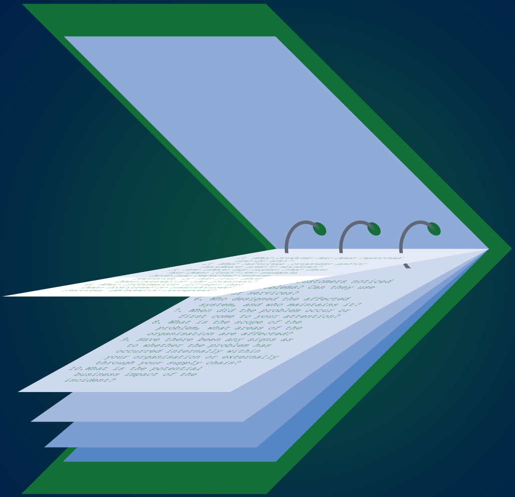
National Cyber
Security Centre
a part of GCHQ

Cyber Security

Response and Recovery

Small
Business
Guide
Collection

How to prepare for a cyber incident, from response through to recovery


customers noticed
elems? Can they use
r services?
6. Who designed the affected
system, and who maintains it?
7. When did the problem occur or
first come to your attention?
8. What is the scope of the
problem, what areas of the
organisation are affected?
9. Have there been any signs as
to whether the problem has
occurred internally within
your organisation or externally
through your supply chain?
10.What is the potential
business impact of the
incident?

Contents

[1] https://www.ncsc.gov.uk/collection/small-business-guide

[2] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/incident-management

[3] https://www.ncsc.gov.uk/collection/board-toolkit/planning-your-response-to-cyber-incidents

[4] https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

[5] https://report.ncsc.gov.uk/

Introduction

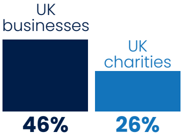
It's natural for all organisations to experience bumps in the road. As a UK business there is around a 1 in 2 chance that you will experience a cyber breach*. When something unexpected happens, such as a cyber incident, it can be difficult to know how to react. Naturally, you will want to resolve the problem as quickly as possible so you can resume business as normal.

For these reasons, the NCSC has created this Small Business Guide to Response and Recovery. It provides small to medium sized organisations with guidance about how to prepare their response, and plan their recovery to a cyber incident. It's a companion piece to our guidance on how to protect yourself from cyber attacks[1].

If you're a larger business, or face a greater impact from a cyber incident, then the Incident Management section in 10 Steps to Cyber Security[2] can further help your cyber response.
Board members should refer to our guidance on planning your response to cyber incidents[3].

What is an incident?
The NCSC define a cyber incident as unauthorised access (or attempted access) to an organisation's IT systems. These may be breaches (when you're aware of the unauthorised access of data or systems) or malicious attacks (such as denial of service attacks, malware infection, ransomware or phishing attacks), or could simply be accidental events (such as damage from fire/flood/theft).

Reporting incidents
If you are experiencing a live incident, call Action Fraud immediately on 0300 123 2040 and press 9 on your keypad. This will allow your call to be dealt with as a priority and your live incident will be triaged over the phone. Next your incident will be passed to the National Fraud Intelligence Bureau (NFIB) who will review your report and conduct a range of enquiries, it may then get passed to the relevant police agency. You will be kept informed of the status of your report. If your organisation has been the victim of a significant cyber attack[4], the NCSC recommends that you start by reporting the incident to us[5].



of businesses/charities identified cyber security breaches or attacks in the last 12 months

£3,230
is the average annual cost for organisations that identified breaches with an outcome

Among the 46%/26% identifying breaches or attacks:

27%
42%
Needed new measures to prevent future attacks

20%
33%
Added staff time to deal with breach or inform others

14%
22%
had staff stopped from carrying out daily work

32%
22%
identified at least one breach or attack a week

*Source: The Department for Digital, Culture, Media and Sport's 'Cyber Security Breaches Survey 2020'

Step 1: Prepare for Incidents

Unforeseen events, both malicious and accidental, can occur in many ways. So it is impractical to develop detailed step-by-step instructions to manage every type of incident, as the list could be endless. Instead you should prepare your business for the most common threats you face by developing plans to handle those incidents most likely to occur.

Identify critical systems and assets

Identify what electronic information is essential to keep your organisation running, such as contact details, emails, calendars, and essential documents. Find out where this information is stored. Is it on single machine in your office? Is it on a remote server? Is it stored in the cloud, by a third party?

ACTION POINT: Make a regular daily/weekly back up copy of essential information. Regularly test that the backup is working to ensure you can restore information from it.

Next, identify what business processes and systems are critical to keep your organisation running. For example, the website where your customers place orders, or the computer-controlled manufacturing equipment you use. If you've not already done so, identify these key systems and processes as soon as possible, and record where they are stored (or how they are accessed).

