Business Guide

Protecting you and your Business against Cyber Crime

Lancashire Cyber Crime Unit

Contents

This guide provides an overview of steps that can be taken to help protect your business against the threat of cyber crime.

Contents:

Risk

Assessing and managing risk can help identify cyber security provisions your business needs to put in place.

Risk Assessment

Many cyber attacks use indiscriminate scatter-gun approaches to targeting victims. If you're an SME or sole trader, you're just as likely to be a victim of these scatter-gun attacks as a large organisation. Attackers may not know who you are until they get a foothold in your organisation.

Cyber security is as much about knowing how your organisation functions as it is about technology. Think about the critical people, information, technologies and business processes to your organisation. Some information (such as personal data) must remain private, but other types of information could be released without any disruption. This basic understanding of **what** you care about, and **why** it's important, should help you to prioritise where to protect your organisation most.

Risk Management

The ability to visualise the future consequences of your decisions - some of which cannot be easily predicted - is essential to risk management. You can't explore every scenario in which you could be compromised, but you shouldn't let that put you off. It might seem natural to start with a decision you've taken, such as adopting a particular password policy in your organisation, and to work forwards from there to explore the consequences. However, it can be more useful to start with an outcome that you want to avoid, and then work backwards.

Quick Tip:

Utilise NCSC resources visit https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security

GDPR

GDPR is an important consideration for Cyber Security and businesses should be aware of this legislation.

General Data Protection Regulation (GDPR)

Requires businesses to protect personal data by processing data securely with the appropriate technical and organisational structures.

If affected by a cyber threat which could lead to a breach of personal data, there is an obligation under GDPR to notify the Information Commissioner's Office (ICO) within 72 hours. Failure to notify the ICO may result in a significant fine! For more information on GDPR visit https://www.ncsc.gov.uk/information/GDPR

The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. The Regulation does not mandate a specific set of cyber security measures but rather expects you to take 'appropriate' action. In other words you need to manage risk.

ICO

The ICO is the UK's supervisory authority for the GDPR and is responsible for promoting and enforcing the legislation, as well as providing advice and guidance to organisations and individuals. The ICO has published a lot of helpful guidance and advice at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

The NCSC have also worked with the ICO to develop a set of GDPR Security Outcomes. They can be found at https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes.

Quick Tip:

If you want to improve your cyber security further, then you can also seek certification under the Cyber Essentials scheme. The scheme demonstrates to clients that you take the protection of their data seriously.

Backing Up Data

Backups help to restore computer devices during the process of disaster recovery and restore data after files have undergone damage or deletion.

Identify Essential Data

- Identify critical data that your business cannot function without and back-up this data **OFF YOUR NETWORK**. For more information visit https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world
- Ensure the separate backup is not permanently connected to your network. Store it on an external drive/ USB which is not accessible to staff.
- Consider storing backups in a different location, so theft or fire won't result in the loss of both copies.

Utilise Cloud Storage Systems

- Utilising cloud storage systems is a cost-effective and efficient way of achieving a secure back-up physically separate to your business network.
- Cloud services offer a limited amount of storage space for free however, a larger space can be purchased at small costs.
- Implement automatic back-ups to ensure that data is maintained and kept up-to-date. This will ensure that the latest versions are available.
- Service providers can supply your organisation with data storage and web services without the need to invest in expensive hardware up front.

Quick Tip:

For more information about back ups within your business visit https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data

Mitigating Malware

The implementation of defence in depth can help mitigate an attack on your company.

Malware is malicious software which, if able to run, can cause harm in many ways including:

- Causing a device to become locked or unusable.
- Stealing, deleting or encrypting data.
- Taking control of your devices to attack other organisations.
- Obtaining credentials which allow access to your organisation's systems or services that you use.
- Mining cryptocurrency.
- Using services that may cost you money (e.g. premium rate phone calls).

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the NHS in May 2017. Normally you're asked to make a payment (often demanded in a cryptocurrency such as Bitcoin), in order to unlock your computer (or to access your data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. The NCSC supports the National Crime Agency (NCA) recommendations. The NCA generally advise **not** to pay the ransom, as there is no guarantee that you will get access to your device (or data).

Using a Defence in Depth Strategy

Since there's no way to **completely** protect your organisation against malware infection, you should adopt a 'defence-in-depth' approach. This means using layers of defence with several mitigations at each layer.

