times2

The Met spent millions investigating allegations of corruption, spying and drugs against this officer. He was cleared and is now up for promotion

Interview with Chief
Superintendent Ali Dizaei
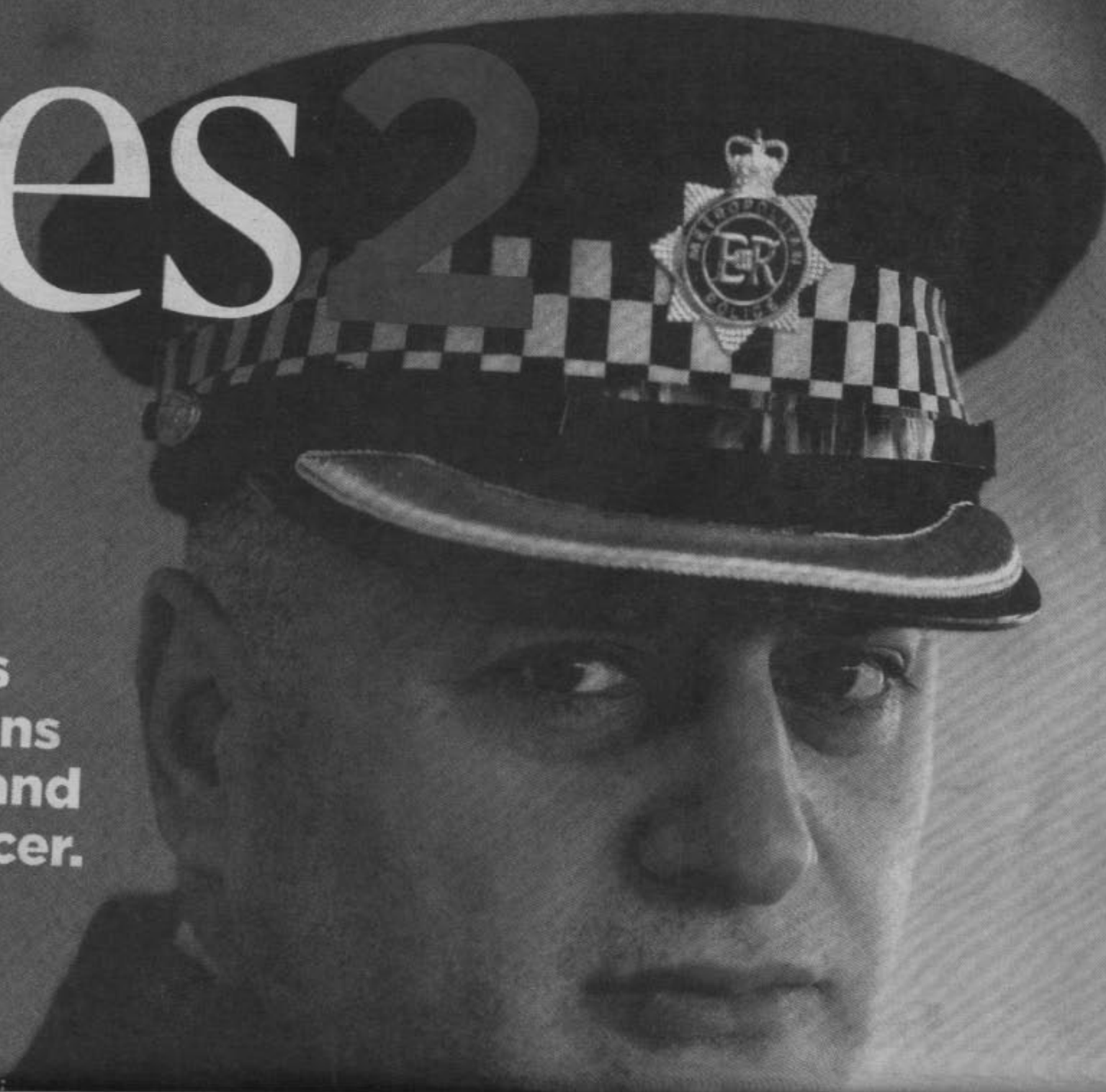
It's one of those statements that people say "really?" to when they first hear it: "97% of UK businesses employ less than 20 people - and there are over 4 million of them".

BY COLIN DUFFY

But even very small businesses find that they do need some of the features that big businesses take for granted. They need to be able to make and receive several calls at once, transfer calls to colleagues and divert calls to their mobiles or home when they pick

der them. They want to customise and personalise their messages "press one for Colin, press two for today's menu, press 3 to call my mobile etc so that their customers get who or what they want quickly.

They often need extensions in different locations, even different continents and they want it to feel (and

that they can get on with generating over 50 per cent of the UK's turnover and 64 per cent of all commercial innovation.

