FEATURE

KILLING THE UC GOLDEN GOOSE  
(Part 1)

By Ian Kilpatrick, chairman Wick Hill Group, specialists in secure IP infrastructure solutions

UC is the strategic dream, the ultimate remedy for all customer communications requirements, the golden goose for all our margin needs - or so it seems.

When you Google UC, you get over three million results. An interesting omission from the majority of these results, from many supplier white papers and indeed from a number of the apparent dummies’ guides is a considered discussion of the security issues that UC brings.

What makes this omission spectacularly relevant is that surveys consistently show users rating security as a higher priority than ‘low cost of ownership,’ and that many UC deployment surveys rate security as the main challenge to deployment.

Given that mobile enterprise application access, instant messaging/presence and application/document sharing are top UC applications, security concerns are going to be either early deal preventers or alternatively will lead to a breakdown in the trust relationship with the reseller, as customers recognise their risk status mid-deployment.

While the largest enterprises are proficient at recognising and protecting against security risks, many smaller organisations will continue to sit on their hands over UC deployments.

Although the threats are clear, apparent and active, there is still significant misunderstanding about how they can be defended against. The biggest misconception is that the existing data infrastructure and security solutions deployed are adequate in a converged environment.

This is incorrect. Many of the threats are significantly different between voice-based and data-focussed environments. Two of many examples include defence against toll fraud, and smart phone security.

Toll fraud is the security risk we are most aware of. While it is grotesquely under-reported, there are many indications that it is in the £billions. That kind of level already impacts prospect confidence in UC.

Smart phones provide access to the corporate network for email (often informally) and for other core corporate applications (both authorised and unauthorised). Yet true two factor authentication for smart phone secure connection is still the exception, not the rule.

In different ways, these are two risk areas (of many) that best-practice organisations will need mitigated and conservative organisations will avoid.

To fatten the goose, rather than killing it, we will need to talk the language of security to insecure customers.

ENDS