Pelican
Underwriting

T: 020 7743 0970
enquiries@puml.co.uk
pelicanunderwriting.com

The Pelican Brief

Risk insights and intelligence

Issue 001 | March 2016

Cyber risks

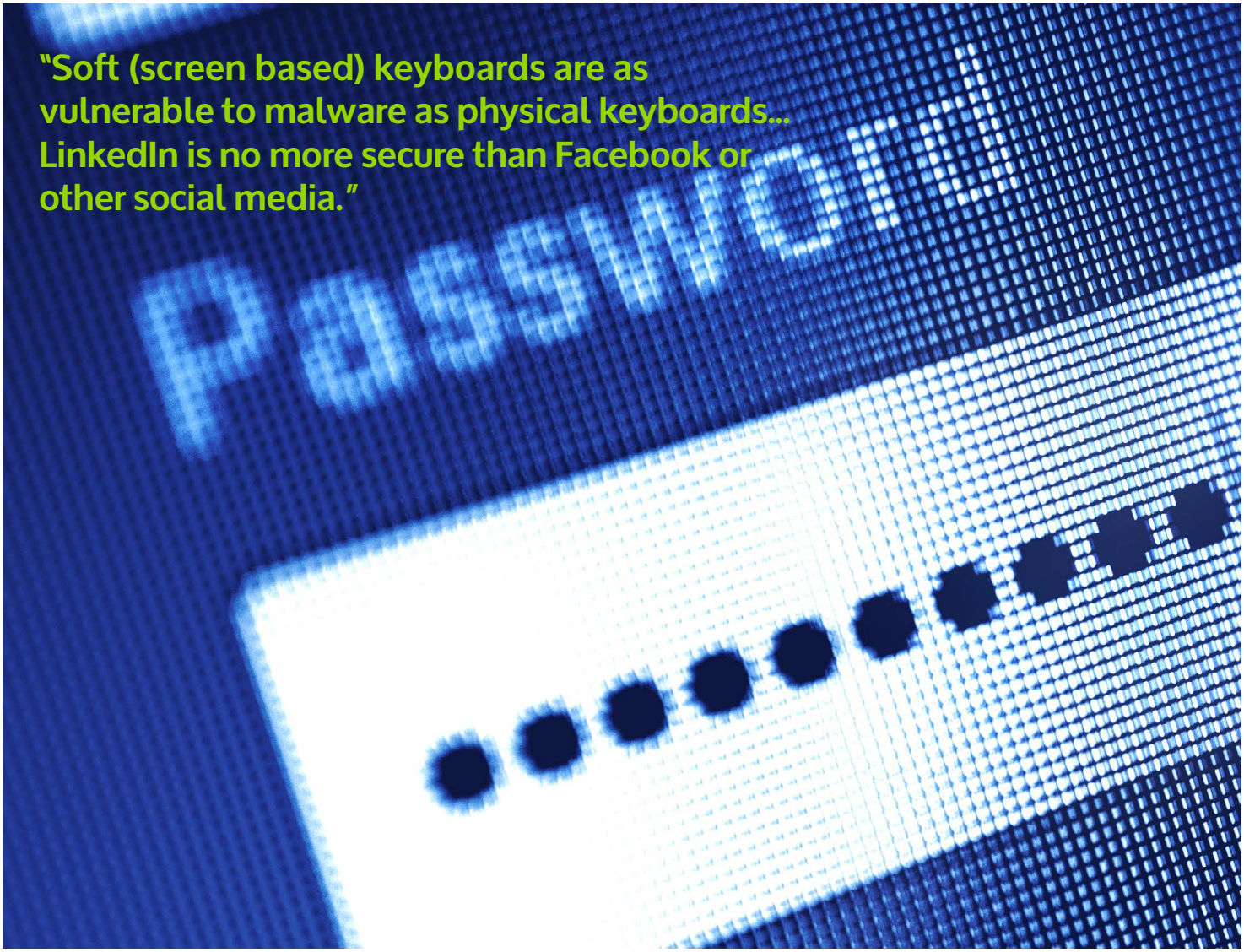
Background

The significant sums held by law firms are being actively targeted by fraudsters. They are being extremely persistent and they don't care whose money they target. This is a risk for all law firms and any failure to protect client monies will cause enormous issues for the firms affected, including potential closure.

We highlight in this Risk Management Update, the types of fraud being perpetrated and the steps that firms should consider in both preventing and mitigating the risk of falling victim to a cyber fraud.

