



Opportunity to leverage their brands

The rousing cheer you heard recently from the Big Telco bunker was in celebration of the demise of VoIP firm SunRocket. At the time of its sudden closure on July 16, SunRocket was the second biggest US VoIP provider, with more than 200,000 customers.

It's a rare piece of good news for established fixed-line players, and it contains a certain kind of logic. Barriers to entry are so low for VoIP services that the would-be disruptors themselves are highly vulnerable. SunRocket's fall suggests Vonage's days are numbered, too, although the Vonage people are bravely claiming it as a win.

But it proves that there's no future for voice-only providers in telecoms any more.

Anything can be reduced to an IP packet, and a commodity like voice becomes just a bundled extra. Which must bring another cheer from the bunker, where the multiservice business plan has become the received wisdom.

This obviously plays to an incumbent's strengths, namely its scale and deep customer base.

But it's the other asset telcos have that gives them a real opportunity, and that is their trusted brand.

For all the complaints about carrier bureaucracy and lethargic response time, the brands remain powerful. Marques like BT, SingTel, NTT, KT, Telstra and Telecom NZ are some of the most trusted in their markets.

So why not apply it to where it's really needed?

Let me nominate an area crying out for someone to take a leadership role: data security.

Securing your data is no different from securing your house or ensuring safety on the road. You don't leave it up to the police. You put locks on your doors. You buy new tires when the old ones go bald. You don't give your home address to strangers.

Lucrative cyber-scams

All basic stuff that we internalized long ago. But as consumers or business owners or staff we are still learning about how to protect our data.

Because of this, and because of the size and reach of networks, our personal and business data are vastly more vulnerable than our physical assets and personal safety.

Organized crime gangs are finding just how lucrative cyber-scams can be. It takes just \$500 to

launch a phishing attack that can reap \$10,000 a month. A whole industry has grown up around it. Software tools are available to mine and extract the customer data.

These threats operate globally, but the police don't. There's no cross-border agency equipped to deal with thieves across the globe.

Richard Stiennon, chief marketing officer for security appliance-maker Fortinet, says the next problem is that financial institutions don't care. Even if a bank is losing \$2 million a month, to a large institution, "that's tiny," he says. To set up a secure perimeter would cost \$20 million plus all the additional opex.

He says right now retailers are the preferred targets. For thieves retail stores offer massive amounts of poorly-protected data in an environment where strangers can come and go.

In what has become the biggest case so far of ID theft, TJX, a retailer with 2,500 stores around the US, has allowed the personal data of 45 million credit cardholders to be stolen. TJX says the thieves got hold of its decryption tool, although it's not sure how. Stiennon says the thieves apparently keyed into the corporate private network via in-store web kiosks.

Meanwhile, fraudsters were caught in Florida buying goods with \$1 million in gift cards acquired using some of the stolen credit cards.

This case is worth mentioning not because of the size but because of the vulnerabilities at various points of the chain: the careless retailer, its vulnerable corporate network and also the obvious signs of money being laundered in Florida.

All of this demonstrates a lack of alertness, yes, but also poor understanding of the threats we face.

What's really needed is community education about network dangers and how both to keep them out and to spot them. There's a role for someone who can run free seminars for customers, send teams out to schools and workplaces and to educate government and business leaders. It's a leadership role and it's one telcos are perfectly-suited to play.

What's really needed is community education about network dangers and how both to keep them out and to spot them

telecomasia

Robert Clark is based in Beijing, where he edits CommsChina newsletter –
rclark@commschina.com