FEBRUARY 2020

UPCOMING EVENT: LPM NORTH, 23-24 MARCH

LPM

LEGAL PRACTICE MANAGEMENT

THE ONLY MAGAZINE FOR LAW FIRM MANAGERS

EXPERT COLUMNISTS AND ADVICE FROM PRACTICE MANAGEMENT

LPM ASKS

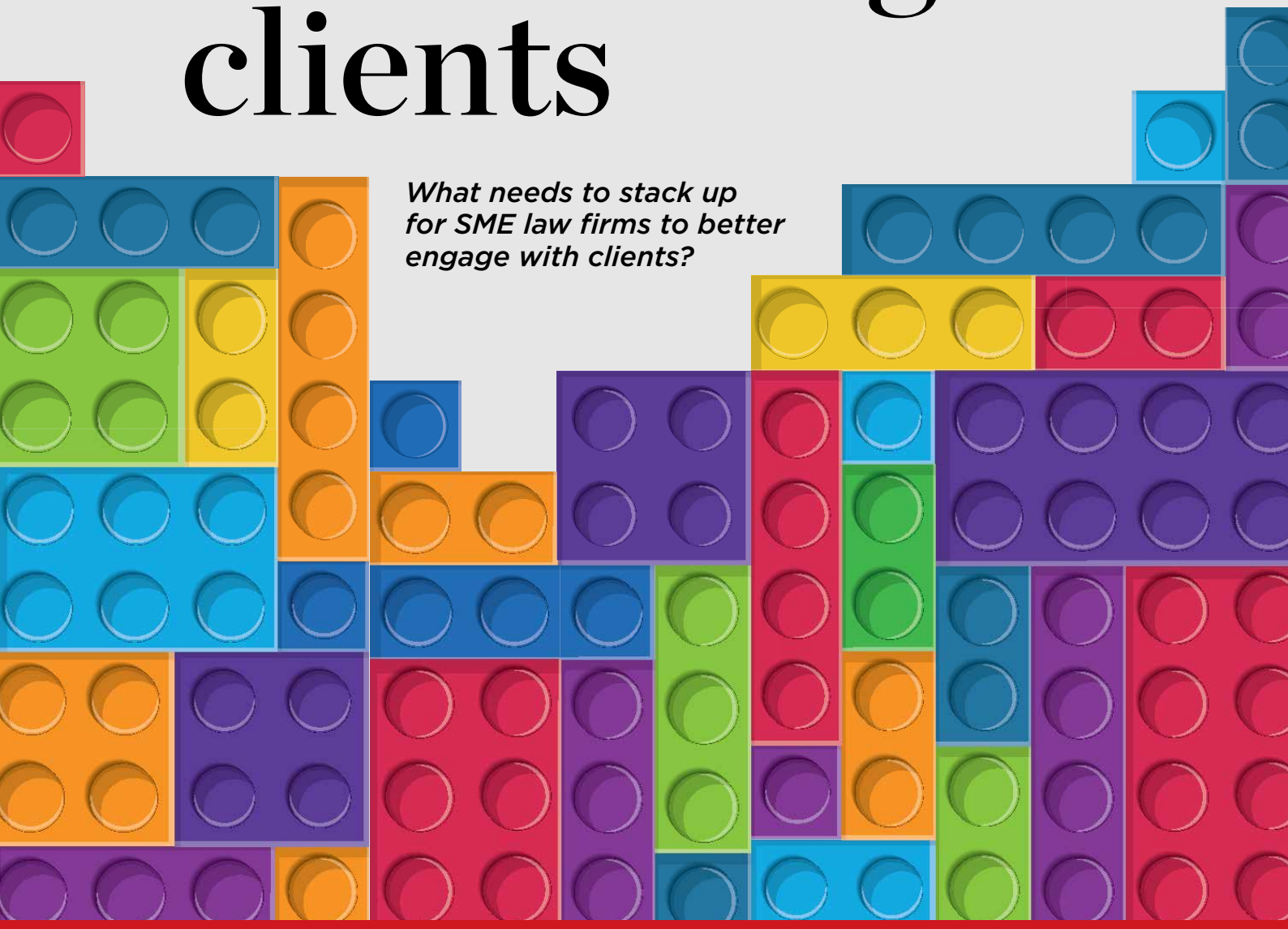
Peter Byrne, CEO at ESPHR, on building tech for clients

PRACTICE MAKES PERFECT

What do piloting and law have in common? Matt Meyer at Taylor Vinters takes flight

Connecting clients

What needs to stack up for SME law firms to better engage with clients?