This factsheet has been produced in partnership with Tim Prior of PNCR Legal due to his extensive experience of law firm risk and compliance issues. It provides a summary of the key risks faced by law firms but should not be taken as providing definitive advice in this fast moving area of risk.

PNCR LEGAL



Specific risks for law firms

The frauds faced by law firms are constantly evolving but here are some examples.

- **Bogus firms and/or transactions.** For the last few years, these have tended to go hand in hand with fraudsters targeting specific properties and then setting up a bogus law firm complete with website to handle the 'sale'. The risk has not disappeared but many fraudsters have moved on to newer frauds. At particular risk are buy-to-let properties or properties vacated, for example, by an elderly owner who has gone into a care home. Fraudsters pose as the legitimate owner and attempt to sell it without the owner's knowledge or consent.

- **Man in the middle fraud.** This is one of the most common threats, often the result of accessing public Wi-Fi, where a cyber criminal joins a public network and relies on an established connection to the victim's device to monitor, edit and redirect emails through the attacker's host network. It also allows the hacker to intercept sensitive data such as the security credentials of the user's business network. Emails are then sent to the firm, purporting to be from the client and amending instructions or bank account details. Alternatively, the client receives an email purporting to be from the firm asking for money to be deposited in the firm's (bogus) client account.

- **Phishing.** An attempt at identity theft by email in which criminals lead users to a counterfeit website in the hope that they will disclose private information such as user names and passwords. Links in such emails also contain malware which can lie dormant on the host device for weeks or months. Soft (screen based) keyboards are as vulnerable to malware as physical keyboards. LinkedIn is no more secure than Facebook or other social media.

- **Vishing.** This is seen by ActionFraud as a type of social engineering due to the fear and panic it seeks to evoke in the victim. Telephone calls attempt to obtain personal or financial information. Alternatively they seek to persuade victims to transfer funds from a 'compromised' client account with successful attacks involving millions of pounds. Fraudsters can spoof the phone number that appears on a caller display so do not trust it.

- **Whaling.** Spoofed emails ask finance staff to rush through a payment to a client or new business partner that the chief executive cannot handle directly, in most cases, due to being out of the country. One of the biggest such frauds in the US netted $47m (£30m). The emails come from web addresses almost identical to that of the target company.

Warning signs

Do not assume that there will be warning signs as an attack may come out of the blue but watch out for:

- Any attempt to put you under pressure to take immediate action. This is a key feature of vishing attacks. End the call or put the caller on hold while you ask someone else to investigate.
- Phishing emails. These emails often have characteristics that shout 'scam': perhaps the language, layout, syntax, font or graphics don't look quite right. The biggest red flag is the email source. Compare the source data with that of genuine emails for discrepancies. If you are not confident about checking an email's 'source data', ask someone to assist you or speak to someone you know at the 'genuine' sender.
- Late changes in instructions, beneficiaries, bank accounts or timescales.

Fraudsters are able to target you and your clients because of information found on your website or LinkedIn that makes them sound convincing. Don't be fooled.

Protecting your firm: internal controls

- **Cyber risks champion.** Appoint a Cyber risks champion responsible for monitoring key developments, including warnings posted by ActionFraud, the SRA, the Law Society and your bank.
- **Plan for the unthinkable.** Set up a crisis management process within your firm so that you know, in advance, who will do what as time may be of the essence.
- **Client vetting.** As part of client vetting and ID checks, ask clients to confirm their bank details if you expect to be remitting funds to them. For extra confidence, ask for supporting evidence, such as a copy of a bankcard or statement to minimise keying errors. For clients not seen face to face consider adding this to ID documents sent by post (not email) but check bona fides of person verifying documents AND verify with client when next speaking to them.
- **Foreign jurisdictions and nationals:** Be wary of new clients instructing you in complex or high value litigation particularly if you do not understand the facts or are offered a significant payment in advance. These clients could be fraudsters who pose a money laundering risk to your firm.
- **Internal fraud controls.** Ensure three way separation of payments from the client account so that the person requesting a payment cannot authorise it and the person authorising cannot implement a payment. Limit those who can authorise payments and adopt written enhanced authorisation procedures for sums over specified limits.
- **Suspect email.** If you receive emails from the SRA, the Law Society, the Land Registry, your bank (or elsewhere) which arouse suspicion, don't act precipitately. Pause and reflect. Discuss them with your Cyber risks champion.
- **Web searches.** Google your website and firm name regularly to check it hasn't been hijacked. If you use your homepage as your screensaver, you will know straightaway. Ask your lawyers to google themselves regularly to see if their identity has been 'cloned'. Fraudsters often set up bogus web sites months before they attempt to use them
- **Passwords.** Require strong passwords throughout the firm which should be changed regularly.
- **Bank instructions.** Insist on best practice protocols when interacting with your bank. Ensure any default payment limits meet your requirements. Disable online banking 'faster payments' for amounts over agreed limits. Put your bank on notice concerning your payment protocols so that if the fraudsters try and access your account via the bank, then they should be responsible for applying reasonable controls.

