PDA

Questionnaire:

How well is your organisation protected?

We have supported dozens of organisations with their information/cyber security, based upon best practice guidance from GCHQ, the UK Government, the Law Society and the ICO. How does your organisation compare?

YES	NO	KEY NETWORK CONTROLS (also required by Cyber Essentials)
		Our procedures set out the regularity of the review of our 'whitelist' and the name of the person responsible for its updating and control.
		Our procedures require that all USB and DVD ports are disabled except on specifically authorised workstations/ devices.
		We have procedures for amendment to user accounts and monitoring of online traffic in the event of notice of termination of employment/contract.
		We maintain a register or lists of approved applications, by device, for every device that connects to our network.
		Our procedures require that the Board receives a report, at least monthly, on the application of any patches (where such has taken place).
		KEY MANAGEMENT AND MONITORING
		Our Board reviews information/cyber security aspects on risk register at least every 6 months.
		All staff receive information security and data protection training at least every 6 months, including enhanced training for the manger(s) responsible for these aspects.
		We have a map/register documenting all of the personal data that we hold, meeting the requirements of Article 30 of the GDPR.
		Our procedures prohibit the use of removable media, unless specifically authorised or managed.
		Our procedures require the review, every day, of the list of spam/junk email received by our organisation to check for potential threats and Data Subject Access Requests.
		We have a register of all devices and the software on those devices that are used for remote/home working by staff or consultants to conduct the everyday work of our organisation.
		Our procedures prohibit the saving of documents saved on 'own' devices through messaging services, or email, unless specifically documented and sanctioned by our organisation.
		Our Business Continuity Plan clearly differentiates between device loss/failure, software failure and malicious attack, and it includes annually tested plans to resolve and mitigate them.
		We have a procedure for reporting on threats and attacks that are currently threatening our network.
		Our Board conducts monthly reviews of our register for recording information security breaches and near misses.

Count your 'Yes's	SNAPSHOT EVALUATION
0 - 10	**At significant risk:** Insufficient controls or monitoring taking place.
13-14	**At risk:** Gaps in controls and monitoring.
15	**Well managed:** Good general controls and monitoring in place.

Supporting your information security

PDA Legal's CyberChecked report
Ask us about it today or visit: www.pda-legal.co.uk

CyberChecked
by PDA Legal

PDA

A report that covers much more

How does CyberChecked compare?

PDA CyberChecked is a report; not a 'Standard'. You get an expert report that covers all of the requirements of Cyber Essentials, plus 10 other key factors that are proven information/cyber security safeguards.

(And, for Lexcel accredited organisations PDA CyberChecked supports and enhances your compliance.)

BEST PRACTICE REQUIREMENT	CYBER ESSENTIALS	PDA CYBERCHECKED	(For Lexcel accredited organisations) TOUCHPOINTS WITH LEXCEL v6.1
Firewalls and boundary controls	✓	✓ Enhanced	Requirement for firewalls at 3.2
Secure configuration of the network	✓	✓ Enhanced	Requirement for network configuration at 3.2
Control of user access	✓	✓ Enhanced	Requirement for user accounts at 3.2
Safeguarding against malware	✓	✓ Enhanced	Requirement for dealing with malicious software at 3.2
Managing software patching	✓	✓ Enhanced	Requirement for a register of all software and for a plan for updating and monitoring software; at 3.2
Homeworking and remote working	✓	✓ Enhanced	Requirement for security of assets at 3.2
Risk avoidance planning	✗	✓	Requirement for Risk Register at 5.1
Map of personal data	✗	✓	Requirement for documenting personal data at 3.1
File sharing / transfer	✗	✓	Requirement for security of assets at 3.2
Use of internet and email and messaging	✗	✓	Requirements at 3.3 (email) and 3.5 (Internet)
BYOD (Bring Your Own Device)	✗	✓	Requirement for security of assets at 3.2
Business continuity for information security	✗	✓	Requirement for business continuity review at 1.3
Dealing with threats (during/post-event)	✗	✓	Requirement for business continuity review at 1.3
Breaches and breach registers	✗	✓	Requirement for reviews of risk data at 5.18
Training	✗	✓	Requirement for data protection training at 3.1 and information security training at 3.2, and appropriate trainiwwng for staff at 4.3

Supporting your information security

PDA Legal's CyberChecked report
Ask us about it today or visit: www.pda-legal.co.uk

CyberChecked
by PDA Legal