through a national on-call rota.	
Incident Response Company	Can deploy a range of security tools, technologies and specialist analysis that will monitor, hunt, and help to detect unknown sophisticated and evasive cyber security threats. Can provide technical and intelligence support to the investigation of a serious cyber security incident.	
Partners / Supply Chain	Partners will share information relating to the cyber security incident. This will help to immediately advise and warn others involved in the supply chain with the intention to prevent further breaches and allow the opportunity to put preventative measures in place.	
Insurance Company	If your organisation has cyber insurance, you should make contact and follow specific guidance in relation to your policy	

Appendix B


A Cyber Security Incident has been declared by IT, information security, senior leadership team, or the business owner
Duty Manager to ensure initial actions are completed
What has happened?
How many people / devices affected?
What is the exact description of what has occurred?
What is the impact to business operations?
Make a record in initial action on **Action card C**
Give advice to staff **Action Card D**
What type of attack?
Attack on your systems
Notify IT point of contact
Activate IT Cyber Security Incident Plan
Notify Senior Leadership Team
Assess Incident using **Appendix E**
Notify Information Security Officer
Activate Information Security Plan
Notify Data Protection Officer
Assess Incident
Notify Media Relations
Support internal and external messaging
notify action fraud of a **live cyber crime** incident
Activate Cyber Incident Response Team
Brief Strategic Manager using **Appendix F**
Appoint lead to mitigate impact on business
Set recovery, strategy, investigation
Activate business continuity plans
Attack on supply chain
Notify IT point of contact
Assess possible impact
Notify Information
Notify Data Protection Officer
Notify Media Relations
Support internal and external
Notify Senior Leadership Team
Any impact?
Monitor and review regularly

Appendix C Incident Log

Maintain a log of initial actions which will assist the senior leadership team and other supporting resources when allocated

Brief circumstances of what exactly has happened? **How many affected?** **What is the impact?**		
Time / Date	Person completing	Log Note

Appendix D Advice to staff reporting cyber incident

Action for managers to follow this checklist if staff report a cyber incident direct

	Give this advice to staff who report what you think might be a cyber incident. Always direct them to the IT support. If out of hours, consider calling the IT emergency contact number.	
	Who else has been affected? Is it just you or other people around you reporting the same or similar problems?	
	Do not turn off the computer, leave it turned on to ensure evidence is preserved.	
	Tell the staff member to log off the computer and put a sign on it to stop others using it, providing the sign in this pack if necessary.	
	Isolate the computer by removing the network cable or put it in airplane mode if connected by Wi-Fi.	
	Secure any memory sticks, discs, DVDs, or any other media connected to or used in the computer.	
	Do not allow the user to take any remedial action or access their emails from another device.	
	Do not let the user log onto any other devices.	
	Do not post on social media or discuss the incident with anyone outside of your organisation.	
	Encourage the caller to start thinking about what they can do to continue their role and direct them to business continuity plans.	

Appendix E Tactical Manager Action Card	
Tactical Manager / Senior Leadership Team / Duty Manager	
1	Coordinate the organisations response to a cyber incident. You will arrange and chair an internal meeting to achieve this.
2	What is the scale of the reported incident? Has it formally been declared cyber incident by IT, Information Security, senior leadership team, or business owner? Only these roles can declare a cyber incident.
3	Has contact been made with the person responsible for IT? Have they activated their plan called IT Cyber Security Incident Emergency Plan? Has contact being made with the Information Security Officer and the Data Protection Officer?
4	Has Action Fraud been notified? If so, what feedback or intelligence has been passed?
5	Brief the duty media officer to prepare communications to staff as well as partners and the media
6	Have any partners been notified that share IT systems that could also be infected?
7	Appoint leads for areas of operational business that may be impacted. This may be one person or many depending on the scale refer to business continuity plans
8	Arrange an internal Cyber Incident Response Team meeting as soon as possible. It should include representatives from IT, Information Security, Data Protection, Communications, and Business Impact staff.
9	Brief strategic lead / Chief Executives ensuring there is a clear strategy set which balances the recovery systems against investigation.

