

Trusting in VoIP

Harnessing the benefits of VoIP while maintaining security

With frequent calls between widely dispersed locations, telecommunications can be a major cost for the financial sector. This is why VoIP, a rapidly growing technology that helps reduce costs and improve efficiency by converging traffic onto a single IP network, is being adopted enthusiastically by financial services companies. According to recent figures from Gartner, financial institutions account for 16% of the total Voice over IP (VoIP) market. This is already an impressive figure, and one that is growing fast.

The move to IP-based next-generation networks delivers cost savings and increases operational efficiency for enterprises. Carrying voice, data and other traffic across a single, unified network reduces management time and costs, simplifying processes by streamlining the types of technology deployed. For service-focused organisations like financial companies, this is often shown most clearly in the call centre, a business critical function that delivers the quality customer service that creates competitive advantage – traditionally at a high cost. However, with VoIP, call costs can be reduced. This is a significant driver in itself, but more than that, with VoIP the call centre becomes more agile, able to be scaled up rapidly with little additional cost.

The benefits of VoIP are clear and the business case may seem straight forward. However, as with any new technology deployment, businesses must think carefully about a number of issues and balance the benefits against costs and potential challenges. Security is always a fundamental concern when evaluating a new technology, particularly for financial services companies, which have a duty to protect the sensitive personal data that customers entrust to them. There is some confusion around security for VoIP following misleading media coverage of this issue.

There remains a lack of distinction between general technology security threats such as viruses or 'phishing' attacks and VoIP-specific threats. In reality, most security threats are incidental to the use of VoIP. However, sensational headlines associating VoIP with identity theft confuse the situation and could slow the adoption of VoIP in a sector which can benefit dramatically from the technology.

An example of a security issue which has been misleadingly linked to VoIP is phone phishing, called 'vishing'. Vishing comes in several different flavours. The most common involves an attacker sending a spoofed email containing voice information claiming to come from a bank or financial services provider, stating that the user's account has been frozen due to fraudulent activity and requesting account details to reactivate it, enabling the criminal to harvest vital account information. However, using VoIP does not make a company or its

customers any more susceptible to this type of attack than if they were using traditional methods of communication.

One threat that should be considered seriously when migrating to VoIP is that of Denial of Service (DoS) attacks. DoS can take various forms, but generally involve an attack that overloads the targeted service so that it “falls over” and is inaccessible to end users. There has been much publicity of DoS attacks on well-known e-commerce web sites in the past and these could be mirrored on IP networks, potentially bringing down a financial institution’s call centre by overloading the network. The main threat comes from Internet-connected services and a DoS attack being launched from outside the company. It is possible, however, that certain threats can also come from within an organisation and VoIP deployments need to be protected internally as well.

This type of attack damages customer service; affects revenue-generating opportunities and also damages the brand, a long term problem that can be difficult to quantify but that has serious repercussions. DoS attacks can be prevented by choosing the right provider with a track record in delivering enterprise-grade VoIP solutions – this will ensure that adequate firewalls are built into the solution during the roll-out phase.

The benefits of VoIP adoption are significant, especially for companies with multiple sites, and those whose businesses depend on frequent communication with customers. Careful planning is required to ensure a deployment is successful. Businesses must look to migrate to VoIP solutions that are able to provide multi-layered, pre-emptive protection from threats affecting the infrastructure that supports VoIP without disrupting the quality of service of voice calls and, fundamentally, customer service.