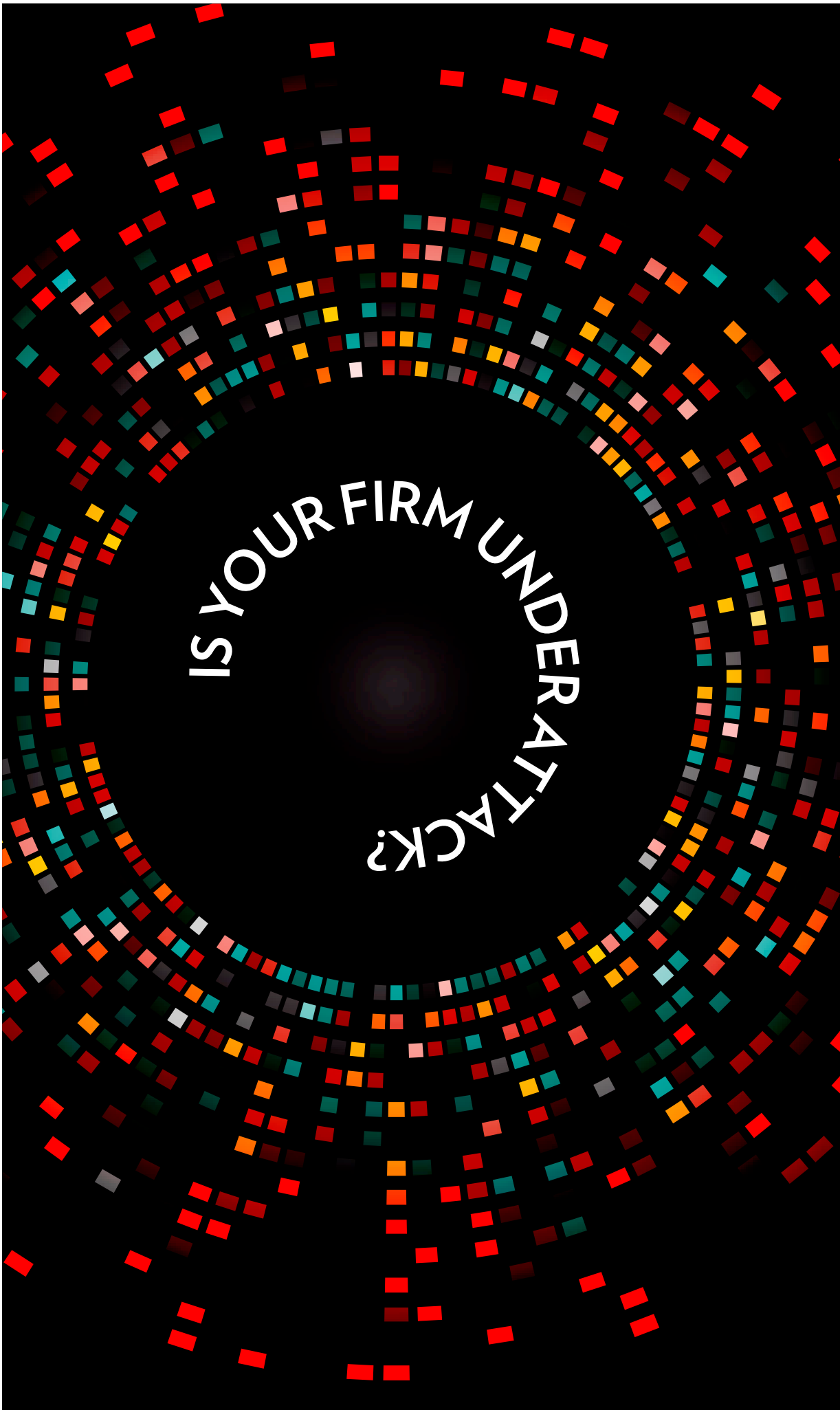
SMARTER LEGAL BUSINESS MANAGEMENT

Briefing



BREACH BODIES
As cyber-criminals expand their net, firms need to know how to stay out of it, and what to do when they strike

