

UNDERSTANDING CYBER RISKS FOR YOUR BUSINESS

WHY IT MATTERS

For many businesses, especially small operations, the threat of cyber crime is relatively low and easy to mitigate. By understanding the risks specific to your business and managing them appropriately, you can help ensure your business is protected.

Responsibility should lie with senior leadership as they understand the company best and have a broad view on what risks face the company. The link at the bottom of this document is an introduction to the cyber security toolkit and helps formulate an effective plan of action to tackle cyber risks.

RISK ASSESSMENT

Small businesses should organise information they keep, know where it is stored and prioritise it by level of importance.

- Examples of data that needs protecting are; personnel records, blueprints, tax forms, customer orders, credit reports, and customer payment records. Define the information type in a way that makes sense to your business
- Identify the digital and physical locations of the data, this includes where third parties are storing it. You should also note who has access to the information, where it goes and whether it is connected to the internet (as that increases the threat)
- Consider what data can be segmented so you do not have to keep it all together, so if there were a breach not all data would be at risk
- Assess all the risks and decide which ones are unacceptable, these must be a priority in your cyber strategy

SUPPLY CHAIN

Suppliers and service providers are a popular stem for cyber crime on small businesses. It is especially the case when companies use cloud services for key business functions such as invoicing, HR, finance and payroll. An effective risk assessment should include how your company would operate if one of these services suffered a breach or a denial of service. In many cases you may need to go for a paper-based/manual approach in such a situation.

CYBER ESSENTIALS

Cyber Essentials is a government initiative to help small businesses identify and prevent cyber attacks. Having a Cyber Essentials certificate will protect your business against common cyber threats, allow you to demonstrate to your customers your competence in tackling cyber threats and enable you to bid for government contracts. Links to this are provided below.

USEFUL LINKS

- Cyber Security Toolkit: <https://www.ncsc.gov.uk/section/board-toolkit/about>
- 10 Steps to Cyber Security: <https://www.ncsc.gov.uk/collection/10-steps>
- About Cyber Essentials: <https://www.ncsc.gov.uk/cyberessentials/overview>
- Cyber Aware Questionnaire: <https://www.ncsc.gov.uk/cyberaware/home#questionnaire>

Save trees, save paper. Please consider the environment before printing this document.