SBC Pacific Bell

CONSULTANT/VENDOR CVSG SALES GROUP

SECURITY
SPECIAL ISSUE
UPDATE – January 2002

THE INSIDE SCOOP

Pacific Bell Broadcast Feb. 13th

LIVE from 9-11:30am PST.

- You're invited to hear the latest SBC/ Pacific Bell News – Call your Liaison Manager or 888-889-6010 for further details. You can be a streamer or visit a location to view.

Daley Named President of SBC

- Former United States Secretary of Commerce William M. Daley has been named President of SBC Communications, reporting to Chairman & CEO Ed Whitacre Jr. He'll be responsible for Strategic Planning, Regulatory Matters, Governmental Initiatives, External Affairs and International Affairs.

SBC-Yahoo! Alliance

- SBC & Yahoo! have formed a strategic alliance to provide broadband access to millions in SBC's 13-state region. They'll offer a co-branded, premium DSL Internet & dial-up service. Expected to launch in mid-2002, the first of its kind service will include a suite of Yahoo! and SBC customized products and services, including many optimized for broadband.

Stay tuned.

HAPPY NEW YEAR!

VICE PRESIDENT'S CORNER

HOW TO BECOME MORE SECURE

"How Secure is Your Business & Your Customers'?" was my cover story in our last issue of ***Update***. Ironically, it was being distributed on Sept. 11th, when most of the World's Vision of "Security" changed, forever. Can we ever feel & be secure again? Benjamin Franklin once said, "The way to be safe is never to be secure." But U.S. Supreme Court Justice William O. Douglas said, "Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness & adapting others to current facts." In this Special Issue of ***Update***, we decided to examine this topic, to look at Security, what you can do about it and how you may be able to attain it. In this issue you'll read an ***Update*** Exclusive Special Report on "Information Security" from Paul Eaton of Booz Allen Hamilton; "The FBI's Top 20 Security Flaws," "How to Handle the 20 Most Critical Internet Security Threats"; "Call Center Business Disruption & Disaster Recovery," plus more on things you can do to tighten your Security. Our columnist, Jagdish Kohli, Ph.D., even looks at "Security through Biometric Technology & Applications". There's even a "Personal Security – Identity Theft" article plus more on SBC/Pacific Bell's latest Products & Services. This issue is designed to help you, our readers & your family and clients. Your Security & Success is Our Mission!

"Security can only be achieved through constant change...."

Kari

– ***Kari Watanabe***
Consultant/Vendor Sales Group
Vice President
(415) 542-4516
e-mail: kmwatan@pacbell.com

An Update Exclusive Special Report...

INFORMATION SECURITY: THE APPROACH AND THE SOLUTION

By Paul Eaton of Booz Allen Hamilton

During an Armed Forces Communications and Electronics Association (AFCEA) sponsored event on the USS Hornet in March of 2001, Booz Allen Hamilton Vice President and former Director of the National Security Agency (NSA), Mike McConnell (Vice Admiral, USN ret.) (pictured at right) stated, "Our technology is far greater than any in the World. Foreign countries know that, and are now using the technology we have in computers and communications as a weapon against the security of the United States. We as a nation have to stand up to that challenge and pay greater attention to the overall area of security."

September 11th brought that statement to the forefront of our minds both from a physical and cyber standpoint. It also left senior managers in the public and private sectors pondering key questions about the security of their own architecture. Across the country, many of the same questions were being asked around boardroom tables of government agencies and commercial companies:

- What danger does terrorism pose to the physical security of employees and facilities?

(continued on page 6)

Jagdish Kohli, Ph.D

Security: Biometric Technology and Applications

Biometric technology successfully establishes the positive identity of a person based on the parts of the human body such as the hands, the face, and the eye's iris/retina. Passwords, though still extensively used, are fast becoming a hazard, requiring an enhanced method of security. Positive identification of individuals is a serious business considering the following situations:

- Credit card use for billions of transactions either at the point-of-sale, by telephone, via fixed Internet or mobile Internet.
- Mobile phones and calling card use by millions of people on the go.
- ATM card use for a number of financial transactions at banks and shopping malls.
- People have to be allowed access to restricted areas only if they are authorized.
- Attendance is to be recorded in all kinds of workplaces eliminating 'buddy punching" and "ghost workers".
- Social and medical benefits have to be paid by the state to qualified people.
- Criminals have to be caught and proven guilty without a doubt.

In this article we explore the following areas of biometrics for enhanced security:

- Biometrics Overview
- Verification and Identification
- Fingerprint Recognition
- Facial Recognition
- Iris/Retina Recognition
- Multi Biometrics
- Summary
- The Future

Biometrics Overview

A young technology called biometrics, which has struggled to get off the ground, suddenly finds itself in the spotlight because of the September 11, 2001 (9/11) attacks in New York and Washington DC. Biometrics is the science of using unique characteristics of an individual's body parts as identifiers.

Biometric systems consist of both hardware and software; the hardware captures the salient human characteristics, and the software interprets the resulting data and determines acceptability. The crucial step in building an effective biometric system is enrollment. During enrollment each user, beginning with the administrator who controls the system, provides samples of that system's specific biometric characteristics by interacting with the scanning hardware.

"The optimist sees the opportunity in every challenge; the pessimist sees the challenge in every opportunity."

The original biometric is the fingerprint, but it is not the only part of our bodies that can be used as an ID tag. The iris and retina of our eyes, the characteristics of our faces, our voices, all can be read by computers like bar codes.

Biometrics holds particular promise in two areas of airport security:

When used as high-tech ID tags, biometrics can help verify that passengers and employees are who they say they are. In what is called one-to-one comparisons, the systems verify that someone's face or fingerprint is the same today as it was yesterday.

The technologies can be used to see if a face or a fingerprint shows up in a database of known terrorism suspects or criminals.

Verification and Identification

When we enter our PIN at the ATM, we are not identifying ourselves. The ATM card itself is the identification. By inserting the card into the ATM, we are claiming to be the person whose name is imprinted on the front of the card. The PIN serves as a verification of this fact. What if the card and PIN are stolen? The person can withdraw the money with a stolen identity and get away with it. The answer to plug this loophole is to identify the user with biometrics input such as fingerprint or face recognition. The above scenario also applies to many other situations such as credit card purchases over the Internet, telephones or mobile devices.

Biometric technologies are moving in the direction where no claimed ID is needed, and a true identification can take place. In this case, we would walk up to an ATM, submit a biometric sample, and get our money, without using an ATM card to claim an identity. Here, the biometric is actually identifying us as opposed to verifying a claimed identity.

Verification is a one-to-one search where a claimed identity is proven valid or not. On the other hand, identification is a one-to-many search where someone is identified with no prior claimed identity. Generally, every biometric is more accurate at performing verifications than identifications.

Fingerprint Recognition

Fingerprint recognition technology identifies an individual based upon the unique characteristics of each person's fingerprint. This system consists of a hardware scanner and recognition software. The unique characteristics of a fingerprint consist of a set of ridge patterns and minutiae (the places where the finger's ridges stop, fork, break, for example- Figure 1). During the enrollment process, each user's fingerprints are stored as a data map in a template. Whenever the user tries to gain access, the user's fingerprint is compared with the stored template and access allowed or denied based on system identification.

Fingerprint systems are accurate, but they can be affected by changes in the fingerprint (burns, scars, and so on) and by dirt, oil and other factors that distort the image.

Figure 1: A fingerprint pattern

Fingerprint based systems have been in use for a long time. History has recorded that a British Magistrate in Calcutta first used the fingerprint in India in the year 1898. What has been used for over 100 years and proven effective, is itself the ultimate statement of this biometric technology now enhanced with the use of computers.

Finger imaging has the following characteristics when used as passwords or access IDs:

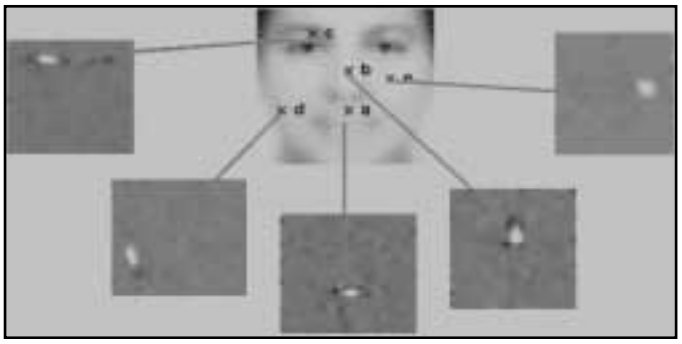
- Fingerprints do not change with time.
- Fingerprints stop unauthorized access.
- Fingerprint systems are easy to use and are cost-effective.
- Users do not forget their fingers.
- A uniform fingerprint system can be implemented in multinational corporations or at national/international airports

Facial Recognition

Facial recognition is a biometric technology that uses an image either from a camera or a photograph to recognize a person. Unlike other biometrics technologies, facial recognition is a passive biometrics and does not require a person's co-operation. It can recognize people from a distance without them even realizing that they are being analyzed. Facial recognition is completely oblivious to differences in appearances as a result of race and gender. This technology is very robust against changes in lighting, facial hair, cosmetics, expression, aging, hairstyle and pose.

The technology uses a highly sophisticated algorithm called Local Feature Analysis (LFA) to identify and derive representation in terms of the spatial relationship between selected local features or nodal points on the face (Figure 2). The algorithm allows for automatic detection of certain landmarks on the human face (such as eyes, nose, eyebrow, lip etc.) and defines identity based on spatial relationship between each of these landmarks. During the enrollment process, the facial recognition engine converts a picture into a compressed data map that acts as a template for comparison with current identification. Due to the small template size, faces can be searched and compared at a very fast speed.

Figure 2: Key facial feature nodal points



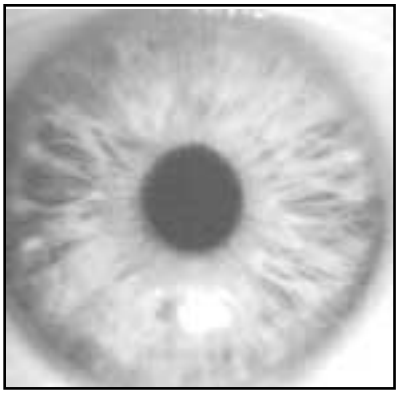
Source: www.biocom.tv.com

Facial recognition technology has been used extensively throughout the World over the last three to five years in such industries like Banking, Gaming, Healthcare, Law Enforcement, Customs and Excise and Retail.

