

Telecommunications Fraud Detection

The silent uninsured loss

The need for IT security to protect business critical data and avoid system disruptions has long been publicised and accepted, however many companies employ little or no security when it comes to their voice networks, these are also a portal to the outside world and are equally at risk.

Telecommunication Fraud is the unauthorized illegal access into a telephone system (hacking) by persons intent on making free telephone calls, ultimately at the system owners cost. These fraudsters making *through dial** calls for resale can typically invoke call bills exceeding £ 25,000 over a single weekend operation.

Telecoms hacking will often occur out of hours, when the telephone system and lines are idle and the chances of being discovered are virtually zero. Telecoms fraud is theft pure and simple, most commercial insurance policies do not cover the *loss* of Telephone Calls under the standard policies.

Often perceived as *victimless* these activities leave companies with crippling debts, the victim involved is liable to pay the bills, or face the consequences. Although these activities carry maximum sentences of 5 years in prison and unlimited fines these are rarely applied, hackers are very good at hiding identities and could even be located abroad.

Unlike more physical forms of theft, telecoms hacking is often invisible, there is no alarm system ringing, no Police called and the fraudsters can work undetected for an undefined period, often causing significant cost and disruption to the victim.

It is imperative that all inbuilt PBX security features are deployed efficiently, however the more common forms of PBX hacking involves gaining access to the PBX programming interface and will allow some of these measures to be circumvented.

Itemised telephone bills will offer no consolation, arriving often a month after the event they will simply tell you how much you have lost. Any security system that simply informs you of losses long after the event is of no practical benefit at all.

Elephant fraud detection does not prevent the hacking, in the same way as your fire alarm will not stop a fire starting, but of course like the fire alarm the swift alerting and a fast response from appropriate people will significantly reduce the impact of any attack.

Considering that telecommunication invoices are presented monthly or quarterly and are often a significant cost centre to almost all business users, it is amazing that controls are not put in place to *police* telecommunication systems.

Traditional call logging has been unable to provide adequate protection against such incidents as detection is reliant on someone sitting down to read the information, this can often be days or even weeks after the event.

Elephants inbuilt fraud detection sends alerts to user definable email addresses in pseudo real time. Criteria is flexible and can include triggers based on cost, volume of calls, numbers dialled or attempts to access remote dial in modems etc.

In summary, good housekeeping will reduce your exposure to the potential losses resulting from Telecommunication hacking, and the alerting system built into Elephant will allow you to make a timely response to limit loss in the event of hacking.

* Through dial/off switch divert, a caller is passed out of the telephone system to an external number, the telephone system owner paying for the outbound leg of the call.