Data Governance and Cyber Essentials

Factsheet 42

Data governance is a popular subject at the moment with surveys, questionnaires and security reports all extolling its importance. This Factsheet explains how the 'Cyber Essentials' accreditation scheme can help firms with their data governance and keep them on the right side of the regulators.

The CE accreditation process forces firms to understand exactly how they manage their data and not just to guess or assume. It asks what security methods are already in place, such as firewalls, logins, virus prevention, passwords, data security protection routines, cyber incident reporting, software patching and controls, security policy standards for employees and the use of office technology, including mobiles.

In this way data governance can enable firms to collect and process data efficiently by using policies and standards for information and data collection in its day-to-day routines. It can also be used to ensure that the data is accurate, consistent, and complete. Understanding the make-up of this data, where it is located, who has access to it, and how often it is reviewed, helps optimised the data collected as well as its value.

Knowing who exactly has access to the firm's data is a key compliance aspect to CE accreditation and ensures only those who need access have it, and no one else. This minimises the likelihood of losing it or having it stolen, whilst ensuring the firm remains compliant with its regulator. It also helps with storage costs; the more refined the information and data is, the better.

Good data governance should make it simple for employees with the right credentials to gain access and block everyone else. Whether data is held on a Cloud based platform or in-house, the security of user ids, passwords, and multi-factor authentication credentials should now be a minimum standard. Included in this are current GDPR legislation and specific industry regulatory requirements, each warranting strict compliance.

Well-disciplined firms will already know to routinely update their information which might be stored at one or more location; perhaps the firm has more than one branch, using more than one Cloud provider requiring a 'single source of truth' (SSOT) to clearly identify their locations.

These elements are key to having a strict data governance strategy which security and privacy-conscious firms will already have built into their culture. Those yet to make a start or struggling, the task will be more difficult but nevertheless adherence to many of the Cyber Essentials data standards will help each to meet their own data governance standards.

Data Governance should not be seen as a chore but as a clear demonstration that the firm is taking its data security responsibilities seriously, giving them a competitive edge over their more hesitant rivals.

This link to the Government's publications Website helps explain the scheme in more detail.
www.gov.uk/government/publications/cyber-essentials-scheme-overview

Apply for further information and advice on Data Governance Cyber Essentials Accreditation
Phone: 01342 301325
Email: thebureau@the-bureau.co.uk