

Telecom fraud: The cost of doing nothing just went up

A white paper by
Craig Pollard
Siemens Enterprise



In today's business environment, security is of vital importance. This importance extends to voice networks just as much as data and the risk of a security breach is growing daily.

While cyberattacks, cyberterrorism and assorted other buzzwords gain media attention, the reality is more mundane but just as fatal. Every business is becoming more dependant on information technology and this technology brings with it inevitable vulnerability.

According to the underground network and drum sounds that come out of Hacker Conferences, it is believed that there are a multitude of aggressive, deliberately destructive hackers and that number is growing. Significantly, the methods used to gain unauthorised access to corporate resources is now rapidly extending to embrace telecommunications systems too.

The terrorist threat

Let's address the hacker phenomenon first. Did the communications on two continents ever get disrupted by moving telecommunications satellites? Have computing resources belonging to government agencies been hacked? Have environmental controls in a shopping centre been altered via modem? The

answer to all of these questions is yes. But, unlike other crime groups reported about, the individuals responsible for these incidents are rarely caught.

As if that is not enough, unauthorised use of telecommunications facilities is the preferred methodology for people who sympathise or support terrorist organizations, or who directly participate in terrorist activities themselves, and who want their activities to remain invisible.

The French authorities that studied the terrorist attack on a Madrid commuter train in 2004, for instance, investigated whether the bombers hacked into the telephone exchange of a bank near Paris as they were planning their attack. The telephone calls involved were made by phreaking - a practice similar to hacking that bypasses the charging system.

Combating telephony fraud

The PBX is the darling and among the most popular areas of fraud in telecommunications. Typical methods of inflicting fraud come through the misuse of common PBX functions such as DISA

SIEMENS

Global network of innovation

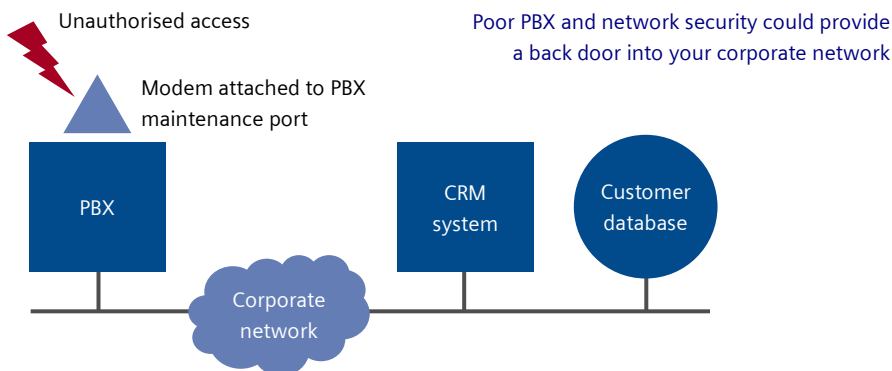
(Direct Inward System Access), Looping, Call Forwarding, Voicemail and Auto Attendant features.

Another area popular with hackers, and where fraud is being constantly committed, surrounds the maintenance port of PBXs – often using the dial-up modem that's attached to such ports to assist in remote maintenance activities. Worse still, when a PBX is linked to an organisation's IT network – as is increasingly the case with Call Centres, for instance – a poorly protected maintenance port can offer hackers an open back door into critical assets such as customer databases and business applications.

The threat from within

As is the trend with hacking data networks, the threat to PBXs comes primarily from within. An employee, contractor or cleaner, for example, could forward an extension in a seldom used meeting room to an overseas number and make international calls by calling a local rate number in the office.

The perpetrator could likewise be the beneficiary of a premium rate telephone number in this country or abroad and serially leave phones off the hook or on a re-direct to that number netting thousands of pounds in illicit gains during a weekend.



When things go wrong

It's clearly important to balance the cost of securing your voice infrastructure from attack against the cost of doing nothing. The consequences from inaction can include:

- Direct financial loss through fraudulent call misuse (internal or external)
- Missed cost savings opportunities through identification on un-needed circuits
- Adverse publicity, damage to reputation and loss of customer confidence
- Litigation and consequential financial loss
- Loss of service and inability to dispense contractual obligations
- Regulatory fines or increased regulatory supervision

And, of course, let's not forget about the new technology in the field of telecommunications such as IP-driven PBXs supported by all the adjunct devices, the deployment of CTS (Computerised Telephone Systems) and CTI (Computer Telephony Integration), Voice over IP and the security revolving around open communications on the Internet.

Prevention is better than cure

So what practical measures can telecom or IT managers take to help prevent being another victim of crime?

One of the most effective approaches to improving the security of telephony systems includes conducting regular audits of:

- Station privileges and restrictions
- Voice and data calling patterns
- Public and private network routing access

