An Introduction to Cyber Security

Council for Small Business Australia

Our Objective

- This presentation from COSBOA aims to introduce you to cyber security and give you a basic understanding of key terms.

- By the end of this presentation you will:
  - *be able to define and describe what cyber security is*
  - *understand that cyber security is more than just a piece of software*

Cyber Security – Key Points

Cyber security is all about protection of your small business digital infrastructure, the information it holds, and your finances.

There is no silver bullet.

It requires a multi-layered approach.

Education is the first step!

Key Content:
What is Cyber Security?

- Cyber security is essentially the different things we do to protect our software, systems and hardware from a malicious cyber attack.

- It includes the training we receive, processes we create, anti-virus software we purchase etc. that is designed to protect.

- Cyber security is complex and requires a sustained engagement from everyone in the community to ensure we are protected.

- Small businesses are particularly vulnerable to attack as they are easy targets for criminal groups seeking to exploit software weaknesses.

Definitions

Cyber security or cybersecurity can be defined as:

"the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" – Google

"the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access" – WhatIs.com

"the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" – NICCS

Why Do We Need Cyber Security?

Small businesses are advised to develop a cyber security strategy to protect their business from criminals.

Criminals are increasingly moving towards cyber attacks to cause harm to small businesses and eventually steal from them.

This could be in the form of finance, intellectual property, or other data.

There are also a range of other people who may try to disrupt your business for political reasons, terrorism, etc.

What Does Cyber Security Consist Of?

Cyber security is not simply about installing a program on your computer. Software is not enough. You and your staff need a multi-layered approach to help prevent cyber attacks.

1. Understanding – business owners and staff need a solid understanding of cyber security issues and management tools.

2. Actions – the entire team in your small business need to take actions to prevent attacks. This includes developing procedures specific to your business.

3. Software – investing in anti-virus and cyber security software can help to minimise risk.

4. Insurance – ensuring that your business is insured in the event of a cyber attack.

Customisation

As KPMG notes in their 2014 Report 'Cyber Security', the key for business is customisation.

Each small business is different and needs to be aware of the risks associated with their particular operations. Staff should understand the risk and manage this by helping to develop a specific cyber security plan. This involves a range of customised strategies.

There is no 'silver bullet' for cyber security. Protection will never be 100% guaranteed, but by taking a series of small actions all designed to safeguard the business, cyber security threats will be minimised.

In Summary

- **Cyber security** is the techniques, software, processes, and actions that are taken to protect technology, software, data, and finances from unauthorised access.

- **There is no silver bullet.** No one action or software will protect a business. Multiple approaches are required.

- **Customisation is key.** Small businesses should to understand the threats to their business activities and customise their approach to suit their needs.