1) Make regular back-ups
2) Prevent malware from being delivered to devices
3) Prevent malware from running on devices
4) Limit the impact of infection and enable rapid response

Quick Tip:
For more information on defence-in-depth visit
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Mitigating Malware

The implementation of defence in depth can help mitigate an attack on your company.

1) Install (and turn on) antivirus software

Antivirus software should be used on all computers and laptops. For your office equipment, you can pretty much click 'enable' and you're instantly safer. Smartphones and tablets might require a different approach and if configured in accordance with the NCSCs EUD guidance, separate antivirus software may not be necessary. Visit the EUD guidance here: https://www.ncsc.gov.uk/collection/end-user-device-security

2) Prevent staff from downloading dodgy apps

You should only download apps for mobile phones and tablets from manufacturer-approved stores. These apps are checked to provide a certain level of protection from malware that might cause harm. Staff accounts should only have enough access required to perform their role, with extra permissions (i.e. for administrators) only given to those who need it. When administrative accounts are created, they should only be used for that specific task, with standard user accounts used for general work.

3) Keep all your IT equipment up to date

For all your IT equipment make sure that the software and firmware is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (a process known as patching) is one of the most important things you can do to improve security - the IT version of eating your fruit and veg. Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option.

At some point, these updates will no longer be available (as the product reaches the end of its supported life), at which point you should consider replacing it with a modern alternative.

4) Control how USB drives can be used

It only takes a single cavalier user to inadvertently plug in an infected stick (such as a USB drive containing malware) to devastate the whole organisation.

When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by blocking access to physical ports for most users, using antivirus tools, only allowing approved drives and cards to be used within your organisation - and nowhere else.

Make these directives part of your company policy to prevent your organisation being exposed to unnecessary risks. You can also ask staff to transfer files using alternative means (such as by email or cloud storage), rather than via USB.

5) Switch on your Firewall

Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on. For more detailed information on using firewalls, refer to the Network Security section of the NCSC's 10 Steps to Cyber Security at https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/network-security

Phishing

Phishing concerns communication from another who purports to be someone else in an attempt to steal personal information.

Implementing a Multilayered Approach:
Typical defences against phishing often rely exclusively on users being able to spot phishing emails. This approach will only have limited success. Instead, you should widen your defences to include more technical measures. This will improve your resilience against phishing attacks without disrupting the productivity of users.

1) Make it difficult for attackers to reach your users

- Don't let your email addresses be a resource for attackers.
- Reduce the information available to attackers.
- Filter or block incoming phishing emails.

2) Help users identify and report suspected phishing emails

- Carefully consider your approach to phishing training.
- Make it easier for your users to recognise fraudulent requests.
- Create an environment that **encourages users to report phishing attempts.**

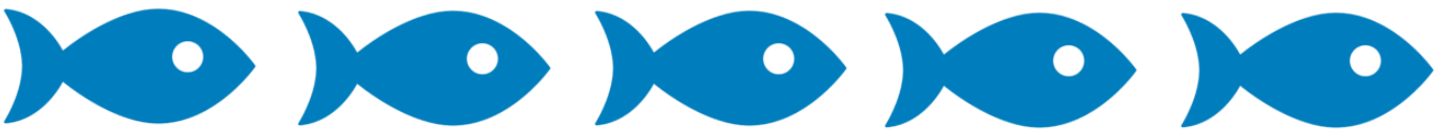
3) Protect your organisation from the effects of undetected phishing emails

- Protect your devices from malware.
- Protect your users from malicious websites.
- Protect your accounts with effective authentication and authorisation.

4) Respond quickly to incidents

- Detect incidents quickly.
- Have an **incident response plan.**

The NCSC are encouraging organisations to lead by example and set up DMARC and begin to ask their contacts to do the same. It's in everyone's interest to promote widespread adoption as the more organisations that take park, the harder it is for phishing attacks to succeed.



Quick Tip:
For guidance on implementing a multilayered approach in your business visit https://www.ncsc.gov.uk/guidance/phishing

Password Safety

Passwords offer first line defence for potential cyber attacks, ensure they are strong to deter the likelihood of an attack on your business.