INSIDE JOBS
A top priority for businesses protecting their information should be their own people

pwc

intercity technology

INDUSTRY INTERVIEW

Plan for attacks

Raoul Rambaut, partner with PwC's law firms advisory group, tells **Briefing** why law firms may find themselves the weakest link in the information security chain, but it is people who need to be stronger

Law firms are under threat – and we aren't just talking about the ABS-converting accountancy giants and other alternative providers looking to undercut what firms say they'll deliver and stealing their clients away.

Firms are also at risk precisely because they're so diligently serving clients. The data they're privy to in the process of producing a piece of legal work makes them a prime target for people who want access to information about any part of a much longer chain of communication.

One recent survey on the subject finds that law firms have experienced a sharp increase in cyber-attacks in just one year – up from 45% two years ago to 62% in 2015, says PwC. And even that comes with one obvious caveat. "We can only count the known experiences," says Raoul Rambaut, partner in PwC's law firms advisory group. "The real number will almost certainly be higher than that, as some breaches will have happened and gone undetected."

Coming at you from all angles

First, information security incidents are spiking in the business world anyway. "If you transact money, you're automatically already more at risk" says Rambaut. "A law firm is an organisation that's in business – so it's at risk. However, law firms don't just have their own money to think about. They also move clients' money – and over the last year it's that money that has been under specifically greater attack."

Moreover, it isn't all about money. The Panama Papers incident clearly highlights that firms are of interest to organisations because of other details their business dealings can bring to light.

"Firms work with a wide variety of clients, often in the public eye. Hacktivists may well have a problem with an organisation that a firm's representing or defending. Correctly or incorrectly, they find themselves in the same line of fire as a result of the relationship.

"Hacktivists also have a tendency to move fast – and not necessarily with perfect information. The chances of falling victim to an accidental attack are higher."

A third and final category of attacker is an increase in targeted information-gathering exercises from nation states. "From intellectual property to raw material exploration and production, law firms are very well embedded in the integrated data supply chain for many organisations," says Rambaut. However, unlike the hacktivists, these parties may be much more wiling to bide their time. "They know that a location is a crossroad in data flow, but they're more likely to invest well ahead of the curve because they anticipate a richer source of data down the line," he says. "It might not materialise for six months, but they're happy to sit and wait.

"Wherever you have nation states you're also more exposed to cyberterrorism. Terrorists will be interested in anything surrounding national infrastructure – and of course, firms will be involved there as well."

To make matters worse, attack sources are also

Above: Raoul Rambaut, partner, law firms advisory group, PwC

PHOTO CREDIT: JONATHAN GOLDBERG

learning from one another to improve their chances of success.

"Organised crime is now much more ... organised," says Rambaut. "We've seen recent examples of criminal groups behaving more like nation states, in that they're increasingly willing to stay hidden and silent throughout the entire lifecycle of a transaction, then only strike as the funds are finally transferred months later."

Meanwhile, the common 'phishing' attacks of emails sent out far and wide to trick people into clicking on an infected link are morphing into more sophisticated disguises. The latest phenomenon is 'whaling', where criminals specifically target some of the most senior people in a business – those more likely to make decisions that'll result in money being released. By phishing, people are trying to hit as many people in an organisation as they possibly can, explains Rambaut. But it may be more effective – and of course, subtler – to go for a single big fish.

Human touches

As attackers change tack, it's even more important firms continually improve their preparedness in line with them. Not only, for example, are criminals targeting senior decision-makers. In other attacks, which encourage link clicks to release malware, they may position themselves as coming from a highly trusted source – a familiar colleague, or even a business leader.

At the same time, there's what is known as a 'drive by' attack – a known website compromised by a third party, but where content looks entirely

correct and therefore safe. People are now much more alert to the typical signs of the spam email, such as poor use of language or incorrect logos, says Rambaut. Criminals are responding to that alertness accordingly – and that means that training must likewise evolve in step.