Colin Duffy is the CEO of the independent UK VoIP company, Voipfone and a Director of ITSPA, the Internet Telephony Services Providers' Association www.itspa.co.uk

Is Skype fit for business?

There is no doubt about it, Skype has transformed telecommunications forever. The Internet start-up that was bought by eBay nearly eighteen months ago has more than 170 million users who can call one another for free as well as call non Skype users for vastly reduced call charges.

In fact, one would find it hard to find a company that better personifies the promise of 'disruptive technology' to take on an established industry and lead the way.

The trouble is, the technology, which started out as a consumer offering, but has since launched as a business service as well, is often labelled as 'unsafe' by corporate VoIP providers.

Safe for firms?

Whilst Skype points to its very strong encryption technology, the companies rolling out VoIP networks in to large enterprises have long warned that because its standards are not open, companies cannot be sure that staff using Skype at work are compromising security.

"Skype's an amazing success story and it's a great product," says Mark Osbourne, Chief Information Security Officer at Interoute.

"The trouble is it's very hard to have control over it because it doesn't conform to normal, open standards VoIP operators use and so it's very hard to stop it working across and out of the corporate network.

"Also, and this is what concerns me as a security person, Skype means a person can leave your company and work for a rival and people are still

contacting them via Skype and maybe unaware they have left. Also, I always insist that clients' staff change passwords every three months and that they are completely random. The problem with home systems is people don't ever change their passwords and, when it's not forced upon them, they tend to go for very predictable words. It's that loss of control that companies should be concerned about. Skype is a fantastic product but it's not, in my opinion a corporate product."

Fit for office

As one might imagine, Stefan Oberg, Skype's General Manager disagrees, pointing out that the software is being widely used by business with no reported problems.

"Approximately 30 per cent of the Skype community today use Skype for business purposes and say that saving money is just the start," he counters.

> ❚❚ Skype's an amazing success story and it's a great product ❚❚

"Some companies who employ an IT manager have asked us for more visibility as to how Skype works and so with our latest version we have enabled IT administrators to have more control over how Skype is used on their networks. We want businesses to be able to use Skype in a way that works for their company and complies with their specific IT policies because we believe companies shouldn't have to pay for the privilege of having their staff talk to one another more easily or naturally."

VoIP security: 'Vomit' worse that 'Spit'

It may be tempting to think that talk of hackers getting in to VoIP systems is just another way for security companies to sell more protection but, according to those who are daily turning on new VoIP systems, the warnings are not without foundation.

"Every time we turn any kind of box on any IP network we immediately notice people are trying to hack in to it," reveals Mark Osbourne, Chief Information Security Officer at VoIP provider, Interoute.

"It's a problem for anything connected to IP that people will try and hack in to it. Personally, I think a lot of the problem is cowboy operators who hack in to other peoples' networks and then sell on that capacity. We all know there are some dodgy companies out there who are at least trying to do that."

Firewall needed

For this reason, any company considering installing a VoIP system should insist their provider puts in a firewall. The term comes from the defensive metal plate placed in between a car engine and the vehicle's passengers to protect against an engine fire. In IP terms it is a device which filters through traffic and ensures that only registered users can make calls and prevents hackers from either making calls on a third party network or, worse, using a VoIP connection to potentially hack in to a company's computer systems.

Most VoIP providers offer varying levels of encryption so that voice traffic is scrambled across the network so calls passing between offices belonging to the same company are only rendered intelligible when the voice reaches the other end. Hence, although eavesdropping is a possibility, it is not the main security fear.

Spam to 'Spit'

One potential misuse of a VoIP network businesses need to be aware of is Spit (Spam Internet Telephony) which, as the name suggests, is the voice equivalent of junk emails where a company's network could potentially be flooded with recorded voice calls offering double glazing quotes and so on.

The problem has yet to manifest itself and, even so, would be, at worst, an annoyance that could be countered by a decent firewall and number filtering technology.

However, Osbourne feels the real threat to VoIP systems lies with another, similarly vulgar sounding acronym, Vomit (Vulnerability Of Misconfigured Internet Telephony).

"Unsolicited sales calls would be annoying but what could really be worrying for a company is if they don't set up their VoIP system to be secure from hackers," he suggests.

"The type of things hackers could do is use an unprotected VoIP gateway to look at files on company computers and hack in to answer phone accounts to pick up executives' messages. It could be hugely embarrassing and damaging."

Disruption attacks

Unprotected VoIP systems could also be prone to criminal attacks across the Net which flood networks with so much data that they are forced to close down. These Distributed Denial of Service (DDos) attacks have been commonly used by criminal gangs to bring web sites to a halt as servers find themselves unable to cope with an attack which orchestrates hundreds of thousands, or even millions, of log-in attempts all at the same time. Betting companies who have refused to pay a ransom have been open targets for these attacks, particularly just before major sporting events, such as the Grand National.