Look who's listening

Conference call facilities may be a convenient and cost-efficient way to hold meetings, but they can also represent significant security vulnerability.

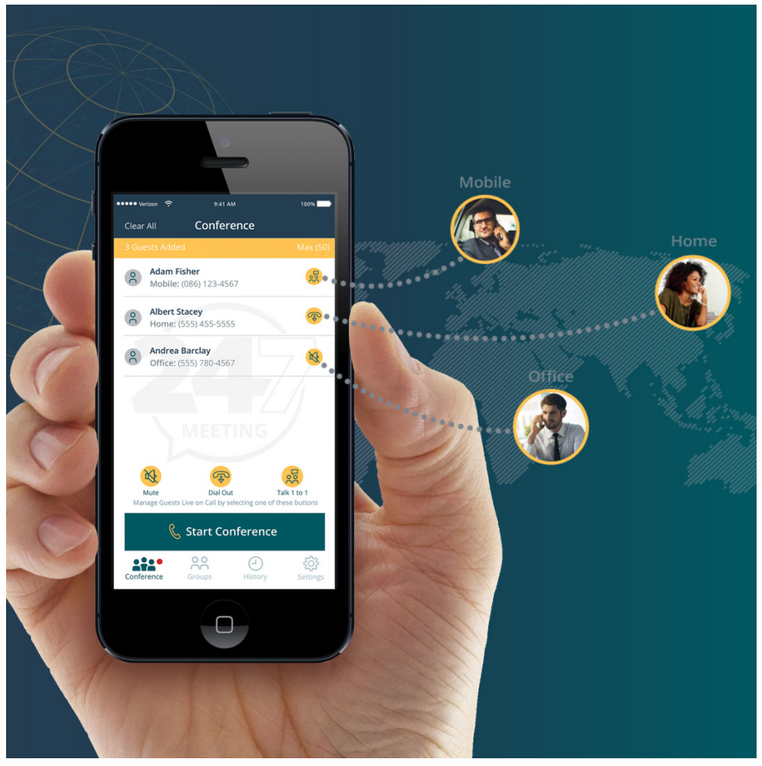
BY BARRY McCALL

When we hear about data security being breached in an organisation or about criminals obtaining commercially sensitive information by nefarious means, we tend to think about sophisticated computer hackers or even old-fashioned industrial espionage agents breaking into offices in the dead of night.

And when we hear the advertisements alerting us to the advent of General Data Protection Regulation (GDPR) and the potentially eye-watering penalties associated with it, our minds again tend to turn to cybercriminals or the theft of laptops or other devices.

One thing we almost never think of is the conference call. This facility has become such an integral part of everyday business life that we have come to take it for granted. Three or four people need to chat about new product developments? Set up a conference call. Hosting a regular Monday morning sales meeting but need your people out on the road selling? Set up a conference call. Need to schedule a management meeting to discuss performance updates in advance of a board meeting? Again, set up a conference call.

Such is the convenience and cost-efficiency of the facility, it is little wonder that users give little or no consideration its security aspects – or lack of them. But organisations need to be very aware of the facility's potential security vulnerabilities.



The main issue boils down to interlopers on calls. Once an individual is in possession of a dial-in number and a passcode, they can listen in to a call and gather vast amounts of sensitive commercial and personal data without anyone being aware of their presence.

The existence of this problem is confirmed by industry research, which reveals that 78% of regular conference callers have experienced the wrong people on their call and 34% have stated they were never sure who was on their call.

"One of the problems with the conference a call is that, quite often, it isn't immediately clear who is on the line," says Gavan Doherty, Founder and CEO of Irish conference call provider, 247meeting. "We get a lot of first-time clients coming to us saying they have had conference calls in the past where suddenly they have heard voices they didn't recognise."

As is often the case, the problem has as much to do with human failings as the technology. "People can be very slow to change their dial-in access PIN codes," Doherty explains. "This can offer a way in to unscrupulous third-parties. You might host a conference call with a particular customer or supplier at 10am every Monday but if you don't change the PIN, there is nothing stopping that third party from dialling in at that time to listen in to your conversation to get pricing and other important information. Direct competitors can also use it to gather similar information to gain unfair competitive advantage. If they mask their caller ID, you have no way of knowing who is listening in."

The vulnerability goes beyond that, however. Most theft is opportunistic and the same applies to cyber and data crime. One stratagem employed by criminals in this instance is to dial in to the conference number from time to time, just to see if there is a call in progress. If there is, they keep listening – or, better still, record it and then listen back to see what commercially sensitive or otherwise profitable information they can harvest.

There is also a very real risk in terms of GDPR compliance. If HR teams are discussing the personal details or staff members on a call, or if sales teams are sharing personal information about individual customers, any security breach caused by unauthorised dial-ins could be very costly indeed with fines of up to 4% of global turnover or €20 million provided for under the legislation.

There is a solution to this issue, according to Doherty, and that is to put the host in complete control of who is on the call. And that's possibly the key benefit of the new 247meeting Mobile app developed by the company.

Instead of waiting for others to dial in, enter PIN codes and so on, the app puts the conference in the hands of the host who effectively calls the different participants into the meeting. You can't get in if you aren't directly invited and the host has full visibility at all times of not only who is on the call, but the number of people on it. This means that there is no prospect of an unauthorised participant simply dialling in and listening.

> "Until we started using 247meeting, we had no idea who was on our calls. We feel more secure now when handling delicate topics – Conal Henry, CEO at Enet.

"There are many advantages to the 247meeting Mobile app, but we think security is probably the main one," says Doherty. "Of course, it makes the whole conference call process much easier and more efficient because you're not sitting there waiting for people to dial in and so on, but that's a minor inconvenience in comparison to the potential losses that can result from a security breach. The app prevents breaches as only those people you invite can join in the conference and you can see who is participating at all times."

While traditional desk-based conferencing still accounts for the majority of the company's business, existing clients are increasingly moving over to 247meeting Mobile. "People like it because it's like having a war-room in your pocket," says Doherty. "If you're a CEO and your company is suddenly hit by a crisis or a major development that requires urgent attention, you can immediately call all five of your generals to start working on the problem together. And you have the comfort of knowing that no-one else is listening in."

247meeting also offers a range of security solutions for its other conference call solutions. These include 'disposable conference calls' with one-time-use PINs activated via 247meeting's online account management tool; Secure Name Record, which can prevent callers from joining unless they say their name; and Roll Call, which tells you how many guests are on your call.

Speaking about the service, Conal Henry, CEO of Enet, said: "Until we started using 247meeting, we had no idea who was on our calls. We feel more secure now when handling delicate topics."

These levels of security have helped make 247meeting a favourite with legal firms and the professional services sector, says Doherty. "We count five of the 'Big Seven' legal firms and top professional services firms KPMG and Grant Thornton among our clients. We believe, because of the quality of service and the enhanced security and transparency that we offer, we will win even more business in these key sectors."

For more information, visit www.247meeting.com/ai or search for "247meeting Mobile" in your smartphone's app store.

Five steps to secure conferences

1. Use a Dial Out Conference Call application to choose only who you want on the call;
2. Choose a conference call solution that allows you to see who is on the call;
3. Change PIN codes regularly or use 'once-off' or 'disposable' codes;
4. Turn on the features like Roll Call and Name Announcements so every guest is identified;
5. Never share your personal PIN codes