Has VoIP security become

It is ironic that one of the comms industry's most important issues is barely talked about and largely not understood – VoIP security. How, by any interpretation, can that be good for customers? Here, four champions of security respond...

Comms resellers and service providers who fail to meet the growing demands of the telephony security threat landscape are so lacking as to be almost complicit, especially in the light of new regulatory and compliance demands, according to Simwood founder and CEO Simon Woodhead. "Apathy and arrogance from CPs remains the primary issue," he stated. "Telling someone how much they've already lost is not protection, it is risk limitation having already profited. We focus on prevention which requires us to invest and forgo profit on compromised customers, which feels the honourable way to do business."

But to contain threats – even for those who care most and see the risk – is a tough challenge. "Sadly, so much service provision at carrier level is me-too and magic boxes," claimed Woodhead. "So for resellers seeking an answer to VoIP security 'intent' should be their number one consideration. Why is the carrier offering me this feature? Are they doing the minimum possible in order to contain their own risk? Or do they genuinely care about a CP's end users and their prosperity? Some may choose to dance with the devil for other reasons. Others will hopefully see through the hype."

Carl Boraman

VoIP fraud sours a relationship, destroys trust and leads to costly disputes, which drives up churn and increases bad debt.

VoIP security is not a 'solution', and anyone offering it as an up-sell on service is demonstrating poor intent, according to Woodhead. "If a car manufacture made door locks an optional extra or talked about their 'extraordinary security' while giving all buyers the same set of keys people would see through it," he said. "CPs definitely need *caveat emptor* to see through the bull and really get a handle on intent."

Simwood works increasingly with security critical clients such as financial institutions and since the advent of GDPR and the Cambridge Analytics issue Woodhead has noted a big uptick in demand for Transport Layer Security (TLS) and Session Description Protocol Security Descriptions (SDES). "We provide these at wholesale level," he said. "However, the value of fraud measures to CPs in the channel or the pursuit of them remains disappointing.

Simon Woodhead

Apathy from CPs is the primary issue. Telling someone how much they've already lost is not protection.

We feel strongly that this would change if end users (business and domestic) were more educated about the risks. Our book 'Speaking up on Telephony Risks' aims to do this."

Responsibility

Resellers are looking to drive sales, increase revenues and deliver a great customer experience, so within the tools they get from VanillaIP as a service provider security measures must feature strongly, according to its Sales Director Iain Sinnott. "In terms of VoIP security, and especially supporting resellers in the SMB sector, we need to take responsibility for the device security, the access security, the integrity of the calls and the commercial risk wherever possible," he explained. "Customers and resellers need to focus on this issue, turn to their service providers and demand solutions that are robust, but without reducing the flexibility that makes cloud services and consumption on demand so attractive."

According to Sinnott the future of VoIP is self-service and security must be in the DNA of the solution, not a fringe defence mechanism put up to deal with the hackers. "Service providers need to consider security in every element of every product they release within the VoIP portfolio," he reaffirmed. "The industry big boys, the carriers and major brands, should be doing more to get the end customers talking about this element of modern communications.

"Those of us investing heavily in security need the customer to recognise the value of the effort and expenditure, otherwise those who play Russian Roulette with customers' security have the commercial advantage. However, compliance helps us – it focuses everyone's minds on security with the threat of action from regulatory bodies, and that means people will attach value to the security services our development teams spend time creating."

Security has become something of a 'cover all' term for the prevention and management of toll fraud risks, data security and GDPR etc, says Sinnott, who argues a strong case for greater education about the matter. "Information is key, and unless a sales person feels well enough informed they may not bring security up as a key point in the sales process, which does neither party any good," he added.

"Service providers need to be clear and upfront and make security a focused element in partner training. It is their moral duty. If you can demonstrate the steps you take to protect customers it makes you trusted and clients look with greater care at every cheap deal. If the reseller is expected to carry too much responsibility they are not being looked after as well as they might. Resellers will always play a role in security and must follow

a comms sector scandal?

deployment guidelines, but the platform owners should do the heavy lifting here."