Appendix F Strategic Manager Action Card	
Strategic Manager / Senior Leadership Team / Chief Executives / Business Owner	
1	You are responsible for the organisation's response to this cyber instant. You must also consider the wider impact on partners as well as the recovery phase at an early stage.
2	What is the current impact of this instant on the company? Is this a widespread national incident or restricted to you only? Are there any other partners also affected?
3	There are often competing demands between ITs desire to restore IT systems and the investigatory desire to secure and preserve evidence ensure you are clear in your strategy where primacy lies.
4	Has a Cyber Incident Response Team meeting been formed to manage this incident? This is the group that should be chaired by the senior leadership team to drive your response
5	Has contact been made with Action Fraud / National Cyber Security Centre? They coordinate / investigate a response to cybercrime. What is their assessment and what support have they offered?
6	Your information management department should consider the reporting of any incident to the Information Commissioners Office which is time critical. They should also brief the Senior Information Owner. They may not be a 24/7 department so check their functions are being carried out within the time scales
7	Does this incident have any impact on your supply chain? Is it likely that the cyber-attack will attract their oversight?
8	Co-locate your team ASAP at a single, safe, and easily identified location near your incident.
9	Communicate using plain English, try to avoid jargon.
10	Agree a lead, identify priorities, resource, and capabilities for an effective response, including times of further meetings.
11	Jointly understand the risk, share information about the likelihood and potential impact, to agree control measures and risk reduction.

Appendix G Lessons Learned Action Card

Submission of this report will instigate a review of the plan by the senior leadership team which is vital for continuous improvement

Name of Plan implemented	
Date and time implemented	
Person implementing	
Brief circumstances	
What went well	
What could be improved within the plan to help you next time?	

Appendix H

Cyber Action

Discover or suspect a Cyber Incident?

Confirm infected devices are disconnected from network?

Have you disconnected network from the internet?

Utilise a secure separate conference call to understand what has happened and review the impact

Insert Conference Call Number

Insert Chair persons & participants dial in code

Consider representatives from Insurance, Legal, PR, IT, HR & Law enforcement?

Allocate someone to track incident/actions/maintain a written log

Preserve all device / server logs

Confirm containment steps and contingencies?

Identify source and ensure other users are not exposed?

Consider password resets (users / administrators / systems)

Confirm availability of CLEAN back-ups?

Consider steps to eradicate?

Plan your recovery phase?

Law Enforcement involved, have you secured evidence?

Keep an infected device powered off and disconnected for police

Complete final wipe & reinstall of a clean operating system

Run anti-virus check / malware protection on all devices

Reconnect to network

Report incidents to the Police via Action Fraud 0300 123 2040

Consider your disclosures?

Voluntarily - Internal / External press releases

Mandatory - Data breach? Report to ICO

Regulatory - Dept of Education / Charities commission

Review lessons learned

Appendix J

Cyber Action

Discover or suspect a Cyber Incident?

Disconnect affected device from network:

- Wired connections (Ethernet / USB)
- Wireless connections (Wi-Fi / Bluetooth / put in airplane mode)

Consider turning off Wi-fi network (routers / switches)

Place sign on device to stop others using it

Secure any connected memory sticks, media

Contact IT support/provider

Insert Name & number

Insert Name & number

Contact Senior Leadership Team

Insert Name & number

Insert Name & number

Make a note of what was you were doing leading up to this incident

Take a picture of screen

Appendix I

IT Informed Date: **Reference No:**

IT Informed Date: **Reference No:**

Appendix K Version Control

Version	Comments / Changes	Editor	Date
1.4	Creation and initial edits	Chris White, The South East Cyber Resilience Centre	20/9/21
1.5	Refresh content	Chris White, The South East Cyber Resilience Centre	5/4/23
1.6	Edits	Chris White, The South East Cyber Resilience Centre	7/6/23
1.7	Edits and refresh content	Sian Mason, The South East Cyber Resilience Centre	15/7/24

THE
SOUTH EAST CYBER RESILIENCE CENTRE