Iris/Retina Recognition

The pattern of the iris is complex, with a variety of features unique in each person. These are named corona, crypts, filaments, freckles, pits, radial furrows and striations (Figure 3). An iris recognition system uses a video camera to capture the sample and software to compare the resulting data against stored templates.

Figure 3: Meshwork and other feature illustration of a human iris



Source: www.labs.bt.com

The retina biometric analyses the layers of blood vessels situated at the back of the eye. The retinal image is difficult to capture, and during enrollment the user must focus on a point while holding very still so the camera can perform the capture properly. The only thing that is actually determined is the pattern of the blood vessels. Since this pattern is unique in each person, identification can be precise.

The two eye-based systems, iris and retina, are generally considered to offer the best security, because of the distinctiveness of the patterns and the quality of the capture devices.

Multi Biometrics

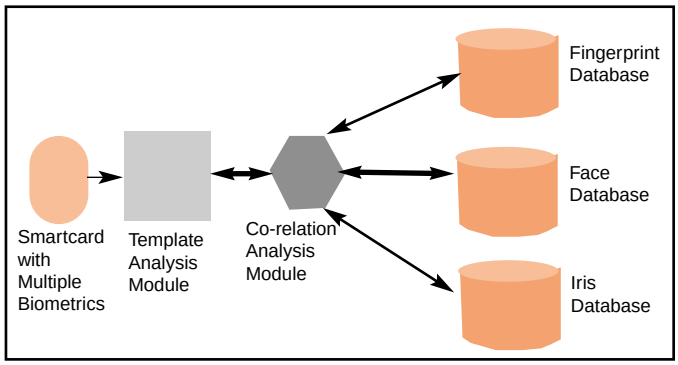
A multi biometric system can be designed by combining two or more biometric technologies. Examples of these systems would include:

- A facial recognition technology combined with voice recognition technology.
- A fingerprints technology combined with handwriting recognition technology.
- An eye recognition system combined with facial recognition system.
- A combination of facial recognition, fingerprint recognition and eye recognition systems.

These systems are being conceived for providing a higher level of security as compared to single biometric system security. An illustrative view of a multi biometric system is shown in Figure 4. In this case, a user carries a smart card with stored user profile including finger, face and eye images. The user presents his/her profile to the system and the system responds with a positive or negative identification.

Some of these systems are in an early stage of development and their success would depend upon the cost, convenience, need and effectiveness.

Figure 4: Components of a multi biometric system.



Source: Healy & Co.

Summary

Need for a robust security system has been elevated to a higher degree because of recent terrorist attacks of 9/11. A number of potential technological security solutions exist for near term deployment. Cost, reliability, convenience of capturing personal identity and privacy protections are some of factors to be weighed in selecting a particular technology for a specific situation or environment.

Near term deployment of currently identified technologies and their success over time will determine the suitability of a particular technology. Multi biometrics will strengthen the security in many applications. A smartcard with a stored fingerprint image, facial photo images and retina & iris images will be a powerful technology for personal identification and verification. This may lead to the development of a national smartcard for security and other applications. A summary of biometric technologies and their respective applications is shown in Table 1.

Table 1: Biometric Technologies and Applications

Technology	Applications	Remarks
Fingerprint Recognition	Law enforcement, Corporate databases	Systems have been deployed for a long time with a high degree of identification accuracy.
Facial Recognition	Airport security, Building surveillance	Systems need minimum involvement of the subject to be identified.
Iris/Retina Recognition	Nuclear facilities, Medical services, Correctional institutions	Systems are intrusive and inconvenient.
Multi Biometrics	High security applications such as access to national classified resources.	Real life systems are in an early stage of development.

Source: Healy & Co.

The Future

A debate has started in various local, regional and national forums to balance the need for security against protecting the rights of the individuals. Most law-abiding citizens would share the needed information for security purposes. It is the role of legislators to enact suitable laws to provide needed protections against the misuse of citizens' private information. Civil libertarians have also voiced their concerns of protecting currently enjoyed liberties of the democratic and free societies as new security measures get implemented.

Some evil individuals and extremist ideology based groups are conceiving new bio terrorism germs based attacks on the civilized world. These threats would allow the development of new real time DNA sensor based technologies. These sensors would be connected wirelessly to the central terrorism control center for a rapid response.

Technology solutions can only go so far in solving human security problems. For the long term, human education and thought process must educate masses of people to respect the sanctity of life, mutual respect for other souls, dignity and compassion to build a healthier social order for peace and human prosperity.

"Above all things," Shakespeare wrote, "to thine own self be true."

Jagdish Kohli is the Principal Consultant at Healy & Co. in the field of IT Strategy and Planning. He has over 22 years of telecommunication industry experience at Bell Labs, Bellcore, Pacific Bell and Telecompetition, Inc. Jagdish holds BS, MS and Ph.D. degrees in Electrical Engineering.

Jagdish recently completed the UMTS Forum's **"3G Portal Study"** – A Reference Handbook for Portal Operators, Developers and the Mobile Industry. This study was approved for publication at the Forum's General Assembly # 24 in Yokohama, Japan.

Jagdish can be reached at jkohli@healy-co.com.

Christine Hertzog
Call Center Solutions
Pacific Bell

Business Disruptions - Is Your Contact Center Prepared?

Like Dante's circles of Hell, business disruptions in Contact Centers are richly differentiated in detail and in levels of pain.

Some disruptions, like the loss of a network for an hour, are temporary and have relatively minor cost impacts. Other disruptions like the loss of a facility to fire or flood can be permanent and/or very costly to an enterprise.

It is a Best Practice in Contact Centers to have a formal Business Disruption Plan. Proactive Contact Center managers identify disaster scenarios and develop detailed responses to address possible disruptions to their operations. These plans are documented and periodically revamped to accommodate changes in business objectives, processes, technologies, and even resources.

Where do you begin in building your Business Disruption Plan? One recommended methodology is to identify a task force that includes Call Center managers, IT and telecom managers, real estate or facilities resources, and HR staff. Step One is to create a matrix that has columns indicating disruption durations. For most businesses, short term is less than 1 week, intermediate term is between 1 week and 1 month, and long term is greater than 1 month. Step Two is to create a list of disruptions categorized by Technology, Facility, and Resources.

Disruption	Short -Term	Intermediate Term	Long-Term
Technology 1. Loss of agent PC	x		
2. Computer virus infection	x		
3. Loss of network	x	x	
4. Etc.			
Facility 1. Bomb scare	x		
2. Fire – facility can be repaired	x	x	x
3. Power blackout	x		
4. Etc.			
Resources 1. Flu epidemic	x		
2. Change in desktop applications	x	x	
3. Reduction in force	x	x	x
4. Etc.			

Once the matrix is defined, the team has a framework that can be easily modified to include other disruptions or different responses based on short, intermediate, and long-term impacts of these disruptions. This framework helps guide the team through the "what-if" scenarios and the diversity of the team ensures that all dependencies, contingencies and even estimated lead times for actions are accounted for in the plan.

Consider a scenario in which a fire destroys a Contact Center facility. The Computer Center is in a different location and is not affected. The team must identify and answer a series of "what" and "who" questions to develop the proper recovery plan. Here are some examples:

- What functions in a Call Center are critical and must be up and running as soon as possible?*
- Can these critical operations be shifted to other Contact Centers within the company? If not, should an outsourcer take the contacts or should a temporary location be outfitted for operations?
- What resources are required to implement the recovery plan?
- What will happen to idled Contact Center agents?
- Who is responsible for internal or external communications regarding the loss of a facility? What will be communicated?

Other scenarios are not so long term as facility destruction but still extremely disruptive to operations. Bomb threats can be a distressingly common occurrence. These incidents require complete, immediate evacuation of facilities…..while calls are still coming in. A simple Disruption Plan might be to provision a Night Service recording, re-route all calls to a Night IVR treatment, call the voice network provider to re-route calls to a different location or send a network busy signal and hustle the people out of the building to designated areas that are safely out of harm's way. Key resources should know their responsibilities to ensure that appropriate calls are made to enact the Disruption Plan and to re-deploy normal operations.

One side benefit of a Business Disruption plan is that some identified disasters may be avoided. For example, power blackouts can be avoided with a back-up generator and UPS equipment. And, it is a Best Practice for Contact Centers to incorporate back-up power into their facilities to eliminate this risk to their operations.

In essence, Business Disruption Plans are detailed project plans that you hope to never deploy. Creating a plan is detailed and tedious work, and like insurance, something you don't want to use. But you will be very glad of its presence if the worst scenarios do become reality – freeing you to deal with the most important part of your operations – your people.

Sadly enough, some centers' processes, technologies, facilities and resources qualify as disasters in and of themselves. Business Disruption Plans can't help these situations – but the SBC/Pacific Bell Call Center Solutions Group has a wide range of solutions that can help!

(continued on page 6)

BUSINESS DISRUPTIONS (CONTINUED)

*This question is easily answered if your Contact Center adheres to another Best Practice – knowing your business. The quantifiable answers are cost per contact and revenue per contact. The qualitative answers are the strategic contributions that the contact center makes to the corporation.

*(For more information on Pacific Bell Call Center Solutions & the development of Business Recovery Plans, contact your liaison manager or Christine Hertzog, Regional Sales Director at **ch7912@msg.pacbell.com** Hertzog has over 15 years experience in Call Centers & Computer Telephone Integration Technologies. She has worked in sales, marketing, product management and as a consultant.)*

FBI's Top 20 Security Flaws
www.sans.org for more information

General

1. Default Installs of operating systems and applications
2. Accounts with No Passwords or weak passwords
3. Non-Existent or Incomplete Backups
4. Large Number of Open Ports
5. Not Filtering Packets for correct incoming and outgoing messages
6. Non-Existent or Incomplete Logging
7. Vulnerable CGI Programs

Windows-specific

1. Unicode Vulnerability (Web Server Folder Traversal)
2. ISAPI Extension Buffer Overflows
3. IIS RDS exploit (Microsoft Remote Data Services)
4. NETBIOS – Unprotected Windows networking shares
5. Information Leaking via null session connections
6. Weak Hashing in SAM (LM Hash)

Unix-specific

1. Buffer Overflows in RPC Services
2. Sendmail Vulnerabilities
3. Bind Weaknesses
4. R Commands
5. LPD (remote print protocol daemon)
6. Sadmind and moundt
7. Default SNMP Strings

What should your agency/company be doing?

