

# Telecom fraud: The cost of doing nothing just went up

A white paper by  
Craig Pollard  
Insight Consulting



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

**Insight Consulting**

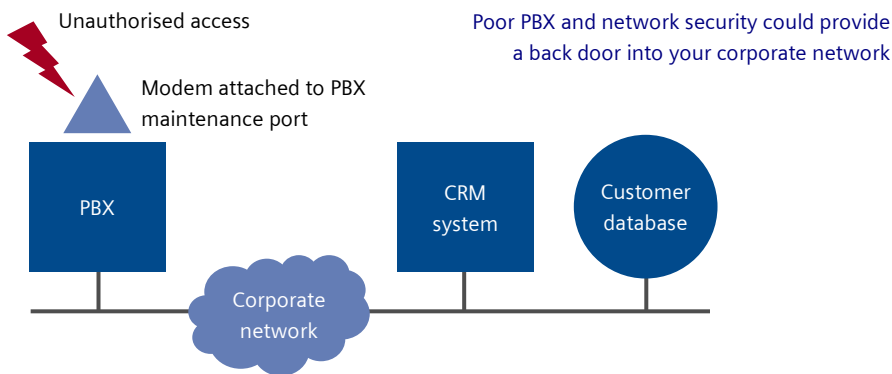
(Direct Inward System Access), Looping, Call Forwarding, Voicemail and Auto Attendant features.

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

- Automatic route selection
- Software defined networks
- Private switched and tandem networks
- System management and maintenance capabilities
- Auto attendant and voicemail
- Direct inward system access (DISA)
- Call centre services (ACD)
- Station message detail reporting
- Adjunct system privileges
- Remote maintenance protection
- Primary cable terminations and physical security of the site and equipment rooms

Other measures include reviewing the configuration of your PBX in the light of known hacker techniques and comparing configuration details against best practice and any regulatory requirements that may pertain to your industry sector.

Ensure default voicemail and maintenance passwords are changed and introduce a policy to prevent easily guessable passwords being used. Make sure that the policy demands regular password changes and take steps to ensure the policy is enforced.

Installing a call logging solution, to provide notification of suspicious activity on your PBX, is a useful measure and one that can often afford valuable early warning of an attack. Review existing PBX control functions that might be at risk or which could allow errors to occur, too.

Be aware that many voice systems now have an IP address and are therefore connected to your data network – assess what provisions you have to segment both networks. Security exposures can also result from the way multiple PBX platforms are connected across a corporate network or from interconnectivity with existing applications.

Research and investigate operating system weaknesses - including analytical findings, manufacturer recommendations, prioritisation and mitigation or closure needs - and implement a regular schedule of reviewing server service packs, patches, hot-fixes and anti-virus software.

Finally, formalise and instigate a regular testing plan that includes prioritisation of the elements and components to be assessed and supplement this by conducting a series of probing exercises to confirm the effectiveness of the security controls used.

Recognising that the expertise to achieve this level of security on a voice network can be advanced in nature, Insight and Siemens have drawn on their combined expertise in information security and telephony solutions to introduce a new portfolio of voice security services that provide a comprehensive approach to mitigating the threats described.

The services include security audits, vulnerability assessments, incident response, forensic investigation as well as telecom policy review and development and will be available for voice equipment from Avaya, Cisco, Ericsson, Nortel, Mitel, Siemens and others.

## Key facts

- Unsecured maintenance ports on PBXs can provide a back door into corporate networks
- Regular audits are one of the most effective approaches to improving and maintaining the security of telephone systems
- Call logging solutions can often provide valuable early warning of an attack on your PBX
- Formalise and instigate a regular testing plan that includes prioritisation of the components to be assessed



Insight Consulting is the specialist security, compliance and continuity unit of Siemens Communications.

We offer a complete, end-to-end portfolio encompassing:

- Research
- Consultancy
- Testing
- Implementation
- Training
- Recruitment
- Managed services

Insight is BS7799 certified, is a GCat and S-Cat (Category 7) supplier and subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services.

If you'd like to discuss how Insight could help you manage risk in your organisation, email us at [insight@insight.co.uk](mailto:insight@insight.co.uk) or visit [www.insight.co.uk](http://www.insight.co.uk)

## Insight Consulting

Churchfield House  
5 The Quintet  
Churchfield Road  
Walton on Thames  
Surrey KT12 2TZ  
United Kingdom  
Tel: +44 (0)1932 241000  
Fax: +44 (0)1932 244590