Vol. 3 No. 5
May 2011

BUSINESS insights

What is Long Distance Abuse Costing You?

Think your organization is immune from long distance abuse? On average, over 22% of telephone calls made during business hours are not business related[1], and the general rule is that 10% of employees make long distance calls to friends and family[2]. 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. There are very simple reasons why call accounting software can protect your business.

- You can educate your employees as to how much their personal long distance calls are costing the organization
- You can verify the long distance charges on your bill for accuracy and ensure that the charges are legitimate
- You can see what each line is costing you and allocate them in the most efficient manner possible

Here is an example of how call accounting software can be used, based on a true story: Every third or fourth Friday afternoon, a large factory received bomb threats. Each time, they would clear the factory, searching the premises for an explosive device. By the time they had finished checking, it was too late to start up production for that day. Then, someone at the organization thought to check the call accounting records. It turned out the calls were coming from a phone in the factory floor. The whole scenario was a scheme to get the afternoon off.

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

Typical signs of fraudulent activity include increases in wrong number or hang-up calls, increases in call traffic during non-business hours and unexplained 1-900 calls.

IDEACOM® NETWORK
102 Timbertrace Ct.
Columbia, SC 29212
1-866-IDEACOM (433-2266)
www.ideacom.org

Reports can be automatically emailed to department heads to help set daily, weekly, and monthly budgets and goals. Call accounting systems are useful for network optimization, including determination of the best combination of carriers. 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. It is possible for a hacker to access your phone system 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[3]. Be sure to talk to your phone system vendor and learn what kind of safeguards and security features are in place to prevent unauthorized access.

An even simpler method of this type of fraud is for hackers to gain access to your 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 an easy way to deal 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[4].

Cellular Cloning

With the advent of digital phones, 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%[5]. 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.

---

[1] "Why Call Accounting," Trisys, Inc., http://www.trisys.com/callacc.htm

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

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

[4] 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

[5] "Technical Paper on Mobile Phone Cloning," TechPaperStore, (2009), http://techpaperstore.blogspot.com/2009/03/mobile-phone-cloning.html

IDEACOM® NETWORK
102 Timbertrace Ct.
Columbia, SC 29212
1-866-IDEACOM (433-2266)
www.ideacom.org