Cyber Security Health Check

Level 1 • Data & Info Security

Securing your business.

0330 174 9996
info@start-digital.co.uk
start-digital.co.uk

Start Digital

What is this Document?

What is this document?

This document is a cyber security audit; you will filter through and answer each question to improve your business's cyber security one easy step at a time.

We describe **what to do**, as well as **what not to do**. This is labelled as **Good Practice** and **Bad Practice**. You may find that some of your current practices or behaviours fall in to the **Bad Practice** category. This cyber security audit will be a key part of your cyber security journey, and show you what you are missing to secure and protect your business online.

This document's core topics will help you know how to answer questions similar to:

> *How do I avoid losing control of my social media accounts?*
>
> *How do I avoid email breaches?*
>
> *How do I recover compromised accounts? (Social/Email)*
>
> *How can I secure my website?*
>
> *Am I doing well with keeping my data safe?*
>
> *Do I have contingency plans ready in case anything goes wrong with my social media/email/website/data?*

Why these core topics are Important:

This document will cover the core topics listed above, as some of them can be easily overlooked by many people. From unskilled all the way up to people who are very skilled with technology. This document will help give you and understanding of your goals and aims regarding these topics. Using the topics covered in this document is a good baseline to help you plan your business's future cyber security plan of action.

What you hope to achieve by completing this document:

The goal of this document is to get you started on your cyber security journey, no matter how small or big the first steps are, any step in the right direction is important.

This is a document you may want to refer back to before and after you've implemented your business's new cyber security policies and procedures.

Performing an Audit

How to Use this Document:

This document is laid out in a very simple user-friendly way, with four core columns to focus on. The four columns are set out for you to follow from left to right in the following way:

1: Do You Have?	2:Yes/No	3: Good Practice	4: Bad Practice
Example Question: Do you have a secure password?		**Example Good Practice** A combination of the below: • Capital Letters • Lower Case Letters • Numbers • Special Characters. • Minimum 12 characters • Long Phrases	**Example Bad Practice:** • Names • Dates • Numbers • Predictable Sequences • Short Single Words • Short Phrases
This is a question to **assess** if you have a **specified cyber security** practice in place Some of these questions may have a simplified version which may be easier to understand.	You will answer with a **Yes/No** in this box	This will be **our recommendation** of what you should do to solve your lack of cyber security labelled as a **Good Practice**. A **Good Practice** is a behaviour that is **identified** as an **industry standard way** of doing particular things.	This is a section where we go over common **Bad Practices**. If any of your **current** behaviours are listed in the **Bad Practice example,** then you should put a **no** in the **Yes/No** box and look at the **Good Practise** for an idea of what you should be doing instead.

How to Use the Total Score Table:

At the end of every module, there is a **Total Score** table. This table is where you **total up** all your **yes/no** answers **for each module** you complete:

Total Score:	*Y:* *N:*	*Notes:*
This is the **total number** of **yes/no** answers in the boxes to the **right**.	This is where you will put the **amount** yes and **no answers** you have **totalled** up per section.	You can use this box for any **additional notes** you want to make for each unit you have covered.

Data and Info Security

Data and Information Security:
Data/information is arguably one the most important things you need to keep secure, not just for customers, but also employees. Having sufficient security for data/information can reduce the risk of data breaches, and also reduce any damage to your reputation. When using/storing data, depending on what data you are collecting, you need to follow certain regulations/legislations to the best of your ability. This generally leads to keeping the data as secure as possible, but if you don't keep the data safe, it is possible for your business to get fined for adhering to data protection legislation.

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have a policy that covers making frequent backups of your business's important data?		Creating backups of your business's most important data, tools, software, and documents. This is not just in case of an outside threat, this also helps protect against mistakes that can be made by employees, or things like power outages. Having a backup policy helps protect against both outside and inside dangers. A backup is a copy of important files and data. A proper backup methodology requires you to have 2 backups locally on different media, and a third backup offsite. The best practice is to also encrypt your backups. Here are some example backup programs/services: • Acronis • AvePoint • Bacula • OneDrive business	You've never made a backup of sensitive, important or critical data. OR Don't regularly make a backup of sensitive or important information.
Do you have a policy to limit who can access certain data/information within the business?		Limiting access to only those who need it is an important step in limiting both outside and inside threats. If someone has access to programs or data they don't need, they could accidentally or even purposefully damage that data. This can cause a lot of unnecessary risk for a business. Here are some examples of access control services: • Kisi • ISONAS • Brivo • Johnson Controls • Pulse Policy Controls To help with this, implementing an access control policy to limit your employees' access to data and software they need to do their role greatly improves security.	Letting employees or staff access all files and documents at all times even though they don't need full access to carry out their job role.