- Determine policy ***before*** an attack
- Pre-determine response options to cyber intrusions – they ***will*** come
- Understand the value of your information assets
- Determine current (and anticipate future) vulnerabilities
- Assess the threats (current and future)
- Upgrade internal capabilities in operations and technology
- Raise awareness across your company/agency throughout all levels from end user to system administrators – you are only as strong as your weakest link

Helpful Web Sites

System Administration, Networking and Security Institute
www.sans.org
Critical Infrastructure Assurance Office
http://www.ciao.gov/
National Institute for Standards and Technology
http://www.nist.gov/
Carnegie Mellon Computer Emergency Response Team
http://www.cert.org/

INFORMATION SECURITY: THE APPROACH AND THE SOLUTION (CONTINUED)

- How do we keep information networks open yet secure?
- Does our organization have the right security capabilities?
- How do we assess the value of our information assets?
- Does our data have an adequate level of protection?
- How do we protect against cyber attacks and threats?

Addressing the answers to these questions is an overwhelming task for the country and there are no overnight solutions. Perhaps, in taking the first step, we all need to ask a more basic question about security: What are we trying to accomplish?

At the End of the Day

According to the Computer Emergency Response Team (CERT) Coordination Center, the number of reported network attacks in 2001 is expected to be greater than 46,000*. This projected number would double the number of reported attacks in the year 2000. Keeping in mind that no system can ever be 100% secure, your security solutions should resemble neither an ostrich with its head in the sand, nor act like a black box on an airplane. Instead, it should deliver the delicate balance that allows you to meet your business objectives while simultaneously making sure that you have a program that ensures security is addressed continually and not as an afterthought at the end of the day.

On September 11, each of us experienced a new meaning of Security. Up to that point we wrote about the importance of securing information systems and critical infrastructures but were not real believers or enforcers of security in our daily business activities. Security, in development of new capabilities and technologies, was a secondary objective - something which could wait another day. Focusing on increased processing speed and exchange of data was more important than worrying about the solutions.

Imagine for a moment a 12 inch ruler. Let's say for measurement purposes, relative to security, that we are at the 1/4 inch point on the ruler. As a nation both private and public, we need to rapidly reach a point in security of 9 inches in a short period of time. We have to make up time quickly and determine first what we want to accomplish. This will require our genius, creativity, imagination and a daily practice of security first in our businesses and lives.

The Best Approach for Security Starts with Policy

Some may believe that their security challenges will be resolved by installing a firewall or an Intrusion Detection System (IDS). However, making spontaneous decisions about solutions can actually make a system more vulnerable. An effective security program starts with policy. A defined set of rules, procedures and

**Projection based on more than 35,000 reported incidences in the first nine months of 2001.*

responsibilities not only establishes a baseline for security but the appropriate response to an incident. A security policy is the blueprint by which to build and manage the integrity, reliability, authenticity and confidentiality of automated information. Some of the important areas that need to be addressed in a security policy document include but aren't limited to:

- Definition of security roles
- Procedures and plans for conducting immediate and annual risk assessments
- Contingency and disaster recovery plans
- Strategy for designing a secure desktop
- Training Program for all personnel from System Administrators to End Users

A security policy is an ever-evolving document. A static security policy is quickly rendered obsolete and can often cause more harm than good. It must be re-examined and updated annually as part of your security program and reviewed every time a change is made to your system. Keep in mind, a system is not just the computer and communications mediums - it involves people, facilities and a host of other things. We must be vigilant to the individual elements of a system and not fail to address all elements when changes are made.

The Risk Assessment

Once the rules and responsibilities have been properly defined, the next step is putting your network to the test with a risk assessment. A risk assessment gives you an understanding of your vulnerabilities and allows you to take corrective actions. A risk assessment not only checks that the rules established under your security policy are being followed and enforced, but also includes a penetration test which essentially launches a hacker's attack on your systems to find the weak links in the chain. The results are typically shocking: weak passwords, poor workstation configuration management, and inadequate file permissions. Not surprisingly, most risk assessments highlight "internal" vulnerabilities that are often the weak links in a company's security posture. While all vulnerabilities compromise the security posture of your network, some will not have easy solutions, such as weaknesses that are inherent to operating systems or applications. However, by prioritizing your vulnerabilities and assigning a level of likelihood of occurrence, you can focus your resources on the most critical. So why not simply deploy the most robust security solution on each and every network?

The Appropriate Solution

Biometrics? Virtual Private Networks? Public Key Infrastructure? Smart Cards? These technologies represent some very sophisticated solutions. However, it is important to balance security needs against performance needs. Just as a civil or commercial agency may not have the same security needs as that of national security organizations, a smaller company may not have the same security needs as a Fortune 500 company. The four elements that a secure network should continuously strive to possess are:

Integrity:
Protecting against unauthorized modification or destruction of information

Authentication:
Ensuring the validity of the transmission, message or originator

Confidentiality:
Protecting the unauthorized disclosure of information

Non-repudiation:
Assuring the sender and the recipient cannot deny the exchange of information

The right technology, regardless of its complexity, will deliver some level of assurance that these elements are being met within your network operations.

It's important to remember that not all of the solutions to your security challenges are technological in nature. A majority of the time, the greatest threat to security comes from within – the insider threat, whether it is malicious or by accident. Employee training, from your system administrators through your end users, can solve a lot of weaknesses that arise from a simple lack of awareness. Many employees don't realize the value of the information they hold and therefore simply don't understand the need to protect it. Making security relevant to their jobs can change that.

Summary

In the past, when data was in motion, it was traveling point-to-point with the period of vulnerability being measurable in seconds or minutes. Policies for securing radio traffic data were clearly defined. Today in a world of highly developed networks, data is continually vulnerable in motion and when stored. However, the threats to these networks are growing - espionage, extortion, web site defacement, alteration of data, theft of data, identity theft, denial of service attacks, and viruses.

The question over what can be considered public information and what should be properly safeguarded will continue to be debated as both the public and private sectors rise to the challenge of protecting our nation's infrastructure. As the value of networked information has increased to satisfy business objectives and simplify business operations, the vulnerability of information has also increased. National boundaries are becoming irrelevant. The responsibility of strengthening the security posture of our nation lies with every agency, company and organization that has a connection to it. Its not only time to start thinking about what we are trying to accomplish with network security but to start implementing the elements of Integrity... Authentication…Non-repudiation…Confidentiality. With each of us accepting this responsibility, we can make a difference in our nation's security posture.

Paul Eaton of Booz Allen Hamilton is a member of Pacific Bell's Consultant Council. He leads the Information Technology (IT) Team for Booz Allen Hamilton and has a background in Information Systems for Military Intelligence and National Security. He's based in San Francisco.

TAKE OFF WITH CONFERENCING SERVICES

With current airplane jitters, timesaving needs, and cost-cutting strategies, many former flyers have turned to virtual meetings. In an effort to continue “business as usual”, businesses are using conferencing to conduct meetings, close deals, conduct training, product introductions, sales presentations, employee coverage, inter-company briefings and focus groups. People are finding new ways of conducting business.

Customers are scheduling meetings through ***1-800-CONFERENCE**® They tell us that they are very pleased with the customer support they receive. Customers have the option of receiving assistance from a consultant that walks them through the entire process, allowing them to feel comfortable with the event before diving in.

Conferencing Services Available:

- **Audio Conferencing** includes several options: from operator-assisted service to our ConferenceNOW® service for meetings without reservations.
- **Web Conferencing** enables you to stage PowerPoint presentations or collaborate online while using audio simultaneously.
- **Video Conferencing** allows broadcasting live meetings at assigned locations within your company with smooth images that make you feel right there.
- **Streaming Audio or Video** enhances your conferencing by letting participants join via the Internet, just by clicking a URL address

For more information call **1-800-CONFERENCE (1-800-226-3373 or www.1800conference.com)**

* Long-distance service, when applicable, provided by certificated carriers through Conference Plus, Inc., and will be itemized separately on your bill.

1-800-CONFERENCE® and ConferenceNOW® are registered trademarks of Ameritech Corporation. Service provided by Ameritech Communications, Inc. (a subsidiary of SBC Communications, Inc.) and Conference Plus, Inc.

– Kathleen Horton
Regional Product Market Director
For Voice Products, Pacific Bell

SBC Long Distance News

SBC has won unanimous FCC approval to offer Long Distance Service to customers in Arkansas and Missouri – a successful milestone that follows the company's entry into Texas, Kansas and Oklahoma. With this decision, SBC Southwestern Bell is the first former Regional Bell Operating Company to have all of its states approved to provide Long Distance Service. SBC will now continue to focus on securing regulatory relief in its remaining markets – California, Nevada and the SBC Ameritech Region.

Michael Brennan, Pacific Bell Advanced Enterprise Solutions

COLLABORATION SERVICES *NEEDED NOW MORE THAN EVER*

The events of September 11 created a context, demand, and requirement for organizational use of collaboration services, now more than ever.

Video Conferencing

Organizations that had previously limited the use of ISDN-based video-conferencing to a $100,000 setup in the conference room of the CEO, re-deployed the technology in the days after the terrorist attacks to use it as an alternative to classes and meetings that had to be cancelled. Stock prices of videoconferencing companies rose sharply once the stock markets reopened.

Audio Conferencing

Telephone audio conferencing spiked in its use and have maintained a higher level of calls placed. In fact, a friend commented, "For the first time in six years, I was unable to book a multi-point telephone conference call on short notice because the bridging company said it was overwhelmed with demand and new customers." Then I told him about our **1-800-CONFERENCE** service with guaranteed port availability and ConferenceNOW’s reservation-less service.

Web Conferencing

One of the most dramatic spikes in demand for collaboration services has been with Web Conferencing and the use of virtual classrooms, enabling real-time presentations and interactions over the Web, while conversing on an audio-conference. Organizations have expanded the size of their licenses with WebEx and Placeware, and the use of our **1-800-CONFERENCE** service, which is a pay-per-use service, has also increased.

e-Learning

The use of e-learning also found a larger place on the radar screen in the past few weeks, as organizations turned to Web-based delivery as a potential alternative to classes and seminars that required air travel. In addition, e-learning tools were put into place as an aspect of knowledge dissemination for rapidly changing policies. One large retail organization rapidly assembled an e-learning module on dealing with security threats in local stores. We are seeing significant increases in senior management interest in e-learning capabilities in these tough times.

You see, everything now being done is being done by the most obsolete methods known. And, everything now being done is going to be done differently. And, it’s going to be done better. And, if you don’t do it better, or your company, organization, customers, prospects or suspects don’t do it better – the competition will. Who

knows, they many be nice people to work for after the shock.

Streaming (Audio & Video)

The Web has been used in ways that folks never would have dreamed even two years ago. There were pages for missing relatives posted on the Web within five hours of the attack. Within hours, corporate Intranets streamed messages from the CEO, suggestions for donations, and important process changes for how business procedures were being altered. I was impressed with the speed at which the hospitals within New York City created a joint, searchable database to provide information about the identities of patients who were admitted in the hours following the blast at the World Trade Center.

