The Forgotten Hole in Client Security

For obvious reasons, law firms treat client confidentiality as sacrosanct.

However, security breaches are a growing concern in the legal world. According to PWC's annual survey, 60% of law firms reported suffering from a security incident in 2017, with phishing attacks still accounting for the majority of breaches. It's no wonder law firms are going to even greater lengths to safeguard clients' confidentiality.

In the ILTA legal technology purchasing survey, security management was recognised as the biggest challenge facing legal IT teams. Email management, cloud computing, information governance and BYOD were called out as more specific challenges relating to security.

Notably absent from the list was any mention of remote working and remote meetings, a daily activity between lawyers and their clients. And that's by no means unusual. Rarely does one hear security concerns voiced about this business activity that's been around for 25 years or so now.

But does this apparent lack of concern stand up to a very basic level of scrutiny?

"Who just joined?"

These are arguably the three most-said words of all time on conference calls and remote meetings. This stems from the method of joining that still dominates the world of conference calling – dial-in.

In a survey by Sapio Research, commissioned by LoopUp, more than 50% of frequent conference callers said the considered it quite normal to be unsure of who was in attendance on their calls.

Why has this been considered okay for so long? Why is it allowed to persist?

The answer is probably because everyone is fundamentally able to do it. If you're the host of a call, you can send out dial-in numbers and access codes with a high degree of confidence that all your guests will appear on the call. People may not like it, and it may lead to a tremendous amount of frustration given its black box nature, but it's unlikely to be a catastrophe.

That is, unless it's not secure...

What's the worst that could happen?

The technology breakthrough that was perhaps most influential in driving the ubiquity of conference calling today, was the arrival of so-called 'reservationless'. No longer did the host need to book a facility, specifying the call duration and number of guests. Now they had their own dedicated facility that they could use whenever they so wished, without reservation.

But dial-in and reservationless are a problematic combination. Numbers and codes are used time and time again, perhaps for years on end, and end up in many different hands. In the same survey of frequent conference callers, 66% said they continue using the same phone numbers and access codes to join their calls for 12 months or more. Already this doesn't sound right if we're expecting a safe and secure arena for sensitive, confidential conversations.

There have been some high-profile cases that call out this security hole. During the 2008 presidential primaries, Barack Obama's campaign lawyer managed to obtain the dial-in details for a media conference hosted by the Clinton camp. Not only was he able to join unnoticed, he even started speaking to the press attendees, taking his opponents by surprise to put it mildly.

In 2012, the FBI admitted that they hosted a conference call with Scotland Yard and other foreign police agencies about a joint investigation of a hacker group and its allies, only to find that the hackers themselves were on the call. To add insult to injury, the eavesdroppers didn't need to hack into the call per se. They simply obtained an email containing the dial-in details.

Let’s get real – lawyers have neither the time nor inclination to attend training on how to host secure conference calls.

These are very high profile examples, but there are rich pickings for professional phishers to exploit in general business life, given the highly sensitive nature of so many client calls.

And then there’s the non-malicious, accidental breaches caused by the combination of reservationless and dial-in. These may generally be less ultimately damaging, but they’re still highly embarrassing nevertheless.

We’ve all been on conference calls where the host has scheduled back-to-back meetings and the guests inadvertently gatecrash confidential conversations. Or perhaps someone simply gets the day or time of the meeting wrong. Thoughtful perpetrators will just silently hang-up unannounced, but all too often the host is left with egg on their face.

What’s not the solution?

Training is the first obvious non-answer. Let’s get real – lawyers have neither the time nor inclination to attend training on how to host conference calls.

What about adding roll-call? Most conferencing services offer that capability. There are two problems here though. First, it’s painful. Calls get interrupted as anyone joins or leaves. Imagine the call with the person on a train, whose mobile phone keeps going in and out of reception. Oh, the joy. Second, it just doesn’t work for the case you’re trying to solve. A malicious uninvited guest could simply not record their name. What does everyone do then? Hang up? Unlikely.

What about some of the more capable software products for remote meetings? They offer a level of visibility to guard against such security breaches. The problem here is that the major players’ products tend to be quite feature-heavy and off-putting. Most lawyers really want something simple that just works. They don’t feel comfortable running the risk of user error and looking foolish in front of clients. And so they shy away from such feature-heavy tools and resort to the ‘safety’ of the devil they know – dial-in. Look at the evidence... Most major international law firms have way more audio conferencing users then web conferencing users.

So, what is the solution?

Reservationless is understandably attractive. It feels quite wrong to go back to a world of not being able to host meetings unless you've booked them in advance.

But dial-in is another thing altogether. If one were to be inventing conference calling afresh today, it's hard to see dial-in in the mix. It persists today because it's become engrained over the years, not because it's a good experience.

How might we tempt people to move away from dial-in? Here are three considerations:

- **Keep dial-in in the mix, at least for now**
  Even if just as a back-up, retain dial-in as a secondary joining option. That way, you still cater for the late adopters, and you offer a familiar safety net to the earlier adopters. It simply isn't realistic to go cold turkey on this one.

- **Make the new way even easier than dial-in. And offer added value for using it**
  If an alternative to dial-in is to take hold, it has to be just as easy, and ideally even easier. How about having the meeting dial out to you? Better still, how about getting visibility of who's on and who's speaking as an extra pay-off?

- **Add features super selectively and exceptionally**
  Hosting a conference call is a very risk-averse activity, and too many features scare people. Training internal users isn't realistic and training external guests is impossible. As such, only add truly important features, and add them with great care for an exceptional user experience. Leave out the rest and let more specialist users who need more features use more specialist products instead. For most legal professionals, less – done well – is more.

Working towards a world where dial-in diminishes – and one day disappears – will make conference calls and remote meetings so much more secure. LoopUp hosts are now using dial-in on just 25% of their meetings. It can be done.