



The Communicator

A Monthly Telecom Update from RAM Communications

Vol 2
Issue 5

copyright
2003

voice 847.358.0917 fax 847.358.1340 www.ramcomminc.com info@ramcomminc.com

New Directory Service Option

RAM Communications can further help clients who wish to lower their directory service costs. For those businesses who allow their employees to dial 411 for number information, there is an alternative to traditional directory service.

US Directory Services is an independent communications company specializing in discounted directory service. The service is fast and accurate according to the few clients we have asked to sample the product. The potential savings can be 25 to 40% depending upon your company's current provider. Ameritech local directory service is 95 cents per call. Competitive carriers typically charge 75 cents per call. US Directory Service charges 55 cents per call. The service is also designed to minimize the expensive connection fees associated with traditional local and national directory services.

US Directory Service is not for everyone. US Directory requires a \$25.00 monthly commitment for 411 calling. US Directory is so confident in their product, potential customers are allowed to sample the service free for one day.

Clients receive a separate bill. There are also programming procedures that have to be implemented on your phone system in order to use the new service. The programming is necessary so 411 calls are connected to US Directory instead of the local carrier. US Directory provides customers an 800 number to access the service. Depending upon your company's comfort level, programming changes can be avoided altogether by using the 800 number directly. Some clients actually program the 800 number on their speed dials instead of dialing 411.

If your company is interested in more information, call RAM Communications today. We will help you determine if US Directory Services are right for your business.

Plan Ahead . . .

Like many industries, telecommunications has been hit hard by decreases in demand and investment. Not surprisingly, every single carrier in the country has been forced to lay off personnel. This has increased the delivery time for new service installations and what we call, "moves, adds and changes". RAM always works hard to meet every customer deadline. Clients can, however, help their own cause by planning accordingly.

RAM suggests the following timelines:

Analog line installs	2-3 weeks
Internet T1's	4-5 weeks
Private line (P2P) circuits	3-4 weeks
PRI services	5-6 weeks
New phone numbers	1-2 weeks
New toll free numbers	1-2 weeks
Service relocation	6-8 weeks
Local Number Portability	4-6 weeks

Acronym Corner

What do all those crazy terms stand for? What do they all mean? Here's a few more:

MAC Moves, Adds and Changes order modifies a customer's current telecom services

PHISHING criminals looking for personal information via deceptive internet tools or sites

IRC Internet Relay Chat is a method of live internet chat designed to prevent outside monitoring

Saving Clients Time, Money and Aggravation



The Communicator

A Monthly Telecom Update from RAM Communications

Vol 2
Issue 5

copyright
2003

voice 847.358.0917 fax 847.358.1340 www.ramcomminc.com info@ramcomminc.com

Security Risks:

Recently, I had the opportunity to visit a lecture on internet security at DePaul University. What I found was both interesting and alarming.

Business executives and IT professionals owe it to themselves to update their internal and external computer services.

In previous newsletters, RAM has highlighted the importance of incorporating proper firewall security for all internet connections. If your business does not have a dedicated IT professional or computer vendor, RAM can recommend several qualified vendors suited to your company's needs and budgets.

The DePaul lecture focused on two issues: internal and external risks to company information. According to the FBI, there is a tremendous amount of internal, employee theft. In fact, your employees pose the biggest security risk to your company data. In most cases, employees are not being malicious as much as they are carelessly sharing files and internal emails. To a large extent, businesses can prevent employee theft simply by establishing sound, computer procedures. According to FBI investigators, many corporations fail to document or establish thorough computer policies. For example, does your business allow employees to download internet radio services or movie players? Take a look around your office. If it's not stated in company policy, savvy computer users may be consuming precious internet bandwidth and company time. How much money does your

business lose to "recreational computer use"? Are there guidelines in place for company laptop computers? What software can be installed? What is prohibited? Computer viruses are easily transferred by laptop users when they are connected to the company network. Is your network equipped with protective software that monitors each client workstation? If you're not sure, your computer servers may be vulnerable to viruses and potential downtime.

People are creatures of habit and people also thrive on structure. It is up to business management to establish and update computer policies so everyone has a clear understanding of what is and what is not acceptable computer use. Many users are not even aware their work habits can be damaging to the network. According to the IT Professors at DePaul, your computer policies should help educate and regulate users.

As for external threats, virus attacks are well documented today. Corporations are now asking law enforcement agencies like the Secret Service and the FBI to help investigate and prosecute internet crimes. After the DePaul lecture, I feel fairly confident the federal government is doing their part to help prevent internet crimes. ISP's or, internet service providers are also being asked to help monitor suspicious activity on their networks. However, the ISP's do not have enough resources to capture and review all the data crossing their networks. We're talking about terabytes of information. (That's really big, folks.) ISP's are required to keep records of electronic signatures, health care records and financial transactions that occur online.

Firewall protection, company policy reviews and proper reporting of criminal activity help your business and the community at large. If you have complaints of internet crimes, you can report your findings to the FBI at: www.ifccfbi.gov. Otherwise, you've been warned.

Saving Clients Time, Money and Aggravation