The two sides of technology

Q&A with Greg Bryce,
Chief Executive Officer,
poweredbypie

> **According to the SRA Risk Outlook 2018/19, in the first quarter of 2018 over 70% of all cybersecurity reports were directly attributed to email modification fraud**

We spoke with Greg Bryce, Group CEO, poweredbypie about technology's role in the spread of fraud in the legal industry but equally how it can be used in prevention.

Why are legal firms at particular risk of fraud?

Legal firms deal with some of the largest transactions anyone will ever make in their lifetime. Property transactions, in addition to wills and probate cases plus commercial transactions all involve significant sums of money. For fraudsters, trying to get the most return for their efforts, it makes sense to target legal firms handling these sizable assets.

These days, it's rarer that individuals go into their solicitor's office to meet in person so legal firms are often working remotely which often makes them an easier target for criminals.

How concerned should firms be?

In short: very! Technology has become more advanced and this offers new ways for criminals to target organisations. Fraudsters have made it their business to become experts in security and how to bypass it, more than most law firms can ever be. Not many legal teams have their own in-house cyber security experts to offset the levels of threat the industry is facing.

Do you think firms currently over or underestimate the issue? Are they prepared enough?

I believe there is a high level of awareness within Law firms about the risks of cyber security. However, there is a huge variation in their level of preparation. The fact is that all organisations are vulnerable. Even household names like British Airways or Marriot, with their vast resources, are not immune to major and well publicised security breaches. As criminals become more sophisticated the issue continues to grow. Organisations need as many checks and balances as possible to try and mitigate the threat.

What kinds of fraud are most prevalent?

According to the SRA Risk Outlook 2018/19, in the first quarter of 2018 over 70% of all cybersecurity reports were directly attributed to email modification fraud, a sophisticated method of interception designed to capture client bank details and personal information.

Therefore, identity theft is the most common problem: basically, people pretending to be other people to intercept funds. Criminals can also falsely claim to be another law firm to gain the same outcome. This is achieved through Phishing attacks. This is where the fraudsters send emails claiming to be from a reputable organisation in order to encourage individuals to reveal personal information, such as passwords and credit card numbers.

How can digitalisation and technology increase the risk of fraud?

Significant amounts of information is now kept digitally both at the law firm but also on customers' phones, iPads and computers.

poweredbypie

Is DMARC for email security enough to mitigate risk?

There are various security strategies available to try and prevent Phishing attacks. Domain-based Message Authentication, Reporting & Conformance (DMARC) is the latest advance in email authentication and should be just one tool in the solicitor's armoury to try and prevent fraud.

How can technology contribute towards mitigating risk?

Here, we need to look to the banks and how they secure client information using two-factor authentication registration using multiple identifiers as a potential solution. This would mean the solicitor would have a secure portal to which they can invite their clients to 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 this area very secure. Given enough time and effort it's easy enough to crack a strong password, but it's very hard to also gain access to someone's device. In this way, the client and solicitor can safely share data in a secure environment.

What the future of safe communication in the legal industry look like in your opinion?

Technology companies and security experts need to develop practical solutions for the legal industry that are safe and yet simple to use.   Working in partnership with trusted technology providers will offer legal firms the efficient solutions they need to communicate safely with clients in the future.

_____

END