A QUICK GUIDE TO CYBER SECURITY

Understanding the types of cyber risks your business could be susceptible to is the first step in protecting yourself and your business from them.

The majority of small and medium-sized businesses rely on the internet to function in one way or another - and some are entirely online operations. With this reliance on the internet comes the potential for cyber security threats.

Unfortunately, the point at which many businesses become aware of a cyber security issue is when it is too late, with damage being done. In some cases this could be of negligible impact, but in many cases a lack of safeguards in place for a business's sensitive data / information can have a big (negative) impact on the company.

It is key to any business's success that they understand the risks their business may face and so must identify which risks they may be susceptible to.

The first step in doing so is to ensure that the responsibility for cyber security within a business is determined. The UK Government has released a paper (and accompanying toolkit) that explains why they believe this should be a board responsibility. You can read more here.

It is also very important to ensure that while overall responsibility lies with one person (or with the board of directors), all involved in the company's use of cyber-related software / hardware and the internet are regularly consulted by those responsible for overall cyber security. The reason for this is that each individual working across an organisation will have a different use for cyber-related software / hardware and the internet within the business and so may be able to offer perspectives on security measures that an overseer may not have considered.

Where possible, consult non-executive directors (or members of your business network!) to discuss best practices within other organisations, as well as tips and tricks that others have learned through their policies, procedures and in some cases, security breaches.

We are stronger together and learning from one another's successes *and* failures is key.

Risk Assessments are a great way to identify and understand the risks your business may face. Here are some questions to ask yourself when doing a risk assessment for the cyber security threats your business may face:

- **What types of data / information does your business handle / hold / process?**

  ie: what categories would they be in? Customer data? Company tax information? etc.

- **What data / information does your business handle / hold / process?**

Taking ‘customer data’ as an example of the type of data, examples of the data within this category could include names, addresses, date of birth, purchase history and more.

- **Does the data / information that your business handles / holds / processes need protecting?**

  The answer in the **vast** majority of cases will be yes. A good practice to follow is if you’re not sure, consider it to be in need of protecting.

- **Where is the data / information that your business handles / holds / processes?**

  The data / information could be saved directly to a computer or within a cloud storage system. It could be saved digitally or physically, on site or off site and in some cases with a third party.

- **Who has access to the data / information that your business handles / holds / processes?**

  You must be able to identify who can access materials that could be subject to a cyber threat, both within and outside of your organisation.

- **Can the data / information you have be consolidated or segmented as the need applies?**

  In some instances, segmenting or separating data can be of use so that not all the data you have that is susceptible to cyber threats is in one location and therefore available all in one location for any cyber criminals to access.

  Alternatively, consolidating some data can also be of use if, for example, you have customer records in physical form in some instances and digital in another.

- **Can the data / information you have be backed up securely?**

  In case of loss, damage or theft (for example, of a hard drive or computer), ensure that the relevant data / information is backed up securely (ie: with encryption, passwords, etc.) and in a secure location separate from the location of the original source of data / information.

- **Is there a fallback if all of the data / information that your business handles / holds / processes is lost?**

  This is possibly the most important question. What would you do if it was all lost? What effect would it have on your business? Answering these questions with a preventative strategy is of the utmost importance.

Alongside the questions listed above, many cyber risks for businesses can be connected to their suppliers. It is very easy to assume that another company has their own security measures in place but it is always worth

asking for information on their cyber threat policies to ensure you are happy working with them. And they may even have tips to help you with your own policies too!

Finally, the government initiative Cyber Essentials is a great resource for tools, tips and more with relation to cyber security for businesses. One fantastic tool they have is the ability for your business to gain a Cyber Essentials certificate which can help you gain a clear understanding of your business's cyber security level. On top of this, it will reassure your customers that your business is working to secure your IT against cyber attacks as well as attract new customers who will be safe in the knowledge that your organisation has a high level of cyber security measures in place.

For more information on Cyber Essentials, please see here.

USEFUL LINKS:

- The National Cyber Security Centre: https://www.ncsc.gov.uk/
- Cyber Security Toolbook For Boards: https://www.ncsc.gov.uk/section/board-toolkit/about
- Cyber Essentials: https://www.ncsc.gov.uk/cyberessentials/overview