"Half of the worst breaches are caused by simple human error on the inside – and often people have no idea they've been manipulated." Prevention, clearly, is better than cure – so firms need to find a way to educate anyone who may be increasing the firm's risk profile as a result of how they behave with its technology.

It doesn't help that lawyers are, of course, encouraged to promote themselves far and wide to develop business. They have an especially large online footprint for that very reason. "When people are the biggest asset, there's more there to target," says Rambaut. "Firms need to leverage social media more than some others, for example for marketing."

PwC would typically simulate a phishing attack (using the criminal's trick of making it sufficiently personal), then work out how many people were caught out and use that to establish the precise level of 'fix' needed. Almost a quarter of people typically open the message and over a tenth will click on an infected attachment.

In fact, a 2015 data breach report found that a campaign of just 10 emails yields a greater than 90% chance that at least one person will be duped.

"It's critical to capture the imagination of a very busy and very bright workforce, who are continually challenged for time."

Raoul Rambaut, partner, PwC

Worst-case scenario planning

However, the training needed to change those stats must evolve in line with changing employee behaviour as well.

"It's critical to capture the imagination of a very busy and very bright workforce, who are continually challenged for time," says Rambaut.

"The most recent graduates are also likely to have a much more open attitude to the internet, so need to be retrained about what's appropriate in a professional environment."

Training should be realistic, regular and consistent to help people make what are, in effect, business-critical split-second decisions about what to do, he says. But interactive or not, a common problem is that material is too dry, emphasising "manual-style compliance" rather than business impact.

It couldn't be done every week, but some good news is that PwC finds firms are increasingly opting for a cybercrime scenario in their full-scale business-continuity test (see feature, p4) – certainly a more dynamic exercise. "Handled badly, a cyber-attack is quite possibly the threat that could inflict most damage because of the ensuing effect on reputation," says Rambaut.

It follows that one aspect that should always go into training is the sharing of security failures or incidents from which to learn.

"One of the best defences is dissemination of what has already happened, and so what to watch for in future. It makes it both more real and personal."

But to make the most of this, departments also need to talk to one another effectively. Business functions can be too segregated – for example, client compliance teams typically report up to the head of risk. Such reporting at a senior level is fine, but the day- to-day functioning of an organisation also need some more fluid reporting lines, says Rambaut.

"Client acceptance process and information – or 'know your client' – should be shared so that all those with cyber-responsibility understand any increased risk from new business."

Firms should also build cybersecurity awareness into the gathering of intelligence on an ongoing basis. "Monitor web and chatroom conversations for developments that could indicate something becoming more likely," he says.

Security status

Clearly tied to the idea of effective communication across the firm is the question of who has ultimate responsibility.

"Chief information security officers didn't really exist 10 years ago," says Rambaut. The typical profile of that role is therefore still taking shape – including embracing new skills.

"It shouldn't just be seen as an IT role. It must be broader than that. We've seen that it's the people who are finally being compromised, and so you need a good 'people' person to get everyone on board with defending the business."

But more important even than that is having a senior partner take ownership of understanding the shifting risk at board level. PwC has found that 68% of firms now have a committee with partner representation dedicated to this area.

None of this is to say that the technical protection can be ignored. PwC's data also shows that 97% of attacks still target the top 10 best-known weaknesses in software.

"People are the problem – but you still need a minimum level of basic housekeeping.

"The lasting message should be that your firm is being attacked every day, and all the time – but knowing that, you'd still want to shut your windows and bolt the door."

www.pwc.co.uk/lawfirms

Building confidence in your digital future

pwc

Concerned about cyber, privacy or data breaches? Contact us.

Raoul Rambaut, raoul.c.rambaut@uk.pwc.com
Naveed Islam, naveed.islam@uk.pwc.com