Cyber Essentials – simple, effective and affordable cyber security for the legal profession.

Are *you* in the cyber hot seat?

With reams of sensitive personal data and transactions that involve large sums of money, the legal sector is undeniably a massive target for cyber crime. Cyber Security - A thematic review published last year by the Solicitors Regulation Authority (SRA) reported the many costs of a cyber attack to a legal practice. Besides the obvious financial loss for both clients and practice (a loss of £4m client funds from 23 firms), the impact of a breach causes huge stress and damage to client relationships, increased insurance premiums and many indirect financial costs. For example, one firm lost around £150,000 worth of billable hours following an attack which crippled their system. pwc research showed that cyber security remains a key challenge for law firms and the sector is increasingly being targeted. Cyber risk was deemed the second greatest threat to law firms meeting and/or exceeding their ambitions, with only COVID-19 ranking higher. It has also been noted that SRA alerts for fraudulent activity are up 147% from the same period last year.

CYBER ESSENTIALS

Assured Service Provider
in association with
National Cyber Security Centre

It is now widely recognised that cyber enabled crime continues to rise in both scale and complexity, with criminals taking advantage of our increased reliance on digital technology. After nearly 18 months of remote working and more services going online, many firms are looking to adopt a hybrid work model that will allow their staff flexible working arrangements. This will mean that many professionals will work more than half of their working hours outside the security of the office network. Masters of opportunism, fraudsters can create scams overnight to take advantage of change. The Solicitors Regulation Authority reported a 300% increase in phishing scams in the first two months of lockdown alone, and every day we read about another breach, or ransom attack to hit law firms . The real problem is likely to be very much larger, due to the typical under-reporting of cyber crime and secrecy surrounding cyber breaches in the legal profession. It is not so much if you have a cyber breach, but when and how serious.

What is Cyber Essentials and how can it help?

The National Cyber Security Centre (a part of GCHQ) introduced the Cyber Essentials scheme as part of its mission to make the UK the safest place to do business online, and to offer businesses a simple and affordable way to tackle cyber security. IASME is the Government's Cyber Essentials partner, and responsible for delivering the scheme This is achieved in partnership with a network of over 260 Certification Bodies who are located all around the UK and Crown Dependencies. The Cyber Essentials controls help guard against the most common threats from the internet and certification helps to demonstrate your commitment to cyber security.

Cyber Essentials will:

Help you to take control of your cyber security

Although many legal firms outsource their IT support to third party providers and think that will take care of the problem, it must be emphasised that cyber security is not the same as IT and is not an IT problem. No matter who is looking after your technology, cyber security remains the responsibility of the senior management within your company.

The Law Society's Lexcel Standard guidance to legal practices states, "Practices must have an information management and security policy and should be accredited against Cyber Essentials. "

IASME has recently created the Cyber Essentials guide to using a third party IT provider to help you manage the responsibility of your cyber security when outsourcing your IT. A comprehensive list of questions is available on the IASME website for you to download or print off and give to your third-party provider. Ask your provider to return the answers and relevant lists to you so that you can check that your organisation has the controls in place to meet the requirements for basic cyber security.

Demonstrate your commitment to keeping client data safe

Reputation is a valuable asset and consumers are demanding evidence of a trusted, secure service provider for their sensitive data. They are increasingly aware of the threats from cyber-crime and they do not want their username/passwords compromised, their data stolen or their account hacked. Organisations need to show that they are taking cyber security seriously.

The demand for comparison websites is rising with 30% of consumers saying that they shop around before choosing their legal services provider, and 45% that they would turn to online comparison tools to help

them compare providers. Reputation continues to be the primary consideration when choosing a legal service provider. By achieving Cyber Essentials certification, you can show your commitment to cyber security and stand out from many of your competitors.

Provide a level of Cyber Liability insurance

If your firm is UK-domiciled with an annual turnover of less than £20m and you achieve Cyber Essentials certification covering your entire organisation, you will be able to opt-in to the included cyber liability insurance. This does not involve any additional cost or forms. The insurance cover includes a 24hr technical and legal incident response service.

Getting certified is a straightforward way of demonstrating to your insurance company, your business associates and your customers that you take cyber security seriously and have your house in order.

"We know that cyber security remains a key challenge for law firms and also that the sector is a target for cybercrime. Implementing the Cyber Essentials controls will help guard firms against cyber attack and achieving certification will demonstrate to your clients that you have put these important measures in place." **Dr Emma Philpott MBE CEO of IASME**

Get started with the Cyber Essentials Readiness Tool

Many legal firms find they have got their resources tied up running the practice rather than focused on IT and cyber security. The barrier to understanding things associated with technology can be a significant hurdle for firms in starting their essential journey into cyber security.

Until recently, much of the general cyber security information and guidance assumed a good level of IT knowledge. Firms have asked for a tool that can help them review their current level of protection and to obtain targeted advice on next steps. IASME responded to this need by developing the Cyber Essentials Readiness Tool, a free online tool with basic level guidance on the five key technical controls and related topics written in 'plain English'. This tool is free of charge and accessible in the form of a set of questions on the IASME website. The process of working through the questions will inform an organisation about their own level of understanding and what aspects they need to focus on. They will be directed towards appropriate guidance and, based on their answers, be presented with a tailored action plan and detailed guidance for their next steps towards certification.

CYBER ESSENTIALS

Assured Service Provider
in association with
National Cyber Security Centre