Law Society of Ireland

CYBER SECURITY ESSENTIALS

Law Society of Ireland, Blackhall Place, Dublin 7

Tel: +353 1 881 5768 | Email: solicitorservices@lawsociety.ie | www.lawsociety.ie

CYBER SECURITY ESSENTIALS

Purpose

The purpose of this document is to outline best practice for protecting your firms and client data and ultimately the reputation of your firm.

The document identifies key questions which need to be raised and the controls which need to be put in place to protect a firm's information. Cyber security is not a once off project but is a continuous task which involves constant amendments to your security controls and monitoring of events to ensure the correct level of security is always in place.

The guidelines can be used as a high-level guide when selecting a new system e.g. storing of your client documents in the cloud or when a cloud service like a new Practice Management system is being implemented from a new provider.

Everyone in the firm has responsibility for cyber security and must always be aware of security threats.

Data

It is important to have a clear understanding of where the firm's data is currently located. Here are some questions which need to be answered.

- What data does the firm currently store?
- Where is it stored
  - On premise or in the cloud
- What restrictions are in place to prevent unauthorised access to this data
- What security measures are in place versus the risk of losing certain data ie classify your data and the security measures you need to protect each data type
- Has a professional and certified security professional set up your environment/tenancy and does someone in your firm understand what controls should be and are in place? Assumption here is that your firm's data is in Microsoft's cloud but someone from your firm must agree on the 200+ settings in your tenancy. This is often overlooked and security breaches can occur if these settings are not set up correctly.

Risk Awareness in your firm
- Perform regular training re the latest risks
- Test after the end of training to ensure users can identify risks
- Test access to your firms building by using a third-party actor (Social Engineering)

Storing data on personal devices
- Ensure relevant controls are in place if data is stored on external storage devices ie password protected when a device is always inserted

Note: Storing of data on personal devices should be forbidden.

BYOD (Bring Your Own Device)
- What is your current policy?
- Is it forbidden in your firm to connect to network using your personal device.

Note: Preference would be to provide firm owned devices and ensure they are properly secured

Phishing scams
- Regular training
- Highlight recent scams
- Test at the end of the training session to ensure users can identify a scam versus a legitimate email

Password protocol
- Are unique passwords used for every system?
- Does the firm use a password manager?
- Is multi-factor authentication enabled?
- Are staff aware of password security?

Unused accounts
- Disable user accounts when a person leaves your firm
- Delete unused / inactive accounts after a specific period of time

Updates and backups
- Set updates like security and major application patches to be automatic
- Backup your data
    - On Premise - by using a leading industry standard application
    - Cloud – what controls are in place to back up your firm's data on a regular basis
- How are these backups tested?
- Do you have a local copy of key client data or are you relying solely on the cloud vendor / technology partner?

Note: Don't assume that your data is backed up by your cloud provider

Further Guidance, insights and template resources are available at www.lawsociety.ie/cyber-security

This resource was developed in consultation with the Law Society of Ireland.

Law Society of Ireland,
Blackhall Place,
D07 VY24
E solicitorservices@lawsociety.ie
W www.lawsociety.ie