Protecting your clients

Retainer. Warn clients that fraudsters are actively targeting them and that using public Wi-Fi for emails and social media may make them more vulnerable. Point out that you will never advise them of new bank account details by email under any circumstances and that you will similarly ignore any such email from them changing instructions without formal verification of instruction changes.

Advise clients that, if they don't provide account details face to face, you will use two levels of security to verify the details, such as royal mail and telephone. Advise them that faster online bank payments are not as secure or as easy to recall as CHAPS payments. In the rubric on the copy client care letter that the client signs and returns to you, add text that confirms specifically that the risk of fraud has been noted.

Dos and Don'ts

Here are some tips to help ensure that you and your clients do not fall victim to cyber crime.

Do:

Think twice before acting on unusual instructions.

Update your software and browser software as soon as releases become available.

Ensure your Managing Partner reminds everyone regularly of the risks.

Advise your clients in writing of the risks.

Appoint a Cyber risks champion.

Ask your IT or office manager to check an email's source is legitimate before acting on it.

Keep up to date with the latest advice from the SRA, Law Society, Action Fraud, your bank and insurers.

Double check 'first time use' bank details. Build in a 'delay' cushion or send a token payment first.

Use strong passwords and change them regularly (eg quarterly).

Become suspicious if someone puts you under pressure to act quickly.

Act quickly if you fall victim.

Think carefully what is said in emails if you do not encrypt them.

Don't:

Panic. Being put under pressure to act immediately may be suspicious.

Reveal login details, PINs or passwords.

Discuss banking arrangements with your 'bank' outside agreed protocols.

Turn your back on common sense.

Post personal details on LinkedIn.

Trust the 269,000 public Wi-Fi hotspots with confidential data. Use 4G instead.

Be guilty of telephobia. If you know your client's voice, speak to them about sensitive information.

Forget that an email is like an electronic postcard. Use with caution.

Click on links in emails that you do not trust implicitly.

Put client funds or your firm's viability at risk.

Victims of fraud: if the unthinkable happens

- **Contact your bank immediately.** Time is of the essence, if you think you have been scammed. Every minute counts.

  Make sure that you know who to contact. The more quickly you react, the greater the chances of recovering funds.

- **Contact Action Fraud** (the police) on 0203 123 2040.

- **Client money.** Notify your professional indemnity insurer as the definition of a claim includes a shortfall on client account. Remember however that notifying an insurer does not relieve partners of their obligation to make good any shortfall on discovery.

- **Office money.** Notify your Office or Cyber Risks insurer.

- **IT Audit.** Consider engaging with a professional IT Consultant to obtain a "clean bill of health" on your systems, security and that you are free of malware such as viruses, worms and trojans.

- **Professional obligations.** Apart from those in the SRA Accounts Rules and the 2011 Code of Conduct, particularly chapter 10, the COLP and/or COFA must remember their obligations in the Authorisation Rules to report material breaches.

- **Data breach.** Consider also whether a report to the Information Commissioner is required.

Essential links

http://www.lawsociety.org.uk/support-services/practice-management/scam-prevention/
for the Law Society's dedicated webpage, launched on 11 February 2016, which brings all its advice together in one place.

http://www.sra.org.uk/home/home.page#Collection_2 for the latest scam alerts.

http://www.actionfraud.police.uk/ for the latest advice from the police.

https://www.getsafeonline.org/business/ Click on the business tab for a wide range of advice.

Pelican Underwriting Management Limited Camomile Court, 23 Camomile Street, London EC3A 7LL. pelicanunderwriting.com
Paul Cusition Managing Director T: 0207 743 0972 M: 07801 349 656 paul.cusition@puml.co.uk
Jay Bowey Director T: 0207 743 0971 M: 07973 348 741 jay.bowey@puml.co.uk