

Crime prevention advice for

The importance of addressing cyber crime



Cyber crime is affecting individuals and businesses on an unprecedented scale. It was reported in the Office for National Statistics Crime Survey that between March 2015 - March 2016 there were 5.8 million incidents of fraud and computer misuse. This highlights the importance of addressing the issue and in the case of businesses, putting it in the boardroom.

Why address Cyber crime?

- Businesses rely on connectivity - internet, telephone, conference calls, banking transactions etc.
- Cyber is the lifeblood of a business; it should therefore be considered a high priority in all strategic boardroom meetings.
- Prevention of attack or loss of data.
- Compliance with regulations.
- Prepared - Business Continuity Plan.
- The consequences are too great to not consider business defences:

The cost of recreating the lost data - either by buying new hardware and software or re-entering the lost data (which may not always be possible)

The cost of continuing without that data (availability)

The cost of informing others about the loss

A company that suffers a data loss can also suffer a loss in its reputation as a professional organisation. This problem is greatly magnified if personal data belonging to other people has been lost.

Taking the initiative

- Should not be a tick box exercise.
- Aim to go beyond the 'compliance' approach.
- Mainstreaming cyber means as well as ensuring your business is secure, it could also lead to new developments within the business.
- Government backed initiatives - Cyber Essentials.
- Overall peace of mind that you have done all you can to protect your businesses.