The world of e-learning and digital collaboration was given an unplanned assignment to demonstrate the new capabilities, and support of linking people and knowledge over time and distance. Now, we may face an even larger role for these tools and processes as we cope with the economic challenges that lie ahead for many of the World's populations. As we read of large-scale layoffs in key industries, it is important to note that training plays a critical role in time of staff reductions.

Organizations that are reducing staff are also shifting the allocation of the remaining staff. People need to be trained to deal with new assignments. Business processes need to be changed to deal with changing customer demand levels. And, there is the need to deal with the motivational elements of severe organizational changes.

We, in the visual communications arena, believe that e-leaning and digital collaboration will have a key role in helping both changing organizations and displaced workers deal with tough times. We can create unprecedented networks of knowledge, support, learning, and retraining capacities for our colleagues who lose their jobs. Digital collaboration can be used to strengthen the supply chain among customers, suppliers, and organizations to increase cooperative planning for changing markets. And, we can find ways of using technology to continue the sense of community and connection that humans need to survive and thrive in difficult times.

A World Full Of Promise

The future will include more and more blends: blended learning that takes classes and e-learning components, blends of video conferencing and face-to-face meetings, and blends of business practices that allow us to go forward with creativity and support. As I see it; for business, it's a world of unprecedented productivity. A world built on state-of-the-art visual communications technologies that facilitate management, planning, communication and evaluation. For people at home, it's a unique opportunity, a chance to explore new ideas and new opportunities. And for each of us as individuals, a world full of promise, a place where we can truly realize our potential: to succeed, to win, through visual communications technologies.

God Bless America

For more information about Visual Communications offered by Pacific Bell, contact Michael Brennan, Regional Sales Director on (949) 838-8244. Brennan began his telecommunications career in 1974. He was a fiber optic engineer in the 80's; a technologist in the 90's and now frequently speaks as a subject matter expert on Visual Communications, Voice/Video over IP and Streaming Media.

PERSONAL SECURITY
IDENTITY THEFT

What to do if you lose your purse or wallet or if they are stolen…

We've all had horror stories about fraud that's committed using your name, address, SSN, credit, etc. Unfortunately I (the author of this piece who happens to be an attorney) have firsthand knowledge, because my wallet was stolen last month and within a week the thieves ordered an expensive monthly cell phone package, applied for a VISA credit card, had a credit line approved to buy a Gateway computer, received a PIN number from DMV to change my driving record information on line and more.

But here's some critical information to limit the damage in case this happens to you or someone you know. As everyone always advises, cancel your credit cards immediately, but the **key is having the toll free numbers and your card numbers handy so you know whom to call**. Keep those where you can find them easily. **File a police report immediately** in the jurisdiction where it was stolen, this provides to credit providers you were diligent, and is a first step toward an investigation (if there ever is one).

Here's what is perhaps most important: (I never ever thought to do this) – **Call the three national credit reporting organizations immediately** to place a fraud alert on your name and SSN. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the internet in my name. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit. By the time I was advised to do this, almost 2 weeks after the theft, all the damage had been done.

There are records of all the credit checks initiated by the thieves' purchases, none of which I knew about before placing the alert. Since then, no additional damage has been done and the thieves threw my wallet away this weekend (someone turned it in). It seems to have stopped them in their tracks.

The numbers are:

- **Equifax:** 1-800-525-6285
- **Experian** (formerly TRW): 1-888-397-3742
- **TransUnion:** 1-800-680-7289
- **Social Security Administration** (Fraud Line): 1-800-269-0271

We pass along jokes; we pass along just about everything. Do Think about passing this information along. It could really help someone.

Identity Theft

See the ***Pacific Bell White Pages' Customer Guide*** to find out more about the fastest growing crime in the U.S. It will tell you what to do. Some important resources, include:

- www.pacbell.com
- www.idtheftcenter.org
- www.privacyrights.org
- www.consumer.gov/idtheft
- www.ifccfbi.gov
- www.dca.ca.gov

HOW TO HANDLE THE 20 MOST CRITICAL INTERNET SECURITY THREATS

By Nalesh Chandra
Associate Director, Managed and Dedicated Hosting & ***Bill Tang****, Associate Director, Data Center Hosting (Co-location) San Ramon, CA*

Companies are increasingly evaluating their security protocols and determining how they will withstand threats and attacks on their business. The good news is that businesses are taking steps in the right direction to protect their buildings and employees. For example, entrance and exit doors are more closely monitored, mailrooms are locked, business travel requires several levels of approval and more uniformed security personnel walk the halls. The bad news is that not enough businesses are moving quickly enough to protect themselves from Internet security threats. Is there something to really worry about?

Unfortunately, there's quite a bit to worry about. Security risks affect Web servers, the local area networks that host Web sites, and even innocent users of Web browsers that can create annoyances or even take down a company's entire web or intranet presence. As soon as a company installs a Web server at a site, they have opened a window into their local network that the entire Internet can look through. Most visitors are content to window shop, but a few will try to view information never intended for public consumption. Others, not content with only looking, will attempt to force their way into the network. The results can range from the embarrassing, for instance discovering one morning that a site's home page has been replaced by an obscene parody, to the damaging, for example the theft of a company's entire database of customer and credit card information.

A web server represents a significant potential hole in a company's local network's security. The general goal of network security is to keep strangers out. Yet the point of a Web site is to provide the world with controlled access to the network. Drawing the line can be difficult. A poorly configured Web server can punch a hole in the most carefully designed firewall system. A poorly configured firewall can make a Web site impossible to use. Things get particularly complicated in an intranet environment, where the Web server must typically be configured to recognize and authenticate various groups of users, each with distinct access privileges.

The following information is a listing of the common Internet security threats and suggestions for handling those threats. This information is technical, but then again, as we have all learned, true security is not easy to come by. Using the suggestions presented here is a great way to start protecting a company's network. This list is an excerpt from: "How To Eliminate The Twenty Most Critical Internet Security Threats" (Version 2.500 - October 10, 2001 - Copyright 2001, The SANS Institute).

Top Vulnerabilities That Affect All Systems

1. Default installs of operating systems and applications

Description:

Most software, including operating systems and applications, comes with installation scripts or installation programs. The goal of these installation programs is to get the systems installed as quickly as possible, with the most useful functions enabled, with the least amount of work being performed by the administrator. To accomplish this goal, the scripts typically install more components than most users need. The vendor philosophy is that it is better to enable functions that are not needed, than to make the user install additional functions when they are needed. This approach, although convenient for the user, creates many of the most dangerous security vulnerabilities because users do not actively maintain and patch software components they don't use. Furthermore, many users fail to realize what is actually installed, leaving dangerous samples on a system simply because users do not know they are there. Those unpatched services provide paths for attackers to take over computers.

For operating systems, default installations nearly always include extraneous services and corresponding open ports. Attackers break into systems via these ports. In most cases the fewer ports you have open, the fewer avenues an attacker can use to compromise your network. For applications, default installations usually include unneeded sample programs or scripts. One of the most serious vulnerabilities with web servers is a sample script; attackers use these scripts to compromise the system or gain information about it. In most cases, the system administrator whose system is compromised did not realize that the sample scripts were installed. Sample scripts are a problem because they usually do not go through the same quality control process as other software. In fact they are shockingly poorly written in many cases. Error checking is often forgotten and the sample scripts offer a fertile ground for buffer overflow attacks.

Systems impacted:

Most operating systems and applications. Keep in mind that almost all third-party web server extensions come with sample files, many of which are extremely dangerous.

How to determine if you are vulnerable:

If you have ever used an installation program to install system or service software (as nearly every company has), and you have not removed unnecessary services and installed all security patches, then your computer system is vulnerable to hacker attack.

Even if you did perform additional configuration steps, you could still be vulnerable. You should run a port scanner and a vulnerability scanner against any system that is to be connected to the Internet. When analyzing the results, keep in mind the principle that your systems should run the smallest number of services and software packages needed to perform the tasks

required of your system. Every extra program or service provides a tool for attackers – especially because most system administrators do not patch services or programs that they are not actively using.

How to protect against it:
Remove unnecessary software; turn off unneeded services, and close extraneous ports. This can be a tedious and time-consuming task. For this reason, many large organizations have developed standard installation guidelines for all operating systems and applications used by the organization. These guidelines include installation of only the minimal features needed for the system to function effectively.
The Center for Internet Security (CIS) has developed a consensus benchmark for minimum security configuration of Solaris and Windows 2000, based on the combined experience and knowledge of more than 170 organizations from a dozen countries (see www.cisecurity.org). Benchmarks and testing tools for other operating systems are in process. The CIS tools can be used to test the level of security and compare the security status of systems across divisions. The CIS guidelines can be used to improve the security of most operating systems.

2. Accounts with No Passwords or Weak Passwords
Description:
Most systems are configured to use passwords as the first, and only, line of defense. User IDs are fairly easy to acquire, and most companies have dial-up access that bypasses the firewall. Therefore, if an attacker can determine an account name and password, he or she can log on to the network. Easy to guess passwords and default passwords are a big problem; but an even bigger one is accounts with no passwords at all. In practice all accounts with weak passwords, default passwords, and no passwords should be removed from your system.

In addition, many systems have built-in or default accounts. These accounts usually have the same password across installations of the software. Attackers commonly look for these accounts, because they are well known to the attacker community. Therefore, any default or built-in accounts also need to be identified and removed from the system.

Systems impacted:
Any operating system or application where users authenticate via a user ID and password.

How to determine if you are vulnerable:
In order to know if you are vulnerable, you need to know what accounts are on your system. The following are the steps that should be performed:

1. Audit the accounts on your systems and create a master list. Do not forget to check passwords on systems like routers and Internet-connected digital printers, copiers and printer controllers.

2. Develop procedures for adding authorized accounts to the list, and for removing accounts when they are no longer in use.

3. Validate the list on a regular basis to make sure no new accounts have been added and that unused accounts have been removed.

4. Run a password-cracking tool against the accounts looking for weak or no passwords. (Make sure you have official written permission before employing a password-cracking tool.)
   a. LC3 – Microsoft Windows NT and Microsoft Windows 2000, **http://www.at stake.com**
   b. Microsoft Personal Security Advisor, – Microsoft Windows NT and Microsoft Windows 2000, **www.microsoft.com/security/mpsa**
   c. John the Ripper – Unix, **http://www.openwall.com/john**
   d. Pandora – Novell, http://www.nmrc.org/pandora

5. Have rigid procedures for removing accounts when employees or contractors leave, or when the accounts are no longer required.