Toll fraud can quickly become big enough to kibosh a small SMB customer, and if they default the burden of debt moves to the reseller. To combat these threats VanillaIP leverages three related areas of its cloud management ecosystem (Uboss) – managing the access security, restricting the availability of channels per extension and running a live rating system linked to an extension level credit lock. "By taking responsibility for the performance of this combined approach we can limit the customer's and reseller's financial exposure to effectively an excess like any insurance policy," added Sinnott.

The cost of fraud continues to eat into already stressed profit margins with the average fraud attack on SIP trunks typically costing £10-15k, with some bigger attacks costing CSPs £200k over a single weekend, observed Carl Boraman, Director of Strategic Alliances at Tollring. "The transition to VoIP and the migration from analogue to SIP means VoIP fraud will potentially increase," he stated. "It is already a multi-billion-pound business and its financial impact is more than double that of credit card fraud."

Modern customers entrust the safety of their information and even their company to their networks and reseller partners. If they don't protect their clients they will lose their trust and a poor reputation could be more harmful to a brand than any fine. "VoIP fraud sours a relationship, destroys trust and leads to costly disputes, which drives up churn and increases bad debt," said Boraman. "But the combination of a poor customer experience and increased churn does focus minds on tackling the problem. We are finally seeing a shift in reseller attitude towards understanding and preventing fraud as they are realising that it also impacts them."

Iain Sinnott

SPs need to consider security in every element of every product they release within the VoIP portfolio, and make security a focused element in partner training.

The ability to spot attacks in advance and address the moving nature of VoIP fraud before it happens is the key to shutting down this highly lucrative method of generating money, observed Boraman. "For example, fraudsters are creating smaller and more frequent 'pick-pocket' style hits across multiple end customers simultaneously," he added. "They use robo-diallers to make high volumes of very short calls, typically 15-25 seconds, to multiple destinations that go unnoticed. This type of fraud is hard to spot and stop in a timely fashion unless you use real-time call profiling, call pattern behaviour monitoring and analytics as part of the fraud management system. Carriers need to use technology that spots the first 'test' call attempt made by the fraudster, regardless of the call durations, and take action to block further attempts."

Firing line

Every business is facing a host of new threats such as these and it is the providers, vendors and their resellers that are in the firing line. "It's up to us to mitigate some of the risks," commented Boraman. "It's not just about storing the right data, it is also about testing for resilience and being constantly vigilant in preparing for attacks. Traditionally, carriers have managed fraud on behalf of the reseller and their customer behind the scenes. Future market developments will be about empowering resellers to see more and do more by giving them direct access to the fraud management tools, and training them on how to protect their customers and apply anti-fraud measures.

"A more collaborative relationship between customers, resellers and providers on individual thresholds, rules and limits is essential in the fight against fraud. Security should be at the heart of a proposition and there needs to be a strong alignment between the vendor, customer and supplier. With machine learning and AI, combined with big data and crowd sourcing of key information from carriers around the world, we can become proactive in the fight against fraud."

Although a source of misery for all those impacted, the containment of toll fraud has nonetheless improved over recent years, observed Firstcom Europe Group CTO Adam Crisp. "But where there's a will there's a way, so businesses must protect their communications infrastructure," he stated. "On VoIP call security, information is present in calls with spoken voice or DTMF data and this should be protected. Data can be processed (switching equipment could be vulnerable to hackers), stored (think information in call recordings) and transmitted (think about VoIP media streams running over the public Internet and eavesdropping). Moreover, GDPR defines 'processed' to mean processed, stored and transmitted, so any business not protecting their VoIP calls in all three categories is in breach."

In terms of compliance and GDPR, the customer owns the data and the service provider and channel partners are processors, pointed out Crisp. "Although both parties are potentially liable, the customer is in control of how they procure their telephony and therefore whether or not they choose a secure service," he stated. "Channel partners and service providers must make their customers aware about which service they are choosing. This could be done by publishing a service data privacy policy which shows the customer where data exists. There's now a clear compliance reason to implement call security and protection systems, and customers must deploy them." ■

Adam Crisp

Where there's a will there's a way, so businesses must protect their communications infrastructure.