



With shades of Donald Rumsfeld, Mike Jay, IPCRes Convenor, reviews the known and known unknowns of IP signalling and presents an insurers perspective.

Have you ever had an email disappear into a Black Hole? Or a download fail? Or your broadband or ISP service disappear? If not, you are a very new internet user or you are not using the same products and services as the rest of us.

Yet the public internet will have to be the medium for alarm signalling systems in the future for a large number (may be the majority?) of fire and security systems if the IP Signalling industry's marketing is to be believed.

The driver? Cost of course. Very little seems to be worth paying much for these days and the signalling service protecting your premises should be "free" and why not if you are already on-line with broadband?

At least one of the well known speakers on 'the circuit' on this subject makes a very good point in his presentation, 'IP is not the internet and the internet is not IP'. There is no more reason to be anxious about the internet protocol than any other electronic messaging format that the alarm industry has used to multiplex signals - sounds quaint doesn't it - in order for clients at multiple sites to have affordable signalling.

If you think about it, what have we got against the internet protocol as such anyway? Nothing! Would we care if the 'classic' signalling systems went over to IP? Of course not - if all that changed was the 'language' understood by the signalling transceivers. The banner under which this debate is conducted is a misnomer. It is not an 'internet protocol signalling' debate at all; it's a 'network signalling' debate. As another speaker said recently,

**"...the signalling is only as reliable as the network that carries it..."**

(John Holden, a BRE specialist).

So now we see what the target for this debate should be. It is the use of a network without any pedigree for secure and reliable conveyance of fire and security signals that we should have in our sights. It might be the user's own in-house network or VPN. It will often be the biggest network of all, the unregulated public internet. Once the signal passes across the frontier into the badlands of the lawless web, (worryingly depicted as a formless grey cloud in most of the marketing literature), how confident should we be that it will re-emerged unscathed and in a timely fashion?

In his talk, John Holden advises "use a secure third party network", and in an article in Professional Security Installer magazine, Pete Conway, striving earnestly for balance, asserts that '...networks can be built that are resilient, fault-tolerant and backed up to ensure a continuity of service...' (my emphasis). Good news indeed John and Pete, but who offers these networks!? Also, who has tested them and can vouch for their ongoing performance?

The fact remains that a significant and vocal lobby in the IP signalling market wish us to connect via the public internet, using the ISP of our choice, pointing to the back-up available from the alternate path should the line-connected internet path fail. They would also like us to accept (on face value it seems) that, if an in-house network is available, we can sleep peacefully in our beds because the user will manage his/her network responsibly and ensure that his/her IT people ensure the necessary capacity, never re-prioritise the network to meet other business needs or take down parts of the network for maintenance.

Whatever the network, if the router through which the signalling passes is powered off or it has its connections interfered with, or is reconfigured by an on-line hacker, or through there being no security setup on the WiFi router - then don't worry, a fault signal will be generated and the wireless path will take over. But will it? Not just most of the time, but every time?

To quote Mr Conway again

**"...many insurance companies might avoid recommending IP-based signalling until the technology has demonstrated a reliability that is comparable with currently recommended secure dual signalling options..."**

Well, certainly insurers hate uncertainty and unpredictability. As I am no longer employed by an insurer as such I can remind you that their ethos is conservative and cautious. They are capable of changing rapidly and radically but until there is an overwhelming need to do so, they may take a "why should we?" stance.

Insurers employ few truly technical specialists in a field like this and they rely a lot of the time on weighing up the advice of those who do seem to know what they are talking about. However when they read in one of the security industry's own authoritative magazines that:

**"There are... a number of new faces from the IT sector who have a business model that is focussed more on selling systems than delivering secure solutions."**

And that

**"...it is not the IP protocol that people have a problem with; it is that those with the better knowledge of IP - those from the IT sector - (who) are not considering the secure implementation of that technology..."**

then can you be surprised that insurers allow their natural caution to rule their thinking?

Having said all that, Insurers accept that a position permanently on the fence is not realistic and there has been a certain amount of exposure of collective head-above-parapet and of sucking-and-seeing. For that reason, the IPCRes group has now published the second paper of its two part guidance document on IP Signalling. These papers are positioned for the consumption of insurance underwriters

---

and surveyors but the second paper contains a model of those features and attributes of two generic IP signalling configurations that insurers may be prepared to trial (at one risk level or another) so that experience can be gained.

The model is available to all interested parties and can be viewed by visiting the InFiReS website ([www.infires.co.uk](http://www.infires.co.uk)) and clicking on the link on the home page.

IPCRes is also motivated to take more constructive action than to just print guidance based on what it has learned through research on a word of mouth basis. In a proactive spirit, it has commissioned some modest field research to evaluate the rates of availability of internet based signalling under various conditions. This project will not be rushed and it may be some time before a reliable picture is formed, but initial results will be made known if it seems acceptable to release them.

Will we look back at this period one day and wonder what all the fuss was about - just as we do when we look back to the Y20 thing? Maybe so, but for the moment the words a certain Donald Rumsfeld ring in insurers' ears:

**“There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know.”**

Well, that sums it up nicely Don (and John, and Pete).

Mike Jay convenes the IPCRes group. IPCRes, (Insurer's Property Crime Research Group) monitors the property crime environment for its members, the great majority of UK's commercial insurers. It carries out research and publishes guidance documents on security issues of the day. In previous times it's projects would have been taken on in an ABI forum.