How to protect against it:
To eliminate these password problems, two steps need to be performed. In the first step all accounts with no password are given a password or are removed, and weak passwords are strengthened. Sadly, when users are asked to change and strengthen their passwords, they often pick another one that is easy-to-guess. This brings us to the second step. User passwords should also be validated when they change their password. Computer programs are available to reject any password change that does not meet your security policy. The most popular are described at the urls below:

1a. For UNIX: Npasswd (SunOS 4/5, Digital Unix, HP/UX, and AIX) **http://www.utexas.edu/cc/unix/software/npasswd**
1b. For Unix: Cracklib" and associated PAM modules (Linux)
2. For Windows NT: Passfilt, **http://support.microsoft.com/support/kb/articles/Q161/9/90.asp**

These programs ensure that when passwords are modified, they will be of the length and composition required to make guessing and cracking difficult. Note that many vendor Unix systems include internal support for password hardening, and that there are other packages available as well.

Many organizations supplement password control programs with controls that ensure that passwords are changed regularly, and that old passwords are not reused. If password aging is used, make sure that the users are given warning and chances to change their password before it expires. When faced with the message: "your password has expired and must be changed," users will tend to pick a bad password. Microsoft Windows 2000 includes password constraint options in Group Policy. An administrator can configure the network such that user passwords must have a minimum length, a minimum and maximum age, and other constraints. It is important to require a minimum age on a password. Without it, users tend to change

(continued on page 13)

DATA WITH DAVID

New Optical Product to Meet Increased Bandwidth Demands

One of the major issues in the networking industry today is tremendous demand for more and more bandwidth. This is especially true for companies that must mirror the contents and computing power of their mainframes and storage area networks and assure that valuable data is not lost in an outage. To this end the development of optical network architectures and the use of Dense Wavelength Division Multiplexing (DWDM) technology has played a very crucial role in this network evolution.

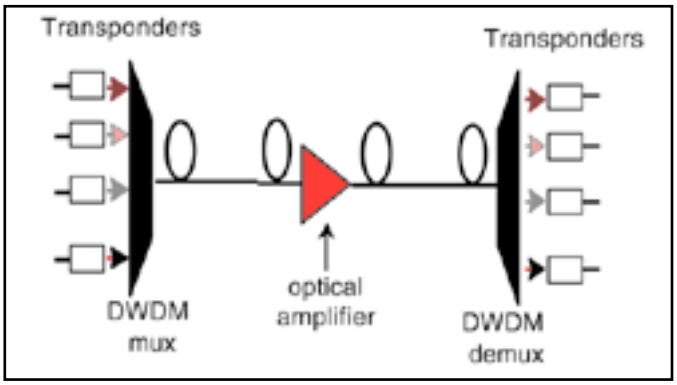
Optical networking uses light to convey signals, enabling the transmission of data over fiber. Optical networks are high-capacity telecommunications networks based on optical technologies and components that provide routing, grooming, and restoration at the wavelength level as well as wavelength-based services. The optical networking market is growing at a rapid pace and according to Aberdeen Group research, the optical networking market, excluding SONET elements, will reach $17.7 billion by 2003.

Multi-Service Optical Network

SBC will be offering a new product in our 13-state region for high-end customers requiring this tremendous bandwidth for mainframe-to-mainframe connectivity and/or data center connectivity applications in a point-to-point setting. The new data service called Multi-service Optical Network (MON) uses DWDM technology and a unique universal optical interface to deliver a wide range of optical protocols. Our initial service offering is a point-to-point architecture while a ring topology will be launched by mid-2002. On November 5, 2001 we filed our California tariff to offer point-to-point service and expect approval in early February, 2002. In the interim, point-to-point service in California will be offered on an individual case basis.

DWDM is an economical way to build and expand networks to meet the unforeseen bandwidth in the local network. Scalable and flexible architecture in DWDM systems minimizes the capital outlay required to meet traffic growth. Customers can purchase a "base" configuration and augment different channels and additional capacity more quickly with DWDM and they have the flexibility to use whatever protocol is the right choice for their network; without changing out the network infrastructure.

The DWDM technology has resulted in the onset of tremendous amount of bandwidth. A single fiber may carry 40 optical signals with each of those signals transmitting data at speeds of up to 2.488 Gbps (SONET OC-48). The high-speed port (2.5 Gbps) will be used for SONET applications only and will always be protected. The lower speed port (1.25 Gbps) is used for all other applications. MON offers scalability and flexibility by allowing customers to change port usage, as their business needs change.



DWDM provides "virtual" fiber. Utilizes existing fiber and expands capacity 32-40 times. Creates optical wave channels; each wave channel can support a unique protocol with the capacity of 2.5 Gbps or more.

Dense Wavelength Division Multiplexing

DWDM technology uses a fiber-optic transmission technique and involves the process of multiplexing many different wavelength signals or colors of light onto a single fiber. Each fiber has a set of parallel optical channels each using slightly different light wavelength. The use of non-overlapping optical channels allows each channel to operate at peak speeds. The technology employs light wavelengths to transmit data parallel-by-bit or serial-by-character. DWDM is a very crucial component of optical networks that will allow the transmission of data: voice, video-IP, ATM and SONET respectively, over the optical layer.

Native Protocols

MON, and the optical CPE offering support a range of transport protocols including Enterprise Systems Connection (ESCON – 200 Mb/s), FICON (1.0625 Gbps), GEOPLEX (Geographically dispersed Parallel SysPlex – a S/390 architecture in which multiple-location host processors appear as a single processor to users), FIBER Channel (1.0625 Gbps – allowing for Storage Area Networks to offload storage requirements from LANs and is a new industry standard that will displace ESCON/FICON), Fast Ethernet (also called 100BaseT), Gigabit Ethernet (1000 Mbps), D1 Video (270 Mbps), OCn SONET (OC3, OC12, OC48 and OC192 in the future) and 10 Gigabit Ethernet in the future.

Data CPE

In collaboration with Nortel Networks, SBC is now able to provide customers with the next generation high-speed data networks that they are demanding to support their bandwidth intensive applications. Both the SBC MON and the Data CPE product offering will utilize the Nortel Networks OPTera Metro 5200 multi-service platform. The Data CPE product will also incorporate the Nortel Networks OPTera Metro 3000 next generation SONET platform for customers who require both optical and electrical interfaces.

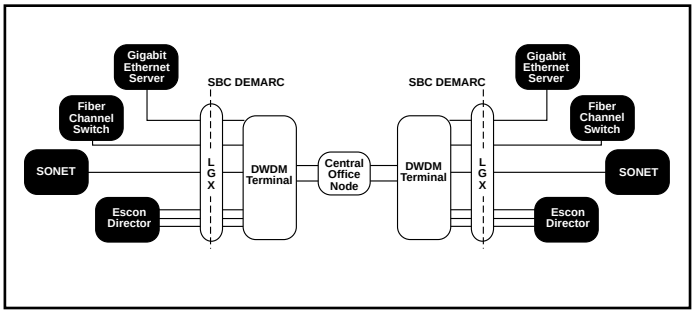
MON Protocols		
Protocol	**Speed**	**Distance limitation**
Escon	200 Mbps	43 km
ETR	8 Mbps	40 km
FICON	1.0625 Gbps	100 km
ISC	1.0625 Gbps	40 km
Fibre Channel	1.0625 Gbps	-
Fast Ethernet	100 Mbps	-
Gb Ethernet	1 Gbps	-
FDDI	100 Mbps	-
D1-Video	270 Mbps	-
SONET OC-3/c	155.52 Mbps	-
SONET OC-12/c	622.08 Mbps	-
SONET OC-48/c	2488.32 Mbps	-
SONET Flexible Speed	From 155.52 to 2488.32 Mbps	-

Benefits and Applications

MON will be offered as a customized solution on an individual case basis to customers who have requirements for mainframe-to-mainframe connectivity and/or data center connectivity applications for disaster recovery, data center mirroring or Storage Area Networks. It is suited well for financial, educational and healthcare markets whose focus today may be a LAN-only perspective to an end-to-end solution that integrates LAN, MAN and WAN networks with eventual introduction of 10 Gbps Ethernet networks.

In 2002 SBC will develop beyond the point-to-point MON service to a ring architecture. This will provide an excellent transport solution for use with a variety of IP services, including integrated voice and data services, SONET, Transparent LAN or Gigabit Ethernet.

You may ask why would a customer use the MON service offering when they today have SONET service? The reason is that existing SONET services are limited in bandwidth and require customers to convert their data connections from their native protocol (e.g. ESCON) to the SONET protocol. This conversion is costly, results in significant overhead and limits the available bandwidth. MON, using DWMN technology, enables customers to keep data transport in their native format and can easily grow from 1.25 Gbps to 80 Gbps (protected) and 160 Gbps (unprotected) of bandwidth, depending on the services installed, without the need for additional fiber placements (4 fibers are required for 32 protected wavelengths).



Example of MON service offering

A recently implemented MON application demonstrates the value of this new service. An SBC customer had outgrown their existing 11-node OC48 ring after just 18 months and an OC192 solution was researched, but considered too expensive. With DWDM, the customer was able to connect their two data centers together with two OC12 point to point circuits, and eventually expects to add ESCON and FICON channels. The OPTera solution allows this customer to shift their point to point data center traffic to the DWDM service and free up capacity on their existing OC48 ring; giving them spare capacity to grow their OC48. This option allows the customer more control and better utilization of their network.

Conclusion

DWDM, which has been used primarily in long distance links, is now seeing new applications for customers as the price of equipment comes down and the customers need for bandwidth increases. Customers are now able to take full advantage of high-bandwidth services without expensive protocol conversion. MON offers integrated voice and data services and will support existing legacy systems and protocols while meeting the need for economical network growth. Bandwidth consumption will grow exponentially over the next several years and high-end customers now may turn to SBC's MON service for their future needs.

– **Tom David**
Consultant Liaison Manager
(949) 855-5055
e-mail: tfdavid@pacbell.com

"No act of kindness, no matter how small, is ever wasted."

HANDLING THE 20 MOST CRITICAL THREATS

(continued)

their password when required and then immediately change them back. Requiring minimum ages on passwords make users remember the passwords and makes them less likely to change them back. Another important supplement is user awareness training that helps users understand why and how to pick strong passwords. The most common advice given for picking better passwords is to pick a phrase or line from a song that includes a number, and construct the password from the first or second letter of each non-numeric word in the phrase, and the numeral for any numbers. Adding punctuation makes the password even more difficult to crack.

Another way to protect against no passwords or weak passwords is to use an alternative form of authentication such as password-generating tokens or biometrics. If you are having trouble with weak passwords, use an alternative means of authenticating users.

