Key Risk Checklist: Cyber Security

It is essential that firms take steps to prevent cyber-crime as practitioners are increasingly at risk of cyber-attacks. This is a list of the things firms need to do to at least *lock the door* on cyber-crime.

□ Ensure staff have **regular training** on cyber security and fraud prevention including:

- risks associated with clicking on links in email which may introduce viruses into the computer system
- using USB sticks that may introduce viruses into computer systems
- protecting passwords
- providing information to people over the phone.

□ Develop and implement an **office policy** about cyber security that addresses:

- storage of client information
- use of email
- use of USB sticks
- use of mobile devices and what to do when they are lost or stolen
- disposing of superseded devices and equipment.

□ Use a **business grade hosted email service** that includes quality filtering to block dangerous email; spam, phishing and malicious content or attachments.

Consider: Microsoft Office 365. You will need a custom domain name

□ Use a **DNS based web filtering** service to block high risk websites. This is a test website that should be blocked: www.malware.wicar.org

Consider: OpenDNS Umbrella
A free alternative is Norton ConnectSafe

□ Install a **reputable security software application** on every computer. Do not use free versions. Make sure it is configured so it will:

- update the signature database at least daily
- carry out a full scan of all files on the computer at least weekly.

Consider: Kaspersky Endpoint Security for Business

□ **Backup** all of your company files using an automated daily service that backs up to the cloud. It is essential that the backup service includes retention of at least three past versions.

Consider: Mozy Pro

□ Keep all of the **software on your computer up to date** by ensuring all updates and security patches are installed. Use Microsoft Update and make sure you get an alert from other software vendors when they release updates, then install these promptly.

□ Use only strong passwords that have a minimum of eight characters containing uppercase and lowercase letters, numbers and symbols. Change your passwords at least every 12 months. Use a password manager program to create and store passwords.

Consider: LastPass, KeePass or 1Password

□ More information

- For further information about cyber threats and security see the cyber security section on our website.
- Information about scams targeting practitioners which have resulted in claims can be found here.
- A blog about verifying emails from clients can be found here.
- A list of websites identifying scams can be found on our website here.
- Reports of the banning of USB sticks by the Pentagon can be found here.

Legal Practitioners' Liability Committee
October 2016

LPLC acknowledges the assistance of Ian Bloomfield of Ignite in preparing this checklist.