Password Guidance

- NCSC recommends that passwords are 12-26 characters long and include a mix of upper and lower case letters, numbers and special characters. A minimum of three random words should be utilised as the base of your passwords.
- Avoid predictable passwords or passwords that are somehow related to your business.
- Activate two-factor authentication on all company accounts and encourage staff to utilise biometrics if available. Both techniques add an extra layer of security to your accounts.

Change all Default Passwords

- It is important to change default passwords to deter unauthorised access to business devices or accounts.
- Encourage employees to change any default passwords when provided with them.

'Password Overload'

- Reusing the same password across different business accounts can be dangerous. A cyber criminal may steal one passwords, and then access other accounts. This means they could break into several accounts despite only knowing one password. Encourage employees to have different passwords for their business accounts.
- To help employees remember different passwords for accounts, password managers can help.
- For more information on password managers please visit https://www.ncsc.gov.uk/collection/passwords

Quick Tip:

Ensure your password is not on this list of the most common 100,000 passwordshttps://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt

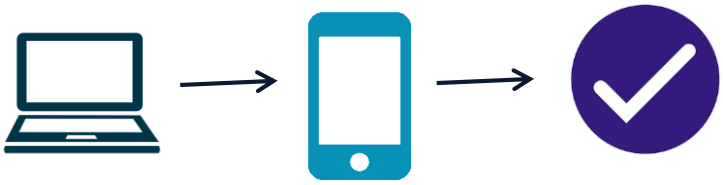
Two-Factor Authentication

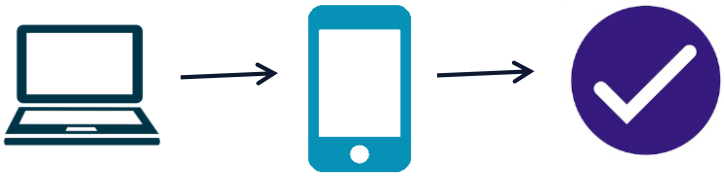
Activating two-factor authentication (2FA) provides a way of checking that you are really the person you are claiming to be.

However good business passwords are, they can only provide so much protection. They could be stolen from your service provider or from devices. Therefore, it is important to utilise 2FA on all business accounts.

What is 2FA?

- 2FA offers an added layer of protection on important online accounts and is relatively easy to activate on many popular sites and applications.
- Accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they won't be able to access the accounts.
- When setting up 2FA, the service will ask you/employees to provide a 'second factor', which is something that you or the employee can access. This could be a code that's sent to a phone by text message, or that's created by an app.





Implementing 2FA

- Activating 2FA on business email accounts can help protect sensitive information. For further information visit https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online?curPage=/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email
- Since any 2FA is better than none, you should use 2FA wherever you can within your business. It only takes a few minutes to set up for each account, and it's well worth it for the amount of additional protection it gives you.

Quick Tip:

Visit https://www.telesign.com/turnon2fa/tutorials/ for guidance on setting up 2FA on online accounts

CiSP/ Cyber Essentials

CiSP and Cyber Essentials are two initiatives that can help keep you update with current cyber threats and guard your organisation from attacks.

Cyber Security Information Sharing Partnership (CiSP)

CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

Benefits of CiSP:

- engagement with industry and government counterparts in a secure environment
- early warning of cyber threats
- ability to learn from experiences, mistakes, successes of other users and seek advice
- an improved ability to protect their company network
- access to free network monitoring reports tailored to your organisations' requirements

To find out more and register your organisation visit
https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-

Cyber Essentials

Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

There are two levels of certification:

1) Cyber Essentials

Our self-assessment option gives you protection against a wide variety of the most common cyber attacks. This is important because vulnerability to simple attacks can mark you out as target for more in-depth unwanted attention from cyber criminals and others.

2) Cyber Essentials Plus:

Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.