To read about the 18 other most critical Internet Security Threats, please go to the SANS (System Administration, Networking & Security) Institute website: ***www.sans.org/top20.htm***

Paul Bedell
Product Manager, Business Marketing - Optical Data Networks

PAUL'S PERSPECTIVE

THE METRO ETHERNET SPACE

The Metropolitan Area Network (MAN) is the portion of the public telecommunications network (PSTN) that lies between the local access network, which directly touches consumers, small-medium businesses and large corporations – and the cross-country backbone network. In figurative terms, the MAN connects the edge of the telecom infrastructure network to its core.

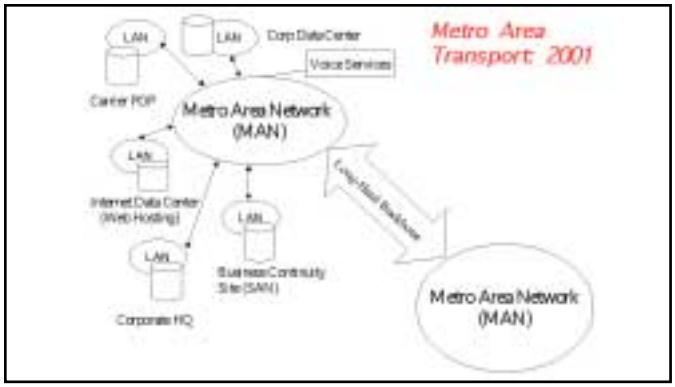
An evolution is taking place in the carrier marketplace today. A capacity squeeze is being placed on MANs. This squeeze is caused by a combination of two things:

1. The backbone of the long-haul networks that inter-connect our cities have historically had plenty of capacity. In this context, the reference is to the "Big Three" of AT&T, WorldCom and Sprint. Add upstart carriers to the mix (i.e. Level 3, Broadwing, Qwest, Global Crossing) and the availability of long-haul bandwidth in the form of "big pipes" is now more than plentiful. Many sectors of the industry contend there's actually a fiber glut in the long-haul networks. As a matter of fact, the capacity in these networks could be increased exponentially if DWDM technology were deployed in the core of these networks. Many of the long-haul carriers have already deployed DWDM in their major routes. (It's easy to economically justify implementation of DWDM in these networks: it's always going to be cheaper to install equipment in the core of these networks versus pulling additional fiber through hundreds or even thousands of route miles).

2. Availability of inexpensive broadband Internet access in the form of DSL and cable modems is allowing consumers and businesses alike to increase the size of the pipes used to go on-line by 15 to 20 times, depending on the technology and the area in question.

So how do the consumers and businesses move from their local Internet access to the long-haul backbones? Through metropolitan area networks (MANs). MANs serve as the bridge between local Internet access and connectivity to far-flung Web servers. Between you and your cousin in a faraway city, whom you call twice a month.

In summary, the squeeze that's being put on MANs today is a result of plentiful capacity in long-haul backbones and a burgeoning, ever-increasing amount of data being pumped into the MAN due to Internet-related traffic and the growth in various types of corporate traffic.



The choke point in today's PSTN is the MAN, and many in the telecom industry see Ethernet as the Heimlich maneuver.

Drivers

Most all corporate data communication transmissions begin and end using the ethernet protocol. Ethernet is a simple, well-understood technology. It exists on over 90% of corporate desktops across the entire United States. It therefore makes sense to attempt to use this technology, if feasible, as the end-to-end transport vehicle for corporate communications.

Ethernet is now making its play in the metro space. There are predictions that Ethernet will make its play in the WAN marketplace within three years. Deployment of Ethernet technology as the sole means of end-to-end transport also makes tremendous sense in terms of economies of scale. In a network topology that consists of only ethernet, there would be no requirement for encapsulation of ethernet frames into other WAN transport technologies such as frame relay or ATM. This would have the effect of flattening the network architecture, which has multiple benefits:

1. Decreased capital equipment costs (i.e. frame relay or ATM switches)
2. Presumably, an end-to-end ethernet network could also handle voice communication needs were VoIP deployed. Theoretically, the legacy voice infrastructure could be significantly scaled back and possibly eliminated eventually.
3. Decreased network management requirements. Less boxes in the network topology equals less boxes to manage. Less interfaces to monitor, less boxes to troubleshoot during outages. This could also translate into reduced headcount requirements.

The benefits of ethernet mentioned above require a few stipulations to be spelled out. First, it's assumed that internet protocol (IP) connectivity is achieved by having IP packets encapsulated within Ethernet frames. Second, it is presumed that the oft-overhyped notion of "convergence" of multiple traffic types can be easily and economically implemented in the scenario depicted above, with at least minimum QOS capabilities and enforcement end-to-end.

In addition to the practical benefits listed above, industry studies and forecasts issued within the last year also underscore the fact that metro area Ethernet is poised to have its "inflection year" in 2002:

underscore the fact that metro area ethernet is poised to have its "inflection year" in 2002:

- Aggregate voice, data and Internet traffic demand in metro areas is projected to grow from a $1.5 billion business in 2000 to a $50 billion business in 2005.
- The overall amount of metro circuits (ports) is growing at approximately 65%, fueled by growth of data centers and carrier hotels.
- Next generation SONET technologies (SONET-lite; Metro DWDM and Gigabit Ethernet) are 30%-70% more cost efficient than legacy networks (i.e. TDM, ATM).
- The top 15 metropolitan areas in the United States account for 80% of total demand and with a select few customers (i.e. ISPs, Fortune 100 companies) generating the majority of traffic flow.
- A cumulative annual growth rate (CAGR) for the metro area network marketplace is projected to be approximately 36% through 2006. Multiple industry analysts substantiate this estimate.
- In 2000, the total demand for metro bandwidth was satisfied by the equivalent of approximately 8000 OC-48 circuits. To put this into perspective, that's the equivalent of 258 million DS-0 circuits. By 2005, metro traffic likely will require more than 100,000 OC-48 equivalents, with service providers, data centers and enterprises driving the majority of the growth. Using the DS-0 perspective, that's the equivalent of 3.2 billion DS-0 circuits. That represents an increase of over 1200% in a 5-year period. Large enterprises currently generate half of metro traffic. With the rapid growth of Internet-based applications and host-to-host traffic carried on private networks, many enterprises have seen their requirements for data capacity grow rapidly. Growing at a healthy 40% per year, these enterprises alone will require more than 20,000 OC-48 equivalents in 2005. In recent years, corporate data centers, Web hosting sites, application service providers (ASPs), firms specializing in storage networking and business continuity, and other "edge" players have generated explosive growth of high-bandwidth, layer two data traffic (i.e. Ethernet). These segments alone have a 65% (CAGR) !!
- In particular, data center traffic is growing at nearly a 100% annually, and will consume 40% of total metro bandwidth by 2005. These data centers happen to be concentrated in the top 15 Tier One metros, the same metro areas that account for 80% of traffic demand. In fact, the top four markets constitute approximately 40% of all MAN traffic.

Residential customers and small-medium size businesses generate 6% of total demand today, and even though this segment is growing at 60%-70% per year, should still continue to only generate 6% of demand in 2005.

The Players

Players in the metro Ethernet space are pursuing one of two distinct business models:

1. Transport businesses that serve data centers and carriers.
2. Access businesses looking to serve enterprises.

The shift to Ethernet that's taking place has spawned a whole new breed of carriers in the metro marketplace. Some of these carriers are known as BLECs (building LECs) because they target their efforts at multi-tenant units (MTUs), in the hopes of signing up most or all of the tenants in the building so it's cost-effective to pull fiber to the demarc of targeted buildings. An example of a BLEC is Cogent Communications. Some of these carriers are known as OLECs, which stands for Optical LEC. They earned this moniker since a bulk of their business is wholesaling dark fiber to all the other new metro ethernet carriers. An example of an OLEC is Metromedia Fiber Networks (MFN). MFN also offers some retail ethernet services. Some metro upstarts are known as ELECs, which stands for Ethernet LEC. These are carriers who sell retail Ethernet (IP) services only.

The most aggressive and successful of the ELECs to date is a well-funded San Francisco-based company named Yipes Communications. Yipes mainly targets the large business segment. Telseon is another successful ELEC, but they mainly target the data center and SAN markets. There are other non-traditional players staking their ground in the Metro Ethernet marketplace. Carriers such as Time Warner Metro (cable TV company) have had success selling major Ethernet-based networks to school districts. AT&T (Local) and BellSouth have also recently announced major Metro Ethernet product offerings. SBC has offered GigaMAN service in the Ameritech region since July, 1999. They launched GigaMAN in the Pacific Bell and Southwestern Bell regions in the first quarter 2001.

Metro transport will be intensely competitive (highly scale-dependent and high concentration of customers) with survivors other than the incumbent LEC to include one or two net entrants, or IXCs that "forward-integrate" into their legacy networks. New metro access technologies, namely Gigabit Ethernet, promise significant upside for established players such as ILECs, well-positioned CLECs and potentially IXCs. The stakes are high in this space, which is why this sector is getting so much attention these days. The well-positioned upstarts (i.e. Yipes) are where they're at due to good execution, sound business plans and substantial funding. Many major equipment manufacturers are trying to stay ahead of the curve by offering Ethernet-Over-SONET interfaces into their SONET muxes to maintain their status with their ILEC customers. There are also many upstart equipment manufacturers that are partnering with the major ELECs and BLECs. Firms such as Extreme Networks, Riverstone Networks, Foundry Networks and LuxN are hinging much of their success on the success of the upstart carriers themselves.

A Lehman Brothers/McKinsey and Company Study released in August, 2001 states that the Ethernet protocol, notable Fast Ethernet and Gigabit Ethernet (GigE) should become the principle access protocol for enterprises in the next fiber years. Their studies suggest that Ethernet should account for 60% of total bandwidth, due to its low cost structure and familiarity in IT enterprise networks. The evolution of the metro access and transport landscape will prove challenging for new entrants hoping to exploit GigE technologies. It is said

PAUL'S PERSPECTIVE (CONTINUED)

that success will be predicated on flawless execution, high building penetration and the realization of reduced peering costs, and the degree of which they can overcome ILEC efforts in this market.

ILECs have the upper hand in this space but need to maintain dynamism in their approaches to Ethernet services. They need to either be first to market or react to competitor moves quickly in order to maintain the upper hand. The biggest inhibitor to the growth of this market – for all players – is lack of fiber. But again, this is one area where the incumbents definitely have the upper hand. In the outlying portion of many metro areas, where many businesses have set up shop since the late 1980s, there is still limited fiber deployed where many of these businesses have their offices. For most all installations of metro ethernet that aren't within the most concentrated part of urban areas, there is still a good possibility that some type of fiber construction will be required. But even in this scenario, the ILEC is much better positioned than all of its competitors simply due to the size of its legacy geographic footprint.