ACTION POINT: Assign joint (or shared) responsibility with another person to ensure there's cover when you aren't available (for instance when on holiday, or away with business). Ensure key documents are made available and are up to date so that in the event of your absence they can be shared/learnt by other relevant people.

Finally, think in advance about how you could minimise reputational damage in the event of an incident. Which key partners do you need to talk to? Building a good relationship with your partners, where you talk regularly before an event has even occurred, will make things a lot smoother in the event of an incident.

ACTION POINT: Make a list of which key partners (customers, suppliers, third parties, etc) that you would need to contact as a result of different types of incident. For example, you would need to contact customers and banks if payment data was compromised, suppliers if corporate accounts were attacked, and the ICO if personal customer data was stolen.

Prioritise the risk, and manage it

Consider what would happen if you no longer had access to the critical systems or assets you've identified above. By understanding:

- what's important to your business
- why it's important, and
- what you are doing to protect them

- you can prioritise where you need the most protection. If you need more help with identifying your 'crown jewels' (i.e. the things most valuable to your organisation), please refer to our guidance on establishing your baseline and identifying what you care about most[6].

Put risk on the agenda

Discussions about organisational risk (what you value, and what you're doing to protect it) should be part of normal business. Make time to discuss these at your management meetings or weekly catch-ups. Find out where cyber security threats sit in the priority list when compared to physical threats (like burglary and stock theft), flood, legal action, and health and safety. The steps you choose to take to reduce the risk to your business have got to be proportionate to the risks you take, and of course affordable.

Organisations that are considering cyber insurance should understand that it will not protect you from an attack, but it may provide you with additional resources during and after an incident. So cyber insurance can be considered as an additional risk management tool, but do take time to:

- understand the scope and scale of the cover provided
- ensure that you are able to meet any operational requirements placed on you by the insurer

[6] https://www.ncsc.gov.uk/collection/board-toolkit/establishing-baseline-identifying-care-about-most

Make an incident plan

Make sure you keep the important information you identified above in a safe place so that you can use it if your equipment is stolen or damaged by a cyber attack. Ensure you know how to restore a backup in the event of any type of data loss, such as a ransomware attack[7], and train the relevant people in your organisation so they can do the same. Assign roles to members of staff, and document who owns each responsibility in the event of an incident, and how can they be contacted.

ACTION POINT: The best way to test your staff's understanding of what's required during an incident is through exercising. Consider using the NCSC's free Exercise in a Box product[8] to test your organisations resilience and preparedness.

Understand and document possible incident 'trigger points' such as when ownership of an action or decision transfers between people. For example, an employee may own the action to identify when there's an issue with the website, but once that has been done, who decides if the website should be shut down? Your plan should identify at what point senior management needs to be involved.

Create a list of external people you need to contact who can help you identify an incident. For example, your web hosting provider, IT support services or cloud service provider. Document the details of the contract, including what is covered, how they can help you, and at what point do you need to engage with them. Being prepared and having relevant documents accessible and up to date could save you time post incident.

ACTION POINT: Have you got the most up to date contact information for those you need to contact? Is it stored in the right place and easy to access, keeping in mind that your normal means of communication may be disrupted during an incident? Schedule in time to check these details every couple of months or as necessary.

If you have Cyber Insurance, have your insurer's details documented including policy number and any specific information your provider asks for. Understand any legal or regulatory compliance you must adhere to and implement any guidelines/policies/rules they set out for you. You should check if your trade association has any help or advice lines that you can contact to help you in this situation.

[7] https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

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

Step 2:
Identify what's happening

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

Find out if you are being (or have been) attacked
Things that might indicate a cyber incident include:

- computers running slowly
- users being locked out of their accounts
- users being unable to access documents
- messages demanding a ransom for the release of your files
- people informing you of strange emails coming out of your domain
- redirected internet searches
- requests for unauthorised payments
- unusual account activity

Find out what's happened
The following 10 questions can help you identify what has occurred. It's a starting point that you can use to gather vital information as soon as you suspect something has gone wrong. The answers will help you provide essential information to your internal or external IT team who will be resolving the problem, and form part of your incident review/lessons learnt report.

10 crucial questions

1. What problem has been reported, and by who?
2. What services, programs and/or hardware aren't working?
3. Are there any signs that data has been lost? For example, have you received ransom requests, or has your data been posted on the internet?
4. What information (if any) has been disclosed to unauthorised parties, deleted or corrupted?
5. Have your customers noticed any problems? Can they use your services?
6. Who designed the affected system, and who maintains it?
7. When did the problem occur or first come to your attention?
8. What is the scope of the problem, what areas of the organisation are affected?
9. Have there been any signs as to whether the problem has occurred internally within your organisation or externally through your supply chain?
10. What is the potential business impact of the incident?