Data and Info Security

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have a process for encrypting the data you store?		Data encryption is very important when it comes to sensitive data. If someone gets hold of encrypted data, they cannot do much without the decryption keys for the data. In most circumstances, the person responsible for encryption is also responsible for the encryption keys. This can reduce a lot of risk that comes with holding sensitive data. Here are some examples of encryption services: • IBM Security Guardium Data encryption • AxCrypt Premium • Boxcyptor • Checkpoint full disk encryption software blade Use the information gathered to encrypt data, that is required by your business.	Not encrypting any data, you store/hold. Especially if the data is sensitive and contains personal data on customers or users.
Do you have any sensitive/personal data stored and know about legislation regarding storing this data?		The storing of sensitive data such as a customer or user's name, address, date of birth, etc, can open you up to legal troubles if you do not take the minimum required precautions to protect that data. When storing this sensitive personal data, there are different pieces of legislation around the world for how you are legally obligated to store and or use it. When storing personal and sensitive data about UK citizens, the following legislation is applicable: • The Data protection act 2018 When storing personal and sensitive data about EU citizens, the following legislation is applicable: • GDPR	Storing personal or sensitive customer data without knowing and or following the required legislation.
Do you have an understanding of what your General Data Protection Regulation (GDPR) requirements are?		GDPR is legislation within the European Union which gives EU countries' citizens more rights over their data. This means you need to take extra precautions on how you are storing and collecting data related to EU based citizens. To have a full understanding GDPR, you can find the full documentation here: https://gdpr-info.eu	Not knowing what General Data Protection Act is and how it works regarding storing personal/sensitive data. AND/OR Not following GDPR

Data and Info Security

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have an understanding what your Data Protection act 2018 requirements are?		The Data Protection (DPA) act 2018 is the United Kingdom's equivalent of GDPR. There are minor differences between them that are mainly focused of a person's individual identity. The biggest differences between GDPR and DPA are: • Age of consent for the law • Personal Information • Ethnic background • Political opinion • Religious beliefs • Health • Sexual life • Criminal History To have a full understanding of The Data Protection Act 2018 you can find the full documentation here: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.	Not knowing about, and not following the requirements of the Data Protection act 2018
Do you have an understanding of what legal requirements you need to follow to safely print documents that could contain sensitive data?		To use printers while following the correct legislation, there are a few key things you need to follow: • Don't leave documents in printer tray or scanner bed • Don't leave documents on your desk for people openly to see • Don't use an unsecure recycling bin • Secure shred any paper documents with personal data on them • Printers should be in view of a CCTV camera Extra steps that can be taken if your printer is compatible are: • Secure print (biometric secured) • Password protect your printer.	Storing personal or sensitive customer data without knowing and or following the required legislation.
Do you have an understanding of what is required from you if you want to share any data you gather?		To share personal data with third parties outside your business, consent from the user is required when first collecting the data. This includes how many parties you will be sharing the data with. When you're sharing data, you also need a lawful basis to do so which can include: • Legal Obligations • Performing contracts with an individual • Protecting someone's vital interests • Performing public tasks • Consent	Not knowing the regulation requirements to share data with other parties outside of your business.

Data and Info Security

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have regular staff training sessions?		Learning how to correctly handle data is important with the possibility of fines from different organisations. Training staff is a huge part of making sure data is handled correctly, this will reduce the chances of any fines that the business may need to pay with bad data management. Due to legislation (GDPR, DPA, etc.) depending on how sensitive data is handled it can end up with your business getting fined, so making sure your staff are properly trained to handle data is an important task.	Not having staff understand their requirements when managing and interacting with data.
Do you have an understanding of what the Information Commissions Office (ICO) responsibilities are?		The information commissioner's office is an independent regulatory office. They work on behalf of the public. If members of the public have issues or concerns with how their data is being handled, they are able to go to the ICO to get help in resolving their issues or concerns. The ICO covers different types of legislation such as: • GDPR • The data protection act 2018 • Freedom of information act To be in-line and be on good terms with the ICO, they have a lot of different resources on their website to help you understand how to ensure your own, and your business's actions are following the required legislation and best practices.	Not knowing what the Information Commissioner's office is and how they can affect your business and its practices.

Data and Info Security

Total Score:	Y:
	N:

Notes:

After completing this section, you should have a better understanding of your business's data security and the steps you need to take to improve. Making improvements in this area will reduce the chances of any data breaches, data leaks, and should help with getting back to normal work quickly after any breach occurs.