Technology's Role in Keeping Clients Secure

*By Carole Ankers,
Chief Product & Technology Officer,
poweredbypie*

The National Cyber Security Centre (NCSC) has recently stated that it defended the UK against 658 cyber-attacks in the past year. The NCSC believes many of these attacks have originated from locations abroad, including Russia, China and Iran.

According to the Solicitors Regulation Authority, in just the first six months of 2019, law firms reported a loss of £731,250 of client money to cybercrime. This is a rise from £9.4m for the whole of 2016 and £10.7m during the whole of 2017. Security is clearly a growing issue and incidents are only set to continue to rise.

In a constantly evolving digital landscape, legal firms are a prime target for fraud due to the high value of transactions, particularly in relation to property sales. As the use of technology within workflows increases, all legal professionals need to be alert to threats.

Phishing attacks, where cyber criminals impersonate either another law firm or a client in attempt to fraudulently acquire funds, are by far the most common way that criminals target the conveyancing chain. Rather than intercept email communication, most cybercrime attackers send 'spoof' emails.

These phishing attempts target individuals by posing as a legitimate source in order to encourage the victim to reveal sensitive information such as bank details or passwords. Often, they mimic a senior member of staff and are sent to a more junior member of staff. Individuals are 'taken in' because communication looks official or is similar to an email they may be expecting. When used to take conveyancing money, this type of cybercrime has been referred to as "Friday afternoon fraud', as so many property transactions complete late on Fridays.

> **"In a constantly evolving digital landscape, legal firms are a prime target for fraud due to the high value of transactions, particularly in relation to property sales."**

Despite the large sums of money involved in conveyancing cybercrime, it has been reported that just 60% of cases are investigated because it is so difficult to secure the evidence which will result in a criminal conviction.

Mitigate the Risk

So, what can legal professionals do to mitigate the risk? The first point to consider is that email is not a safe way to communicate confidential data so avoid this. For legal professionals under pressure to speed-up the conveyancing process, this presents challenges as in theory, increasing digital communication should increase the rate of transactions. Further, there is an expectation from clients in our 'digital age' that communication will be electronic and instant. However, with email confirmed as 'not secure' lawyers now need to communicate with vendors, buyers, lenders and other legal firms through a different medium.

Some firms have resorting to 'print and post' in an attempt to keep clients' data secure. But this can have its own risks if intercepted and it also adds delays to the conveyancing chain. The information which needs to be communicated between solicitor and client securely is wide-ranging: from key documentation which requires signatures, to the supply of law firms' bank details and those of the client. One solution is an online area which enables solicitors to store, access and share client documents safely, negating the need for physical copies, which can only be accessed securely.

Look to the Banks

Financial institutions and banks handle and secure client information by using two-factor authentication registration, using multiple identifiers. In this way, multi-factor authentication software has the potential to make secure communication instantaneous for law firms too.

Clients register with two factors of authentication: a password and a one-time use pass code sent to their physical device on every login. It's using the two methods in conjunction which makes an area particularly secure. Given enough time and effort, it's possible to crack a strong password, but it's very hard to also gain access to someone's device. In this way, two factor authentication offers the client and legal professional a solution to safely share data in a secure environment.

Work with Technology Experts

To protect clients, law firms understandably need to trust in any new technology application which has been designed to solve these threats and speed up workflows. However, lawyers' expertise is, quite rightly, in handling complex legal cases and firms often don't have access to the necessary in-house IT resources to tackle these technical developments. Therefore, to take advantage of these kinds of advances in technology, law firms need to have the opportunity work in partnership with technology experts who can make a real difference by being focused on developing applications that solve specific challenges. Introducing technology for technology's sake could be detrimental to both business and trust and potentially erode client confidence so careful consideration needs to be given to workflow and processes.

Technology certainly can't solve all the 'bumps in the road' but it can help with certain elements. Multi-factor authentication software has the potential to make secure communication instantaneous. Therefore, we anticipate successfully deploying secure communication systems that require multi-factor authentication in this way, will be a game changer for law firms in the future.

For further information please see: www.poweredbypie.co.uk

END