Some industry analysts predict that Ethernet will eventually make a play into the consumer and small business marketplace as a new means to offer Internet access. The boom in home computing lends some credibility to this prediction. Anyone who picks up and reads a Best Buy or Circuit City flyer these days will notice that almost all the computer systems that are advertised come with an Ethernet network interface card (NIC) as a standard part of the package. Will Metro Area Ethernet become the next DSL? Wait and see.

SBC's Paul Bedell also teaches at DePaul University. His latest book, **Wireless Crash Course,** *is published by McGraw-Hill. He can be reached at paul.a.bedell@msg.ameritech.com The opinions expressed in this and other columns in* **Update** *are the authors and not necessarily those of Pacific Bell or SBC.*

GigaMAN Update

The GigaMAN product that was launched in Pacific Bell territory has met and exceeded sales expectations year-to-date, 2001. The service is being purchased by medium, large and "global" businesses. Many major companies have bought GigaMAN circuits to link their metro locations together with this economical, high-speed LAN extension service. A mid-span repeater option is being evaluated for possible launch in mid-year, 2002. This option would effectively increase the end-to-end distance capability of GigaMAN circuits around 60%. With 2002 predicted to be the "inflection point" for metro ethernet services, sales success of GigaMAN should continue vigorously this year. More to come……

– Paul Bedell

WEB WATCH

By Paul Bedell

Here's a useful web site for you: **www.lightreading.com.** It bills itself as " The Global Site For Optical Networking". This site offers a wide array of information related to optical networking. If you want to know what's going on in the "optical industry" – which means learning more about the equipment and service providers – this is the place to go.

The main page has a "Newswire" section, which contains articles about industry developments. White papers are also available on a multitude of optical network topics and technologies. The white papers cover such topics as passive optical networking ("PON"); optical ethernet; metropolitan area optical networks and packet ring technology (i.e. Resilient Packet Ring, or "RPR"). The only caveat about the white papers is that they're vendor-sponsored, so the reader needs to remember that when reading through the material.

There's also a "Research" tab on the main page, which takes the surfer to a page that offers tutorials for the "beginner"; and tutorials on other optical network-related topics and technology. There's info on upcoming events such as conferences and seminars too. The Research tab even has a "chat" option, and a section where readers can vote on various polls the site takes.

There's an entire tab dedicated to "Storage", which is actually a hyperlink to a site called "byteandswitch.com. That site bills itself as "The Storage Networking Site". It's essentially the equivalent of lightreading.com, but for the SAN industry.

At the right of the main page, there's also an option for the reader to register for free "Webinars". Webinars are free, sponsored educational seminars that are accessed over the Internet through lightreading.com. You can register for upcoming Webinars or view archived presentations via links at this section of the site. On the main page, there's also a link to a glossary of optical terms.

This excellent site also has regular columns on optical topics, interviews with industry executives and a section that discusses stock-related perspectives. Readers can even make suggestions for story ideas.

If you're looking to get up to speed on optical networking, this is the site for you. It's not really "light" reading, but it will surely enlighten you.

"Once the game is over, the king and pawn go back in the same box."

Cassandra Jessie-Johnson,
Data Solutions, Pacific Bell

DSL DATA -JOURNEY 2002

2001 was a year of significant growth and monumental changes in DSL for SBC. The first quarter began with price restructuring for DSL Internet service and a partnership with computer manufacturer Compaq to discount PCs for customers ordering DSL Internet. Relationships with global leaders like Cayman, Efficient and Alcatel continued throughout the year to provide quality broadband gateway solutions to your customers. April brought price restructuring for DSL Transport to Internet Service Providers and RLAN customers. In June, a new product, Office Gateway/Home Networking was introduced to allow customers to create LANs without having to add additional wiring.

In July, the Get Up To Speed campaign was launched to re-introduce DSL Internet & re-educate SBC employees to synergize around marketing the product. The campaign proved quite successful, as SBC saw more than 14K employee referrals during the "slow" summer season. Due to customer popularity (demand and acceptance), SBC also saw an increase in Customer Self-Installs (CSI), prompting several enhancements to the solution. Broadjump software CD was deployed. The software was consolidated for an integrated/seamless DSL installation and provided end-to-end "self-help" information, which addressed and answered nearly 200 possible errors for clients. Some of the features included PC minimum requirements checklists, an Ethernet NIC test, automated software installation, PPPoE client installation and connection, and more. A new integrated CSI kit rolled out in August. This kit included a modem, NIC, 2 CDs (SBC Express CD & PPPoE drivers) and a new welcome letter which disclosed a "one-stop shopping" service/support number. CSI enhancements continued through out the summer, resulting in newer modems and NICs becoming available. SBC began to offer internal and external modems. The CSI option became available with the RLAN application to allow corporations the option of installing the DSL CPE themselves, bringing additional cost savings to your customers.

An alliance with McAfee.com was formed to provide more security and added defense for DSL Internet subscribers at discounted rates. The third quarter brought the filing of a new FCC tariff for 5 ASI products – ATM, Frame Relay, NAP, DSL Transport and RLAN. The change order process for customers served from remote terminals was tested and successfully implemented, allowing customers to change speeds without experiencing any loss of service. As of November 1, the Business DSL Internet product was grandfathered. Existing Business DSL Internet customers will continue to have the service and the product will be supported. Additional static IPs were available for ordering with the Enhanced DSL Internet Service effective November 11. The standard Enhanced product comes with 8 IPs (5 usable). Additional IP's can be ordered in groups totaling 16, 32, 64 and 128. Previous IP addresses cannot be guaranteed so routers and LANs may need to be re-programmed. There is a one time set-up charge and very minimal downtime associated with increasing the IPs. Year's end brought the purchase of Prodigy. There were 1333 DSL-ready central offices within SBC at last count in November.

With well over 1.2 million DSL lines in service, SBC is looking forward to the difference 2002 will make in continued rapid deployment of DSL technology, offering advanced broadband services affordable prices. Plans for first quarter include the release of Prodigy 7.0, a new client kit software. Visit this link to tour the new console: **http://myhome.prodigy.net/pserv/tour/.** The new Prodigy 7.0 console replaces web clutter with a sleek design, created with your customers in mind. Everything they want — e-mail, contacts, calendars, instant messaging and media player — it's all in one place. With one click on the Task Bar, customers can access it all, from anywhere with an Internet connection.

Permanent bundled solutions are on the horizon for this quarter, solutions that will combine access lines, usage, custom calling features and DSL Internet service. Advancements will also introduce Centrex/Plexar DSL, which will provide customers with a high-speed data connection to the Internet or to their host server at their main office location. Centrex/Plexar DSL is the provisioning of DSL data over the same pair of wires that provides the analog circuit switched voice capabilities of Centrex/Plexar. The competitive alternative today is Centrex/Plexar ISDN. Centrex/Plexar DSL will provide another quality, high-speed Internet access option to your customers.

For your clients concerned about total protection, SBC will continue partnerships with McAfee.com for added protections against viruses and hackers. SBC will also introduce a DSL protection service for your customers, a convenient way to protect their investment in DSL technology. There will be two plans: one for clients with modems and one for clients with routers. Both plans will be subscription services that provide customers with CPE trouble isolation, repair/replacement of modems/routers, NIC cards, and filters associated with their DSL service (data and/or future derived voice). The monthly subscription rate is intended to cover all labor & material required to perform the repair/replacement of CPE. Minor PC or Mac troubleshooting as it relates to resolving DSL issues would also be covered. A customer wishing to subscribe to DSL Protection should consider becoming a Telco Wire-Plan Service subscriber. This package of Wire-Plan and DSL protection would provide DSL subscribers with "peace of mind", and protection from unexpected Inside Wire repair bills or CPE replacement charges. In other words, a DSL subscriber with Wire-Protection Plus and DSL Protection will have complete coverage including all wiring, jacks, telephones and DSL equipment from the network interface up to their PC.

DSL will continue to be one of the main drivers for growth and SBC expects the broadband market to continue to grow exponentially. With the addition of Prodigy, SBC has over 3.3 million Internet subscribers and is the leading DSL-based Internet Service Provider in the nation. SBC's goal is to create a robust, "data-centric" network architecture capable of delivering the most advanced broadband technologies, which, of course, includes DSL Internet service. For more information, to qualify your customers for DSL Internet Service, as well as to order DSL service for your clients, contact the Emerging Products Center Consultant Queue at **1-866-234-4DSL (4375)**.

Cassandra Jessie-Johnson is Associate Director of Data Solutions at Pacific Bell.

INSIDE CINGULAR

CINGULAR WIRELESS MEANS BUSINESS!

By Wayne Harvey
Regional Director, Global Accounts - So Cal

A Successful Tradition in the Consumer Market

As the second largest wireless carrier in the U.S., with over 21 million subscribers, Cingular's individual wireless properties have enjoyed a successful history of focusing on the consumer market. Now as a unified company, with a combination of company owned, and agent licensed retail stores across the country, Cingular is even better positioned to continue it;s successful track record in the general consumer market.

Because of the traditional regional consumer focus, and lack of a nationwide marketing and support structure to meet the needs of larger corporate customers, the individual wireless properties have had limited success in the past in the enterprise arena. Although a couple areas can boast of established bases of strong, loyal business customers, most regions, including the previously known *Pacific Bell Wireless* area, have not had the tools and resource to offer the Fortune 1000 customers competitive value… up until **now**!

Focusing on the Enterprise Customer

Now, with a nationwide culmination of wireless properties from SBC and Bell South, Cingular Wireless is on the momentous course to **redefine the way in which it approaches, and does business with, the enterprise customer**. Cingular in its first year as a nationwide wireless solutions provider, has embarked on an aggressive path towards redefining its role in the B2B marketplace. Many of the executives laying the groundwork for this market focus come from the SBC or Bell South landline business segments, and know what it takes to effectively service and support the requirements of larger corporate customers.

Business Market Segmentation

Similar market segmentation to SBC in the business marketplace provided the initial formation of **Cingular Wireless Global Accounts**, a separate and distinct organization apart from the local direct and indirect sales forces. This group is a nationwide sales and support organization with accounts mapped directly from the SBC Globals and Health Care Market Group landline accounts. Consisting primarily of Fortune 500 accounts, the Federal Government, and a few select large regional concerns, Cingular Wireless Global Accounts provides a specific and focused approach to business slake and support. An Account Representative provides a single point of contact at the customer's headquarters location, and works with associates in other regions specifically designed to support the customer's remote locations. Additionally, each Global Account Customer has access to their own unique Extranet site called Global On-Line Distribution (GOLD) for placing orders, securing authorization, tracking delivery, and generating management reports.