Crime in Action

Understanding what to do when experiencing a cyber attack is essential to ensure you can get your business running as normal, as soon as possible.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

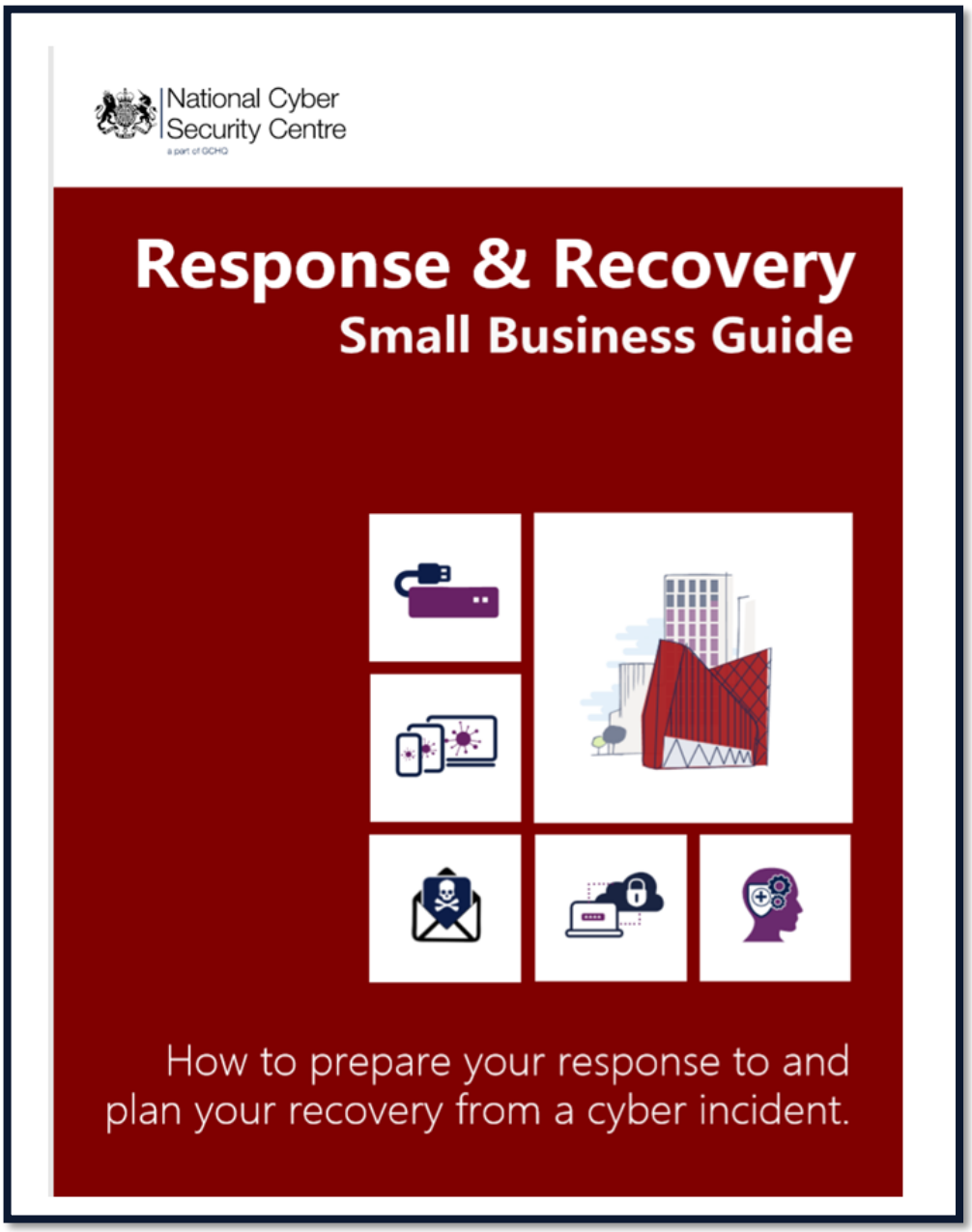
If you are experiencing a live incident, call Action Fraud immediately on 0300 123 2040 and press 9 on your keypad. This will allow your call to be dealt with as a priority and your live incident will be triaged over the phone. Next your incident will be passed to the National Fraud Intelligence Bureau (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.

Access the NCSC small business guide: response and recovery at: https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

Don't forget GDPR!
Your will have 72 hours to report a data breach to the Information Commissioner's Office.

