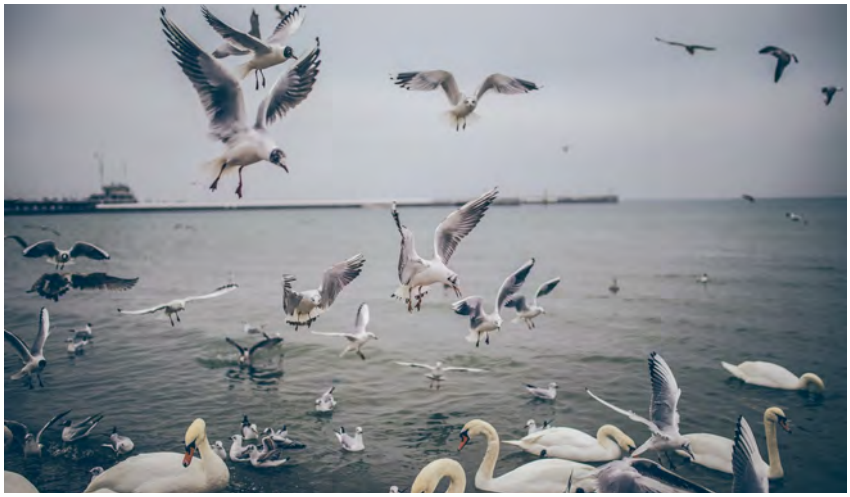
The Look Out

Professional Risks News from TLO

In This Issue

In Our Next Issue

In May 2018 the General Data Protection Regulation comes into force. Compared to the Data Protection Act, there are new elements and significant enhancements, so firms will have to do some things for the first time and some things differently. We will look at the subject in detail.



Phishing season never ends?

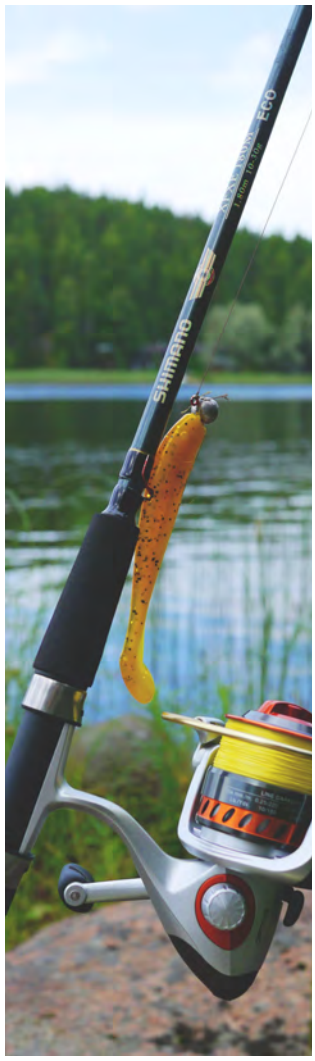
Jim Brindley - Account Executive, TLO Risk Services

Fraudsters targeting solicitors and their client's money during a property transaction is unfortunately still happening. The Solicitors Regulation Authority recently advised that £7m of client money was lost to cyber-crime last year. This risk is simply not going to go away and such frauds will become more and more sophisticated in order to avoid detection. Law firms must ensure they put measures in place to detect and avoid such risks and inform their clients of the dangers of cyber crime.

The internet and newspapers are regularly reporting on distressing stories of people losing their savings and deposits to these frauds. Many of these reports claim that the conveyancing solicitor did not fully warn their client of the dangers or put adequate protections in place.

cont'd

Phishing season never ends?



What can Law firms do?

It is good practice to alert and warn clients of the risks from the outset of the transaction through client engagement letters, email and the firm's website. The following procedures and steps are vital tools in combatting fraud, both for the law firm and their client. Firms, staff and clients should:

- Look out for poorly worded and incorrectly spelt emails
- Check the actual detail of incoming email addresses and links - being wary of masked emails or very subtly changed addresses
- Protect financial and confidential attachments by separate password
- Use anti-virus protection and ensure software is regularly updated and patched
- Use strong passwords and change them on a regular basis
- Train and regularly alert staff to current scams
- Not accept transfer of funds request from clients by email instruction, instead use fund request forms with client signature and bank statement identity
- Send bank details to customers on a letterhead and ideally by post, but if emailed, send as a pdf attachment rather than in the body of an email
- Include reminders on emails of the risk of cyber crime
- Remind clients of the risk of cyber crime at various stages of the transaction and to always be vigilant and on the lookout for any unusual instructions by email
- If in any doubt, always call on a verified phone number to authenticate information.

Why "wait and see" isn't acceptable

Damian Walton, Director of Professional Services, Inta Forensics

An often quoted statistic is that 80 per cent of cyber security risks can be tackled by 20 simple to implement preventative steps.

The UK government introduced a relatively simple "light touch" assessment process in the form of **Cyber Essentials** and **Cyber Essentials Plus** in 2014. Having supported companies of all types around the UK, we can attest that this programme proves that even companies with a modest budget can significantly improve their chances of being secure in the face of growing cyber threats and is a far better strategy for most than "wait and see".

cont'd

Why "wait and see" isn't acceptable

Changing technology = changing threats
Unfortunately, our desire to create an environment where our every need can be achieved by the press of a button or the downloading of an app is undoubtedly exposing us to financial, moral and, occasionally, physical danger.

Damian Walton is the former Head of Northamptonshire Police's Hi-Tech Crime Squad and also the former lead of the Data Compromise Management Team at Visa Europe

www.intaforensics.com

Security versus compliance
Some business sectors are already a long way ahead in their efforts to remain secure. The major payment card brands mandate that all entities who store, process or transmit cardholder data must be compliant with the requirements of the Payment Card Industry Security Standards Council (PCI SSC) Data Security Standards (DSS). These reflect current threats identified against payment card environments and a substantial number of the requirements are common-sense processes, i.e. complex password enforcement.

If, however, a business is attacked and payment card data is stolen, a thorough investigation will be required and can only be conducted by an accredited PCI Forensic Investigator (PFI) company of which there are currently only 22 in the world.

In addition to the financial cost of the investigation, consideration must also be given to the other intangible expenses – loss of productivity, reputational damage and long-term effects on the business. In such cases, it is vitally important to secure the services of a professional, diligent and empathetic PFI company. Think security, implement security, and maintain security.

DON'T BURY YOUR HEAD IN THE SAND

Plan ahead – it is far better to have a planned response ready to go.

If you need help planning, understanding the risks, or ensuring the right technical responses are in place, ensure you get help.

Retain any external assistance you may require and obtain contracts. Put arrangements in place before any incident occurs.

TLO Risk Services (TLO) is a privately owned insurance broker. Since 1996, we have specialised in helping firms that provide professional advisory services, from accountants and law firms, through to investment agents, surveyors and estate trustees. For more information visit www.tlorisk.com or speak to our experts on 0121 212 9090 or 020 7183 4925

In our next issue

Brexit will have no short term effect on the EU's General Data Protection Regulation (GDPR) which will come into effect from May next year. In our next issue we look at the subject in more detail as well as the role of Cyber Insurance