Cyber Crime - How should we fight it?

Insurance for your reputation
Another month passes and yet more high profile names finding themselves in the press having been a victim of a serious security breach and consequent reputational damage leaving them with a fight on their hands in order to win back the confidence of their customer base.

These attacks, as is clear by now, are many and varied, but one common thread would seem to be that each victim either holds significant volumes of sensitive client data (big data) or significant amounts of client money.

Many professional practices will find themselves exposed in both areas. For some, there is talk that regulation may in due course extend to the need for a Data Protection Officer.

So, what do you do?

A link up with a good security specialist company will for many firms now be foremost in their thinking. One such firm have kindly provided us with a number of tips which, whilst aimed more specifically at firms within the legal sector, will apply equally to many other professions and in the hope you find this information useful we set out some key points as follows:-

Minimising breach potential

A lot of firms hold a mass of client data and, with more firms offering client services online – and often through interactive websites – what actions should firms take to prevent a hacker accessing their site and redirecting clients elsewhere? How can firms ensure client data is protected, and what can be done to minimise the potential for a data breach?

Managing that client data is important. The top two components on your list of strategic positions are big data and cybercrime. The increasing amount of client sensitive data amassed by firms, the move to an everything online, digital model, and the historically relatively low cost of storage has created a huge online stockpile for firms that has put the management of big data firmly on the risk register of every firm.

Buying disk space is only part of the equation. Making this data safe is a critical issue, which means understanding the data and ensuring it is secure. Further, best practice policies in relation to security need to be overlaid to ensure that, should the regulator come knocking, there is not too much or too little information buried in disks spread across your firm.

Denial of Service (DoS) attacks

Cybercrime is not just about businesses being under threat from fraudsters or those looking to cause heavy disruption; there are some other interesting crimes using wired and wireless access. With eight new users joining the internet every second and 250,000 new viruses released daily, cybercrime is now a well-organised and highly professional industry. It's even possible to buy services to launch denial of service attacks (DoS) on competitors' websites, which is what happened to MumsNet in 2015. DoS attacks render a network unavailable by 'flooding' them with useless traffic.

The Information Commissioner's Office serves civil monetary penalties on organisations, large and small, for failing to take the necessary measures to keep personal information secure. In the legal sector, where reputation is a significant asset, a fine for a lack of professional diligence around confidentiality would be devastating. So, what can be done? Here are a few handy tips:

Put in place a risk management committee to review and manage the risks. This governing body should be connected to the board. Ignore data management and security at your peril;

Establish ownership for data protection and information security;

• Put in place some simple but effective data access policies and controls for systems and key data, as well as detailing who should have access to what;

• Understand your data. Where is your business data and your client data? Design a data strategy or, at least, start with a workable retention policy which covers both paper and electronic material;

• Ensure password policies are implemented across the business;

• Use double verification (2 factor) security to access your IT system and files and limit the potential for hackers to access all parts of your IT systems and files;

• Train staff to be aware of potential threats, including bogus emails and suspicious requests for information;

• Take advice from a specialist and review your IT security position to ensure you have a reasonable level of defences against external attacks and malware, as well as ensuring penetration tests on your systems are a regular event; and

• Take an honest view of your capability and consider moving data and applications to a secure hosted environment.

Also important we feel would be the creation of a suitable Disaster Recovery Plan, perhaps incorporating testing of a worst case scenario, e.g. a regular all server shutdown, inclusion of a wide staff test group including junior as well as senior staff in realistically testing your resilience to disruption, ascertaining the recovery time and sustainable time lost. Just a few aspects highlighted here but giving you a flavour of the areas you need to look at and perhaps seek outside help.

Successful testing here will give you the confidence that your firm can withstand a cybercrime attack without suffering the sort of reputational damage faced by many as touched upon within our opening paragraph.

Once the consideration of risk transfer might be the final defence, with the purchase of a Cyber Insurance product which dovetails appropriately with the Crime and/or Professional Indemnity Insurance you hold. MFL Professional has a facility available that does this.

For more details, visit our website or contact us:

W: www.m-f-l.co.uk/cyber
T: 0161 236 2532