THE GROWING RISKS OF CYBERCRIME

JAYNE WILLETTS | SOLICITOR ADVOCATE | JAYNE WILLETTS & CO | SPECIALISTS IN PROFESSIONAL REGULATION

The growing practice of email intercepts and the significant losses that have ensued through fraudsters hacking into e-mail exchanges has been in the news of late. The risks here are considerable and growing. Law firms - especially those with exposure to transactional work such as conveyancing - are often small businesses lacking in sophisticated IT departments, but handling substantial amounts of money during numerous transactions. Fraudsters, on the other hand, are becoming increasingly sophisticated in their operations and have access to software programmes that enable them to scan thousands of communications for the transaction and financial details they require.

The scale of the threat facing law firms was highlighted in a feature in the Daily Telegraph on 16 May - recommended reading for all who can trace it. Having successfully hacked into emails shortly before completion between the vendor and his solicitors, the fraudsters, using the vendor's email address, sent amended banking details to his solicitors, thereby diverting the sale funds to them on completion. The bank refunded most of the monies but the dispute as to the liability of the law firm for the remainder was one of the issues reported in the piece, with the firm concerned claiming not to have been responsible for the outstanding losses.

Those responsible for the IT systems within their firms would be well advised to read a highly critical report by the Information Commissioner dated 5 August 2014, written mostly from the perspective of the harm done to clients through failure to manage data securely. The main thrust of this report is that encryption should be used on a much greater scale than at present, and that data should not be regarded as being sufficiently protected if a device is merely passworded, given the availability of software programmes that will unscramble such codes. We seem to have forgotten what was said in the earlier days of email usage, that sending an unprotected email was rather akin to sending a postcard through the postal system. We have resorted instead to gaining the client's consent to the use of email in our terms of business documentation and a confidentiality notice in our footers: the first will probably prove to be ineffective in the eyes of the Information Commissioner and the second is hardly likely to deter fraudsters.

On a more general level it will be useful to consult the Government's "Cyber Essentials Scheme" containing guidance on the basic controls expected from the adoption of "strong" passwords, and changing them at regular intervals, to the safe configuration of firewalls and network devices for detecting malware and spam messages. Whether on economic grounds or other, the firm that chooses to outsources these functions must be responsible for the vetting any such agency, a requirement of the Code of Conduct at O (7.10) in any event.

Meanwhile, at an operational level, it would be well worth ensuring that all members of the conveyancing department are well aware of the risks of fraudulent intercept. Other reported forms include:

- fraudsters purporting to be solicitors acting on the sale of a property, dealing with bona fide purchasers who are represented by conveyancers unaware of the scam, who cannot be traced once they have received the purchase proceeds (see *Davisons v Nationwide Building Society* [2012] EWCA 1626 and *Santander UK PLC v R A Legal Solicitors* [2014] EWCA Civ 183; and

- acting in conjunction with dishonest estate agents who are able to tip the fraudsters off as to completion details intervening at a late stage of a transaction and claiming now to be acting for vendor or purchaser through a bogus firm operation with a view to intercepting the sale proceeds or the mortgage advance.

Taking all of this into account, perhaps one of the most important amendments to the Office Manual now is one requiring any late change of the other party's representatives or the banking details in any form of transaction to be brought to the supervisor's attention and then questioned by the firm directly and robustly. ■

Jayne Willetts is also a director of Infolegal - a law firm compliance and risk management consultancy. Infolegal subscribers can now download the second edition of the Solicitors Office Procedures Manual by Matthew Moore and Vicky Ling in advance of its publication and can also access a range of detailed guidance notes and factsheets on these topics and many others. www.infolegal.co.uk.