

Cybercrime is Thriving:

Here's How Your Firm Can Stay Safe in 2022

Cyberattacks are not only becoming more frequent, but are becoming more sophisticated, and therefore, more successful. And law firms are a prime target. So, how can your firm protect itself from the ever-increasing number of cyberthreats?

Email Security & Monitoring



Over 7 billion users globally send and receive 333.2 billion emails a day. Email security enable you to set rules about which emails can be received or sent from your email networks, meaning that you are able to eliminate unwanted or unsafe emails before they can reach your server.



Endpoint Detection & Response (EDR)

70% of successful breaches start on endpoint devices, such as laptops, mobile phones, and desktops – traditional antivirus software is no longer enough. EDR can be a big advantage for law firms and the security they can provide for the wider business, clients, and data.

Multi-Factor Authentication (MFA)



Password theft is common, and the legal sector is a prime target. Multi-factor authentication (MFA) requires the user to verify themselves and confirm the log-in attempt, which provides a second layer of security, preventing unauthorised users to gain access to your systems.



Cybersecurity Training

There is an undeniable link between basic cybersecurity knowledge and the mitigation of breaches – it is vital that your end users undergo continuous training to keep abreast of the ever-evolving threat landscape.

Specialist MSP Partnership



Partnering with a specialist Managed Service Provider (MSP) gives you the reassurance that they are experienced in dealing with the unique auditing and compliance requirements of the legal sector, in addition to the non-sector specific, yet just as significant, regulations such as GDPR.