

## Protect Your Organization from Long Distance Abuse

Think your organization is immune from long distance abuse? On average, over 22% of telephone calls made during business hours are not business related<sup>1</sup>, and the general rule is that 10% of employees make long distance calls to friends and family<sup>2</sup>. The results are wasted phone charges, as well as lost productivity and revenue.

The good news is that you can protect your organization from long distance abuse with call accounting software. Typical software in this category will produce a variety of different reports on long distance and other calls including:

- Detail and summary reports
- Reports on all telephone activity by extensions
- Reports by departments
- Reports by trunk
- Account codes
- Call types
- Most expensive calls
- Longest calls
- Frequently dialed numbers
- Exception reports

Reports can be automatically emailed to department heads to help set daily, weekly, and monthly budgets and goals.

Call accounting software has many other bottom-line advantages including identifying long distance charges per line and verifying the accuracy of phone bills. You can also see what you are paying for other services such as data, video and imaging.

Call accounting systems are useful for network optimization, including determination of the best combination of carriers. The technology can also help with phone system diagnostics. You can determine phone system performance, evaluate if all lines are working, and determine if all of the circuit packs are operational. Typical call accounting technology can tell you which lines you're getting traffic on, or which line carried a 48-hour long call overseas. Additional functionality includes 911 and other custom alarms that can be set up to alert staff of any emergency calls being made from the business.

### External Long Distance Call Fraud

Another potent threat is external toll fraud. If UDP port 5060 (SIP) is left open on your network, a hacker may be able to access your PBX for the purpose of making free long distance calls. A recent attack on VoIP phone systems in Romania resulted in 11 million Euro worth of damages to the victims<sup>3</sup>.



102 Timbertrace Ct.  
Columbia, SC 29212  
1-866-IDEACOM (433-2266)  
[www.ideacom.org](http://www.ideacom.org)

To engage in toll fraud, a hacker will ping out IP addresses looking for an organization that left UDP port 5060 open on the network. One way to protect against this is to have the outside firewall block SIP traffic from unknown sources. Another step would be to have the IPPBX use a non-standard port number for SIP traffic, known only to your enterprise devices.

A simpler method of this type of fraud is for hackers to gain access to your PBX through the voicemail system. System access is gained due to voicemail menus that are not properly password protected. Cautioning staff to not use simple passwords (such as 1234) and not to leave default passwords in place is good start towards dealing with this issue.

#### Ongoing Threat

A recent study found that 90% of resellers still don't fully appreciate the security risks associated with IP telephony, particularly toll fraud<sup>4</sup>.

### Cellular Cloning

With the advent of digital phones and GSM technology, the rate of cellular cloning fraud has dropped off. But it is still a possibility as there is a lucrative black market in stolen and cloned SIM cards. If your business pays for your employee cell phones, that puts you on the hook for another form of long distance fraud. One of the best methods to protect against cell cloning is to ensure employee verification using Personal Identification Number (PIN) codes. An 8-digit PIN requires approximately 50,000,000 guesses and tests conducted have proved that having a PIN code reduced fraud by more than 80%<sup>5</sup>. Cell cloning defense also depends in large part on the carrier. By deploying encryption, call blocking and blacklisting, user verification, traffic analysis and other security measures, carriers can put a serious dent in shutting down this form of fraud.

It is always advisable to ensure that company mobile devices are covered by your corporate security policy. Call accounting software is also useful in protecting against these types of abuses. When you have the visibility to identify call patterns that are out of the norm, you can identify fraudulent access to your business call portfolio.

With the right strategy and vigilance, you can dramatically reduce your vulnerability to long distance abuse. Whether the threat is as serious as a hacker trying to sell access to your long distance service, or as benign as someone calling an Aunt or Uncle, the method of dealing with both issues is often the same.

<sup>1</sup> "Why Call Accounting," Trisys, Inc., <http://www.trisys.com/callacc.htm>

<sup>2</sup> "Why Do You Need Call Accounting," Trisys, Inc., <http://www.trisys.com/callacc.htm>

<sup>3</sup> "11 Million Euro Loss in VoIP fraud...and My VoIP Logs," SIPVICIOUS by EnableSecurity, (December 14, 2010), <http://blog.sipvicious.org/>

<sup>4</sup> Christine Horton, "Nine out of 10 IP Resellers don't Appreciate Security Risks," ChannelPro, (December 6, 2010), [http://www.channelpro.co.uk/news/689682/nine\\_out\\_of\\_10\\_ip\\_resellers\\_dont\\_appreciate\\_security\\_risks.html](http://www.channelpro.co.uk/news/689682/nine_out_of_10_ip_resellers_dont_appreciate_security_risks.html)

<sup>5</sup> "Technical Paper on Mobile Phone Cloning," TechPaperStore, (2009),

<http://techpaperstore.blogspot.com/2009/03/mobile-phone-cloning.html>



102 Timbertrace Ct.  
Columbia, SC 29212  
1-866-IDEACOM (433-2266)  
[www.ideacom.org](http://www.ideacom.org)