Why your firm needs Cyber Essentials certification

When it comes to cybersecurity, the legal sector faces a unique problem. On the one hand, most law firms realise the importance of cybersecurity and have taken the steps they think are necessary to protect themselves. On the other, the number of cyberattacks on law firms tells a different story.

The SRA's 2020 cybersecurity review reveals some alarming findings. Three-quarters of the firms visited by the SRA reported they'd been the target of a cyberattack. In the remaining quarter of firms, they reported that cybercriminals had targeted their clients during a legal transaction.

Of course, not every attack was successful. However, in the cases cybercriminals succeeded, the results were disastrous. The 23 out of 30 cases in which firms were targeted led to a total of more than £4m of client money stolen. Most of this money was later reclaimable through insurance policies, but some £400,000 had to be paid directly out of firms' pockets.

What's more, this figure doesn't take into account the 'hidden' costs of these incidents such as reputational damage, higher insurance premiums, fractured client relationships and lost time. The report gives an example of one firm that suffered systems downtime after an attack and lost £150,000 worth of billable hours as a result.

Why are law firms such an enticing target for cybercriminals?

It's not an exaggeration to say that a law firm represents a dream target to the average cybercriminal. Law firms process highly sensitive client data and handle large amounts of money daily. And, in the modern era, most of this is conducted online, allowing criminals easy access.

The situation is exacerbated by the recent COVID-19 pandemic. Many law firms are currently working remotely, with staff using less secure equipment and networks than they would in the office.

Add to this that cybercriminals know that lawyers are extremely busy people and have little time for anything beyond basic cybersecurity measures, and it becomes clear why law firms are so often targeted.

The problem for many firms is that cybersecurity isn't a core area of business, nor does it bring clients through the door. This means it's hard to justify hiring an in-house expert, but sourcing outside expertise is expensive. So what can law firms do to better protect themselves and their clients?

What is Cyber Essentials?

Cyber Essentials offers part of the answer as to how law firms can better protect themselves. But what is it?

Cyber Essentials is a government-backed certification scheme. It covers the key actions every business should take to ensure its digital security and protection from cyberattacks. Think of it as 'cyber hygiene, a bit like washing your hands, brushing your teeth or wearing a face mask.

The scheme assesses five key criteria:

- Is your internet connection secure?
- Are the most secure settings switched on for every company device?
- Do you have full control over who is accessing your data and services?
- Do you have adequate protection against viruses and malware?
- Are devices and software updated with the latest versions?

These five criteria may not sound like much of a defence. However, research from Lancaster University concluded that simply ensuring these five controls are in place can protect a business from up to 98.5% of common cyber threats.

Why is Cyber Essentials best practice for law firms?

For many law firms, getting Cyber Essentials certification is a compliance requirement. The Law Society has made Cyber Essentials a requirement for firms signed up to its Lexcel Standard in its recently published v6.1 release.

But even for those firms for whom it isn't a compliance requirement, Cyber Essentials is a worthwhile investment. For a fraction of the price of hiring outside expertise or expensive software, you can ensure your people, process and technology are working safely – protecting you and your customers.

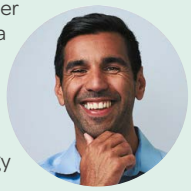
Who is CyberSmart?

CyberSmart was born out of the NCSC incubator four years ago, and we've been growing rapidly ever since. We're the UK's leading certification body for Cyber Essentials, typically completing the certification process for a law firm in 24 hours.

Using a self-serve digital platform, we've developed a simple, low-cost way for businesses to protect themselves, with no need for cyber expertise.

Although Cyber Essentials is a worthwhile investment for any business, it only guarantees your business is cyber secure on the date of certification – much like an MOT on your car. So, to keep you safe year-round, the CyberSmart platform monitors all your business's devices 24/7. It checks for the most up-to-date applications, operating systems, firewalls, security measures and compliance with Cyber Essentials.

Getting certified can seem like yet another compliance hoop to jump through, but in reality, it's a simple, cost-effective way to protect your firm. So if your firm is considering it, ask yourself the question: can you afford not to?



Jamie Akhtar is co-founder and CEO at CyberSmart, a VC backed cybersecurity startup that provides automated compliance for SME's. Jamie's obsession with technology started at a young age, he has been building and breaking things since he could turn on a computer. He's built over 100 web applications, served as the CTO of several organisations and wears a white hat as an ethical hacker.

CyberSmart

cybersmart.co.uk