

Fiona Cain in Law360: Why English Courts are Prepared to Assist Cyber Victims

By Fiona Cain | November 29, 2018

RELATED PRACTICES Litigation

Cybercrime is a growing problem for individuals and companies, and law firms are no exception. The Solicitors Regulation Authority, in its risk outlook report in July, considered cybersecurity to be a significant increasing concern for the legal profession so much so that it identified cybersecurity as a separate risk for the first time. This is not surprising when in 2017 £10.7 million of client money was reported as lost to cybercrime. The PwC Law Firms' Survey 2018, which was published last month, highlights that cyberattacks are a major threat for law firms because "firms hold significant client funds and information that is attractive to fraudsters and other criminals."

The risk outlook report advises that the most common type of cybercrime encountered by law firms is where criminals intercept and falsify emails between a client and the firm, or even within the firm, which results in money being transferred to the criminals. Law firms need to be vigilant and try to prevent cyberattacks and ensure that everyone in the firm knows how to recognize the signs of email modification fraud and common phishing scams. The SRA risk outlook report and the PwC Law Firms' Survey recommend that law firms prepare to respond to a cyberattack and deal with it in their business disaster recovery and business continuity plan.

In the unfortunate event that a law firm becomes a victim of cybercrime, in addition to reporting it to the relevant authorities, and informing the SRA and the clients affected by the cybercrime, the firm should also consider whether it is appropriate to take steps in the courts to limit the consequences of the cybercrime. ...

To read the full article, click on the PDF linked below.

[Cain-Cybercrime-English-Courts.PDF](#)

[First appeared in Law360 on November 28, 2018.](#) (Subscription required)