

Cyber crime and the board

A half-day workshop

Overview

How confident are you that you and your fellow board members fully appreciate the full range of cyber crime and IT risks to which you are exposed?

If you're not as confident as you should be, then this workshop is for you.

Objectives

- Ensure that you have properly addressed the full range of risks around cyber crime.
- Highlight – and rectify – any gaps in your IT and risk governance.

Who should attend?

This overview workshop has been designed primarily for board members.

Workshop format

- Usually delivered as a half-day session
- Can also be delivered as a high-impact, bite-sized boardroom briefing session
- Highly interactive, with plenty of discussion around different scenarios and issues of specific concern to you and your organisation

Special features

This workshop can be tailored to meet your specific requirements. You can choose to follow the agenda set out below or you can talk it through with the trainer and set a new one. The choice is yours.

Meet the trainer

Stephen is an expert trainer and consultant with over 20 years' experience providing services to the private and public sector in fraud (cyber) risk management, data security / protection and internet investigations, and open source intelligence.

Agenda

This is an indicative agenda – a starting point for a conversation with you. Stephen would be happy to tailor it to your precise requirements.

- 1 **Update** – current impact of 'cybercrime'
- 2 **Key IT risks** – internal and external (including back-up failure, hacking, theft of data)
- 3 **WiFi, remote working, mobile computing**
- 4 **Concerns with social media**
- 5 **Cloud computing** – is it safe?
- 6 **IT legislation** – understanding your rights and responsibilities
- 7 **Creating a secure culture** – IT governance and controls

For a no-obligation discussion about running this workshop for your organisation on an in-house basis, just give us a call on 01582 463465.