BUSINESS INFORMATION FOR EVERYONE IN PRACTICE MANAGEMENT

Quiss

Excellence through experience

MANAGED IT THE WAY LAW FIRMS WANT IT

With more than 50% of our managed service clients in the legal sector, no one knows how to address the challenges you face like we do.

Experience measured in decades

For more than 30 years Quiss has helped clients adopt and implement digital technologies to maximise business opportunities and improve efficiency

Quiss benefits

- ✓ Deep knowledge of all legal sector independent software vendors
- ✓ Experience deploying sector specific critical applications
- ✓ Comprehensive 24/7/365 support with nationwide coverage

£14m

OUR REVENUE

Solid stable business with strategic plan delivering double-digit growth, year on year

OUR PEOPLE

More than 135 dedicated qualified professionals available with just one call

OUR SUPPORT

Helpdesk with 45 technicians, 24/7/365 support available and 40 mobile engineers

Azure Practice

Over the last few years Quiss Technology has invested significantly in the development of an in-house Microsoft Azure Practice – and we are now helping numerous professional services business transition parts or all of their environment to the public cloud.

If you are looking for advice or support on evaluating the options please contact us for more details.

0333 222 4334

www.quiss.co.uk

enquiries@quiss.co.uk

SPONSORED EDITORIAL

If you reuse passwords, there's a risk that the compromised password will be used to test other systems

The Travelex bug

NICK HAYNE, THE DATA MASTER

When Travelex decided to take its currency exchange services offline after discovering its systems had been compromised by an 'REvil' ransomware attack on 31 December, cybercrime again became headline news.

More disturbing perhaps than the $6m (£4.6m) ransom, is the cybercriminals' claim to have downloaded sensitive customer data, after accessing the Travelex network six months ago, apparently without anyone noticing.

It's highly likely the hackers will have gained access to Travelex by targeting some of the more than 7000 people who work across the organisation globally, with a range of attack methods, including phishing.

This is why we make no apology for focusing again on cybersecurity. You will have mapped your digital transformation strategy, but unless everyone in your firm lives and breathes cybersecurity, you could face a crippling attack you never recover from, financially or on reputation.

What are some security tips for 2020? Let's start with passwords. Never reuse passwords. Create unique ones every time for every application. Criminals now use automated bots to brute force attack systems using passwords revealed from past data breaches.

If you reuse passwords, there's a risk that the compromised password will be used to test other systems – a great reason to use password managers to ensure unique passwords for every system. And never reuse the password you use to log onto your firm's network.

Any good password manager will work, but only if you and everyone in the firm uses one. Remember, you and your colleagues have to protect your futures, every minute of every day – the criminals only need to be lucky once and it could be game over.

Phishing is still the major problem. The Verizon data breach investigations report cites hacking as the most common threat, with 81% of the hackers using stolen credentials, typically surrendered unwittingly during a successful phishing attack.

Spotting a phishing attack for what it is remains the best defence. And educating everyone within your firm about them – how to identify one and what to do – is the least you should do.

Typical signs of an email phishing attack to watch out for are:

- The sender is unknown to the recipient
- The sender is known, but on closer examination the address is a letter or two wrong – a very common approach
- Nothing in the email seems personal to the recipient
- The email was not expected – parcel status notices, tax refunds and so on
- The email refers to a bank/product/service the recipient does not use
- Words are misspelled, the grammar is poor, or the layout looks wrong for a large corporate
- The email body copy doesn't address the recipient by name
- The message asks for personal information – it may request a single piece that appears innocuous, but when combined with info from previous requests causes a problem.

Importantly, your people must be extremely careful with emails that show any of the above characteristics when combined with a suspicious attachment or a link to a website. Above all, everyone must treat every email with caution and not become click-happy.

And remember, the closer you get to your clients, the greater the risk of cross-infection, which could end a beautiful relationship before it has started! LPM