Stop the incident getting any worse
Take a look at your security software (such as antivirus alerts and server/audit logs) to see if you are able to identify the specifics of the attack, and subsequently the cause of the incident. If you are unable to do this (but you know which device has been affected) run your antivirus programme to complete a full scan[9], and take notes of the results it gives you. If nothing is found, consider using an alternative antivirus programme.

Use the information you have gathered to look for advice online from trusted sources such as police or security websites. You may be able to find instructions there on how to fix the problem, although care should be taken before acting on unverified advice.

In the case of internet outage, contact your ISP (using the details you've already identified in your incident plan) in the first instance; most will have pages that relate to service availability. You might learn that the outage is due to a fallen tree, rather than a DDoS attack. In addition, ensure that you understand your provider's escalation process, and know what data they need to act on, and what type of SLA/support you have paid for.

[9] https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product

Step 3: Resolve the incident

The actions in this step will help your organisation get back up-and-running as soon as possible. You'll also need to confirm that everything is functioning normally, and fix any problems.

If your IT is managed externally: contact the right people to help
Contact your external IT providers (that you've identified in Step 1) to help you fix the problem. These contacts are there to fix the problem and establish the impact to your organisation.

If you manage your own IT: put your plan into action
It's time to activate the incident plan you made in Step 1. Depending on the type of incident you are responding to, this may involve:

- replacing infected hardware
- restoring services through backups
- patching software
- cleaning infected machines
- changing passwords

ACTION POINT: If you're considering using services from a cyber security consultant[10], take appropriate steps to make sure you use reputable organisations, understand their experience, and know how their offer meets your requirements and your business type. Relevant technology qualifications are a plus. This will help you to choose a provider that suits your organisation.

[10] https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?productType=Consultancy&start=0&rows=20

Step 4:

Report the incident to the wider stakeholders

Once a cyber security incident has been resolved, formal reporting will often be required to both internal and external stakeholders. There are certain incidents that you're legally obliged to report to the Information Commissioner's Office (ICO), regardless of whether your IT is outsourced. Check the ICO website[11] to find out which incidents require this. Other regulatory bodies which you belong to may also require you to report a breach.

Report to law enforcement

Always remember that a cyber attack is a crime. Report to law enforcement via Action Fraud[12] or through Police Scotland's 101 call centre. The NCSC strongly encourage the reporting of a cyber incident; many go unreported because of personal embarrassment. However, if a cyber incident has been committed against you, someone else may have suffered a similar crime. The more individuals report, the more likely it is that perpetrators will be arrested, charged and convicted.

Keep everyone informed

It's important to keep your staff and customers informed of anything that might affect them (for example, if their personal data has been compromised by a breach).

ACTION POINT: Make staff aware of any incidents at a time that is proportionate to the effect of the incident. So, if you have experienced a minor incident out of hours, is it proportionate to contact staff in the middle of the night? If relevant, contact your customers as soon as possible through the most appropriate channels.

Consider legal advice

You might want to consider seeking legal advice if the incident has had a significant impact on your business and/or customers. If you have a cyber insurance policy, they will be able to provide you with more advice.

[11] https://ico.org.uk/for-organisations/report-a-breach/

[12] https://www.actionfraud.police.uk/report_fraud

Step 5:
Learn from the incident

After the incident, it's important to:

- review what has happened
- learn from any mistakes
- take action to try and reduce the likelihood of it happening again

Not only is it important to review your technical controls after the incident, it is also a great opportunity to review and implement staff awareness or training measures to help develop your staff's security culture.

Review actions taken during response
Collate and review the actions you documented throughout the response to the incident. Make a list of things that went well and things that could be improved from the response stage.

Review and update your incident plan
Where necessary, make changes to the incident plan you created in Step 1, to reflect the lessons learnt.

Strengthen your defences
Reassess your risk and make any necessary changes. For example, if you were a victim of a password attack you may need to create a new password policy, provide new training, provide physical secure storage for passwords (or password manager apps) for your staff.

Consider the terms of your contracts
Depending on how successful the incident response was, you may need to make a strategic decision on your third party contracts. You might want to consider the following:

- Does this incident mean the way that you do business has to change?
- If you currently outsource, did their response meet your needs?
- If they didn't meet your needs consider renegotiating the terms of the contract or cancel, changing to a new company.
- Did you have the skills in-house to do it yourself, negating the need to outsource in the future?

For further information, or to contact us, please visit: **www.ncsc.gov.uk**

@NCSC

National Cyber Security Centre

@cyberhq

Information correct at the time of publication - October 2020

Designed and created by Agent Marketing Ltd.
agentmarketing.co.uk