NCSC Guidance

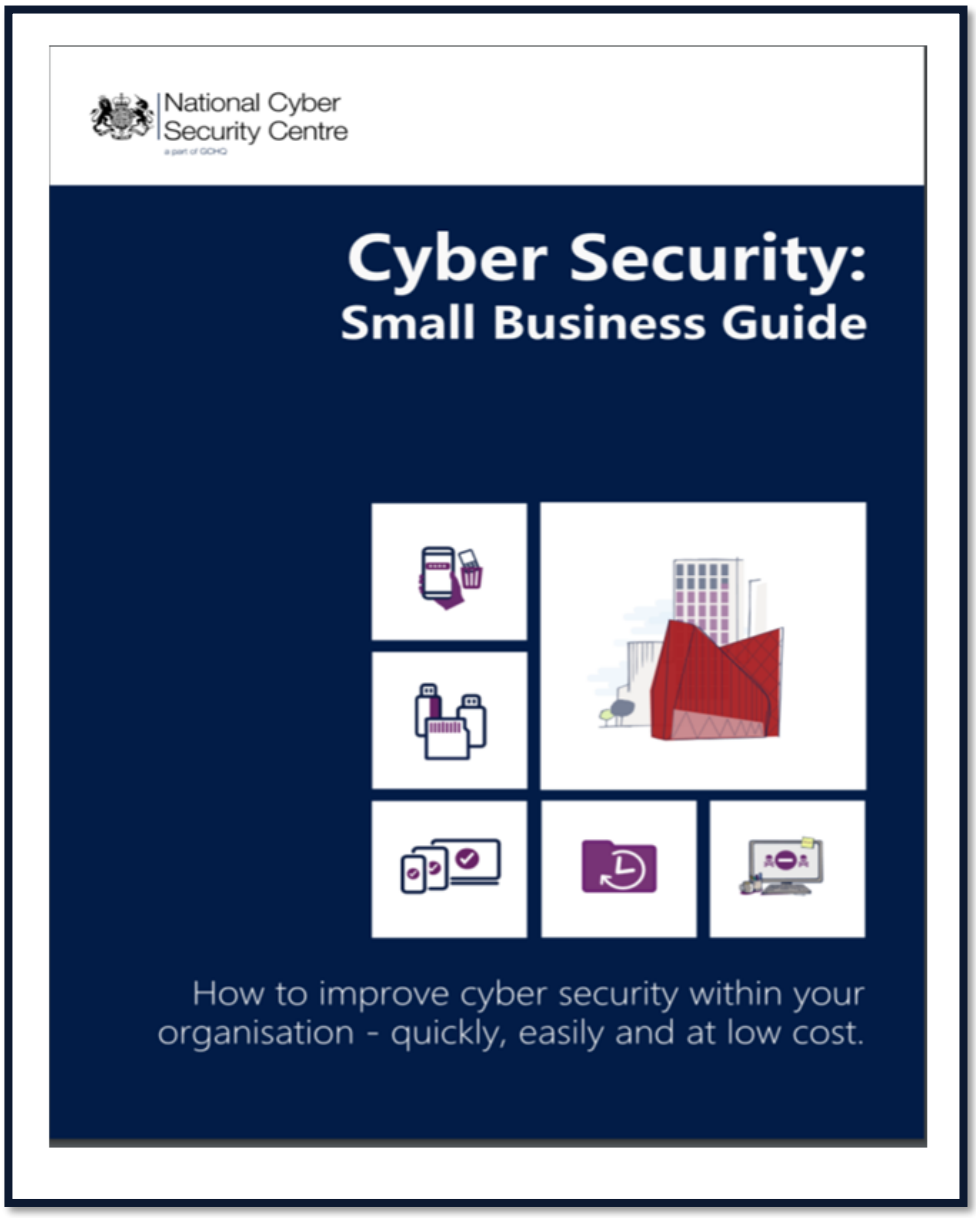
Utilise the NCSC Response and Recovery Small Business Guide to help you deal with the repercussions of an attack.



https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery

NCSC Guidance

Utilise the Cyber Security Small Business Guide to help improve cyber security within your organisation.



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

Support

CiSP
https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

Cyber Essentials
https://www.cyberessentials.ncsc.gov.uk/

National Cyber Security Centre
https://www.ncsc.gov.uk/

Action Fraud
https://www.actionfraud.police.uk/

Take 5 to Stop Fraud
https://takefive-stopfraud.org.uk/

Get Safe Online
https://www.getsafeonline.org/

Turnon2FA
https://www.telesign.com/turnon2fa/

No More Ransom
https://www.nomoreransom.org/

The Cyber Helpline
https://www.thecyberhelpline.com/