Cyber Essentials 2022 Update

What has Changed and Why?

Since its launch in 2014 the government backed Cyber Essentials scheme has evolved to ensure that it stays effective and provides appropriate protection as cyber threats evolve. Following the recent review by a team of experts, a series of changes have been introduced to keep the scheme current. Here is our summary of the key changes which apply from January 24th 2022.

Cloud Services are now in scope

This is the biggest and most onerous (but very appropriate) change with cloud services now fully integrated into the 2022 update. Businesses are now responsible for assessing cloud services against the Cyber Essentials standards and applying the controls wherever possible. Previous iterations of Cyber Essentials assumed, to an extent, that security was handled by the provider and that they were secure by default. Applications firmly in scope now are, for example:

- Electronic ID services and related onboarding services
- Online search providers
- Microsoft 365/Office 365
- Salesforce
- Hosted Practice Management and Case Management systems

Businesses are now responsible for user access control and the secure configuration of these services and for ensuring that security updates and controls are implemented by the provider.

Devices used for home working are more in scope (But routers are not)

If you have employees working from home for any amount of time they are now classified as a 'home worker'. **The devices that they use** to access organisational information, whether they are owned by the organisation or are personal devices, are in scope for Cyber Essentials. Thin clients also fall into scope now when they connect to business information or services.

Prior to this update, one of the key issues was trying to secure and configure home routers provided by ISP's. This requirement has now been transferred directly to the device (PC, Laptop, Mobile Phone etc) where software firewalls should be applied along with other relevant protection.

So, the ISP supplied router is now out of scope, but if the business supplies the router then it is still in scope.

Mandatory Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) MUST now be used for all accounts when connecting to cloud services to provide additional protection. Previously only administrator accounts were mandatory and it was recommended to use MFA for other accounts.

Unsupported Software

All software installed on devices listed as being in scope must be:

- Licensed and supported

- Removed from devices when it becomes un-supported or removed from scope by using a defined 'sub-set' that prevents all traffic to/from the internet.
- Have automatic updates enabled where possible
- Updated, including applying any manual configuration changes required to make the update effective, within 14 days of an update being released.

Organisations now need to apply all high and critical updates for all systems without exception.

Passwords

When using passwords, **one of the following methods should be used** to protect against brute-force password guessing:

- Using multi-factor authentication (MFA)
- Throttling the rate of unsuccessful or guessed attempts.
- Locking accounts after no more than 10 unsuccessful attempts.

Technical controls must be used to **manage the quality of passwords**. This will include one of the following:

- Using multi-factor authentication (MFA) in conjunction with a password of at least 8 characters, with no maximum length restrictions.
- A minimum password length of at least 12 characters, with no maximum length restrictions.
- A minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list

Smart Devices

All smart phones and tablets connecting to organisational data and services are now in scope when connecting to corporate networks or mobile Internet such as 4G and 5G.

- Biometrics or a minimum password/PIN length of 6 characters must be used to unlock a device.
- The scope of an organisation must also include end user devices.

There is a grace period of 12 months to allow organisations make the necessary changes for the following requirements:

- The requirement for MFA will apply for admin accounts from Jan 2022 and the requirement for MFA for users will be marked for compliance from Jan 2023.
- The requirement for support and updates on Thin Clients will be marked for compliance from Jan 2023.
- Unsupported software remove from scope will be marked for compliance from Jan 2023

To explore what steps your practice should take now to protect your practice from cyber threats and to ensure that you can comply with these new requirements, get in touch with Frank Manning at Carton & Co. A preliminary discussion in confidence, with no commitment will cost you nothing and could save you and your colleagues financial loss, damage to your reputation and the stress that comes with every breach.

CONTACT: fmanning@cartonconsultants.com

Tel: 07778 572420

Or, you can schedule a 30 minute appoint with Frank at a time that works for you here >>