In January, 2002, a continued market segmentation in the business marketplace will result with the delineation of Globals, Majors, Corporate and SoHo markets, and the implementation of Siebel Sales Force Automation software to effectively manage "modules" of business customers, depending on the size, number of employees, and geographic scope. These segmentation is similar to the SBC/Pacific Bell landline market segments of Globals, Priority, Signature and Valued business accounts. Additionally, we in the Cingluar Wireless business segments will be joined by our counterparts at Cingular Interactive to focus on voice and data applications that enable the mobile workforce within large enterprise customers.

Business Applications

Voice, of course, is the "killer" application that has grown mobile services users from 600,000 in 1987 to over 100 million in 2001. Cahners In-Stat Group says "there are about 600 million users worldwide, which could grow to 1 billion over the next year". Although this growth has been, and will undoubtedly still be from primarily consumer based "voice" users, over the **next double years we will see a tremendous focus on the business customer applications** as enterprises move rapidly to deploy cost saving, and productivity boosting solutions for their unique mobility needs. A majority of these applications will be "data" driven, and all wireless carriers, including Cingular Wireless realize that mobile devices have to be more than just making phone calls.

Cingular Wireless currently provides data delivery services on both the traditional voice handset (WAP, SMS…Text Messaging), and RIM Blackberry "always-on" data only devices, to a multitude of business customers. Whether it is simple e-mail, scheduling, tracking inventories, dispatching, processing work orders, or monitoring remote devices from the field, early adopters have realized the productivity gains associated with wireless communications for their remote work forces. Power utilities, freight forwarders, field service technicians and sales forces all have evolved from simply voice handsets and pagers, to more sophisticated PDA's and laptop devices for their communication needs.

Positioned for Success in the Business Marketplace

Cingular Wireless, in combination with it's Cingular Interactive entity, is uniquely positioned to provide valuable solutions to the business customer who will be faced with a multitude of choices as wireless technology evolves and hardware selection becomes more complex. Large enterprise customers may need several different devices, depending on the number and complexity of the applications. Most likely, a single application may require a multitude of devices for various types of users. With strategic partnerships with all the major hardware manufacturers, such as Nokia, Ericsson, Motorola, Siemens and Research in Motion (RIM), joint developments are under way to provide devices and applications software for the business customer.

With the availability of multiple developers and partners, Cingular Wireless is positioning itself for "device

agnostic" delivery of those applications to our business customers, and will strive to deliver value to our customers regardless of device and/or network. When making a solution decision, it shouldn't be based on the network, middleware, device or price, since these are constantly changing in the wireless industry. It should be based on the job function requirement, and **which wireless provider is best positioned to deliver a solution for that specific application…now and in the future.** Cingular Wireless is committed to evolving with the business customer, providing the resources to develop and support mobile business applications, and upgrading the network to accommodate the growing need for higher bandwidth delivery.

High Speed Data for Enterprise Customers

On October 30, 2001 Cingular Wireless announced it will begin upgrading its network to third generation (3G) wireless data technology. With the introduction of EDGE (Enhanced Data Rates for Global Evolution). Cingular will bring faster speeds to customers nationwide. The upgrade to EDGE will put in place wireless always-on packet data technology capable of transmitting data up to peak rates of 384kbs - fast enough to support full-motion video.

"Cingular - already the national leader in packet data – is going a step further to transition our network to a worldwide3G standards," said Stephen Carter, president and CEO of Cingular. "At the same time, we will be providing our customers with a single voice technology from coast-to-coast."

The move to EDGE will begin with the installation of GPRS (General Packet Radio Service) packet data and GSM (Global System for Mobile Telecommunications) voice technology over Cingular's TDMA and analog networks. GSM is the world's leading digital wireless technology. More than half a billion GSM phones are in use worldwide, accounting for more than 70 percent of the world's digital wireless market. Cingular already uses GSM technology in California, Washington, Nevada, South Carolina, North Carolina, Eastern Tennessee and Coastal Georgia. The GSM technology also allows customers with tri-band or "world" phones to use their phones seamlessly in more than 160 countries.

"GSM is clearly the world's choice for wireless technology," said Carter. "Plus, having a common technology throughout the United States will allow us to provide additional capabilities and features for our customers."

EDGE will be installed in all markets throughout Cingular's coverage area. GPRS is already marketed in Seattle, Los Vegas, Eastern Tennessee, North Carolina and South Calolina as Cingular Wireless Internet Express. The EDGE network will also be "backward compatible" meaning customers with GPRS devices and also use them in EDGE Markets.

Cingular's decision to pursue EDGE as its third generation technology path is made possible by a number of factors and commitments including:

- Increased spectrum efficiency achieved through the GSM technology.
- Availability of GSM network infrastructure that operates on 850 MHz and 1900 MHz spectrum.
- Development of GAIT wireless phones, which will allow Cingular customers to seamlessly move between its TDMA to GSM networks.
- Commitments from network infrastructure and terminal vendors to supply cingular with EDGE infrastructure and devices.

Cingular's large business focus in California is headed by the following contacts:

Shannon Carr, Regional Vice President, Global Accounts - West Region
(714) 734-3239 - shannon.carr@ cingular.com
Wayne Harvey, Regional Director, Global Accounts - So Cal (714) 734-3244 - wayne.harvey@cingular.com
Dale Bouguennec, Regional Director, Global Accounts - No Cal (925) 227-4773 - dale.bouguennec@cingular.com

CRITICAL INFRASTRUCTURE: TELECOMMUNICATIONS

Introduction

The FBI's National Infrastructure Protection Center (NIPC) states its mission is "to serve as the US Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures." NIPC lists the 8 critical infrastructures that the government considers essential to the life of this country. Telecommunications is at the top of the list. Although the list is not ranked by importance, all the other infrastructures do rely on telecommunications.

Critical Infrastructures

Critical infrastructures are the capabilities in our society that enable us to do all the other things we do in our lives. We need our society's infrastructures to deliver food to our children, to get medical care when we need it, to be informed of events in the world around us. We need them to produce and deliver all the goods and services we produce.

The 8 Critical Infrastructures

- Telecommunications
- Banking and Finance
- Water Supply Systems
- Transportation
- Emergency Services
- Government Operations
- Electrical Power
- Gas and Oil Storage and Delivery

There certainly are other infrastructures that are important. Entertainment and tourism, for example, play huge roles in our economy and in our society but they are not as important.

NIPC Description of Telecommunications

Under the Telecommunications NIPC states the following: *"A critical infrastructure characterized by computing and telecommunications equipment, software, processes,* ***and people that support:*** *(My emphasis)*

(continued on page 20)

Critical Infrastructure: Telecommunications (CONTINUED)

- *"The processing, storage, and transmission of data and information*
- *"The processes and people that convert data into information and information into knowledge*
- *"The data and information themselves."*

Our Role

The government can tell us how important we are as an industry, but there's only so much it can do to protect us. We have to do most of the work ourselves. We're great at delivering communications to our customers and at making communications work for us as a company. In light of our place in the country's critical infrastructure, our ability to do this securely is an important part of our national well-being and our corporate responsibility. For SBC, protecting the telecommunications infrastructure means protecting both our physical assets such as our switches and networks, and our intangible assets such as SBC's Proprietary Information. We need to see the security implications in our daily jobs and act on that awareness. We have to make appropriate security a component in everything we do, in every service we deliver.

Security Consulting

CIS Security Consultants consult with and assist in new information projects. They review project plans for security information and use SBC's security standards to make the projects more secure.

InfraGard

SBC participates in the InfraGard initiative. From the InfraGard website: *"InfraGard is a Partnership between Private Industry and the U.S. government (represented by the FBI). The InfraGard initiative was developed to encourage the exchange of information by the government and the private sector members."*

As you might imagine, one of the concerns within Infragard is protect member companies who share information from being harmed by disclosure of that information.

Conclusion

We have to and do take seriously the importance of our place in society. That's why SBC Consulting Services offer Security Policy Development and Penetration Testing. Please contact your Liaison Manager for further information. Thank You.

– **Jerry Hinek, CISSP**
Senior Business Security Manager
Corporate Information Security
SBC Services

MARK YOUR CALENDAR

Live SBC/Pacific Bell Broadcast Feb. 13

You're invited to hear the latest SBC/Pacific Bell News from 9-11:30am PST. Call your Liaison Manager for further details or you can be a streamer. More info will be posted on 888-889-6010.

PACIFIC BELL CONSULTANT/VENDOR SALES GROUP

Toll-Free Hotline 1-(800) 552-5299
(For any other number, toll charges may apply.)

Vendor/Consultant Service Center – **1-800-773-3318**

Kari Watanabe	CVSG Vice President (415) 542-4516 e-mail: kmwatan@pacbell.com
Tom David	Liaison Manager (949) 855-5055 Fax: (949) 348-2941 e-mail: tfdavid@pacbell.com 27402 Camino Capistrano Room 211, Laguna Niguel 92677 Helps Consultants and Vendors in the following area codes: 619, 714, 760, 858, 909, 949
Bree Ma	Liaison Manager (415) 542-1071 Fax: (415) 542-2648 e-mail: bcma@pacbell.com 370 Third Street, Room 711 San Francisco 94107 Helps Consultants and Vendors in the following area codes: 209, 408, 415, 510, 530, 559, 650,707, 831, 916, 925
Craig MacDonald	Editor/Communications/Seminars/Conferences (714) 284-2370 Fax: (714) 563-1736 e-mail: ccmacdo@pacbell.com 200 Center Street Promenade, Room 100 Anaheim 92805
Lowayne Shieh	Liaison Manager (626) 576-3045 Fax (626) 576-5081 e-mail: leshieh@pacbell.com 500 E. Main Street, Room 540 Alhambra 91801 Helps Consultants and Vendors in the following area codes: 213, 310, 323, 562, 626, 661, 805, 818
Eric Aguirre	Data Administrator
Sibyl Clark	Graphic Designer, Sacramento Graphic Arts

UPDATE HAS GONE TO NEW HEIGHTS

One of our readers climbed to the top of Mt. Whitney (14,496 feet) – the highest mountain in the continental United States – and discovered this fellow reading ***Update***. This chap is one of more than 30,000 regular ***Update*** readers. If you find ***Update*** being read in unusual places, please send the editor a photo.

Thank you for reading ***Update***.