AT&T Consultant/Vendor Sales Group
UPDATE
Summer 2007

inside...

kari's corner

It is amazing to think that the year is two thirds over! Graduations, weddings, vacations – 'tis the season! I hope you're enjoying some well-deserved recreation this summer. You are some of the hardest working people in the business, and your contribution to AT&T continues to be a driving force in our success.

Analysts at Yankee Group Research predict this year more than 42 percent of the American workforce will be "mobile," which means they spend more than 20 percent of the business workday away from their primary workspace. Check out Data with David in this issue to review some of the great Ethernet solutions from AT&T to expand your customer's reach. Then see if you agree with Nancy Grover's conclusions in the Mac versus PC debate (Get a Mac?).

We're also very pleased to introduce a new writer in this issue. Mark Steinberg has been with Hill Associates since 1994. He is a Certified Information Systems Security Professional, and holds an MBA in International Finance from the University of Santa Clara, California, a BA in Pre-med/Biology from Hartwick College in Oneonta, New York, and has done graduate work in Astronomical Physics at the University of Colorado. Mark has spent more than 25 years in the business of technology, providing consultative services regarding the strategic implications of technological change. His knowledge of convergence, both voice/data and wireline/wireless, has allowed him to create a variety of programs that address these business strategies. His focus in this issue is on Business Continuity, and we look forward to contributions from him in future issues of Update.

If you haven't already taken a moment to register, be sure to visit www.thefocus.org and sign up for membership. You'll receive information on regularly scheduled FOCUS events including local FOCUS Chapter meetings, Special Interest Group Meetings, and the National Conference. Take advantage of this opportunity to network with peers, and hear how AT&T is approaching network convergence and next-generation capabilities.

Now, as we begin the home stretch of the year, we have more opportunities to strengthen relationships, more opportunities to sell, and more opportunities to provide cutting-edge solutions tailored to customers' exact needs, now and as they evolve. Enjoy the rest of your summer – and get ready for a busy Fall!

Kari Aguinaldo
CVSG Leader
415-644-7118
kw6875@att.com

in this issue...

UPDATE Editor
Elaine Tipping
elaine.tipping@att.com

Contributors
Kari Aguinaldo
John Cushman
Tom David
Nancy Grover
Jerry Hinek
Mark Steinberg

Layout & Design
Lillian Cram
AT&T MultiMedia Productions

Publisher
AT&T West
Business Communications Services
Sales Operations

AT&T Customer Service Numbers

Pre-Merger SBC Areas:

California	Sales & Billing	Repair
Small Business	1-800-750-2355	611 or Toll-free 1-800-750-2355
Medium Business	1-800-891-1800	611 or Toll-free 1-800-332-1321

Nevada	Sales & Billing	Repair
Business/Consumer	1-800-288-2020	1-877-469-2355

Southwest	Business
Sales	1-800-499-7928
Billing	1-800-559-7928
Repair	1-800-286-8313

Midwest	Small Business Sales & Billing	Small Business Repair
Indiana	1-800-660-3000	1-800-727-2273
Wisconsin	1-800-660-3000	1-800-727-2273
Illinois	1-800-660-3000	1-800-727-2273
Ohio	1-800-660-3000	1-800-727-2273
Michigan	1-800-660-3000	1-800-727-2273
Español		1-800-426-2902

East (CT)	Sales & Billing	Repair
Business	1-800-448-1008	1-800-922-4646

Pre-Merger AT&T Mass Market Areas:

Local and Long Distance Service: 1-800-222-0300

AT&T CallVantage Service: 1-866-596-8464

AT&T Worldnet and DSL Service: 1-800-WORLDNET (1-800-967-5363)

AT&T Alascom (Alaska):

Business Services: 1-800-955-9556

mark steinberg

What About the Business?

Business continuance has been in the news a lot recently. Whether it is due to the catastrophic events of September 11, 2001, the devastating consequences of Hurricanes Katrina, Rita, and Wilma in 2006, or the seemingly endless news stories of tapes gone missing, identity theft, and phishing incidents, there appear to be daily posts on the subject. To add fuel to the fire, the National Oceanic and Atmospheric Administration (NOAA) recently predicted this year to be a stronger than average hurricane season. There are a lot of statistics that now back up the feeling of uncertainty related to the topic of business continuity.

According to the most recent Global State of Information Security Report, published annually by *CIO Magazine* (http://www.cio.com/article/24979/The_Global_State_of_Information_Security_), the desire to back up data was to be the number one action item for 2007, up from number three in 2006. In the same report, business continuance went from number one to number four.

What are the reasons for these numbers? According to many sources, including one published by AT&T (http://www.att.com/gen/press-room?pid=7922), nearly one-third of all businesses in the United States do not have a business continuity plan, and of those that do, nearly three-fourths do not test it! It is estimated that almost half (40 percent) of businesses do not have redundant servers or backup locations for critical business functions. This is especially true for small and medium-size business (SMB), and it is estimated that there are 25 million SMBs in the U.S. (20 million with less than 100 employees according to the Small Business Administration, (www.sba.gov). According to Gartner, of those, only 20 percent of those protect remote office data, and 60 percent of storage professionals are unhappy with their remote office backup options.

These are pretty frightening statistics, given that according to a recent article in Storage Magazine, 30-35 percent of corporate data is in remote offices, and it is growing by an estimated 50 percent each year. In fact, a report in March by EMC (http://www.emc.com/about/destination/digital_universe/) stated that in 2006, there were estimated to be 161 exabytes of digital content in the world. (That's about three million times the information contained in all the books written to date.) That number is expected to grow six-fold by the year 2010 to 988 exabytes! That's a lot of content.

What is driving all this growth? According to the EMC report, 70 percent of it comes from digital cameras and cell phones, along with medical and other digital imaging sources. Let's also not forget that email boxes grew from 253 million in 1998 to 1.6 billion in 2006. And then there's the astronomical growth of personal content from websites like MySpace, FaceBook, and YouTube.

But it is not just individual demands driving growth. We are also seeing more use by commercial applications, such as in London's city center where 200 traffic surveillance cameras send 64 trillion bits of information every day to a command center.

So, what can we do about protecting all this content? Actually, several things, but let's start with some basic questions.

- Do you have a security program in place?
- Is there a security policy driving requirements?
- Is it tied to business requirements?

Continued on page 4

Nearly one-third of all businesses in the United States do not have a business continuity plan, and of those that do, nearly three-fourths do not test it!

Continued from page 3

- Have you performed a risk assessment and business impact analysis?
- Do you know what your assets are, what their vulnerabilities are, and what threats can exploit them to perform the risk and threat analysis?

If the answers to these are mostly, "No," it's time to get serious about an information security (InfoSec) program.

Fortunately, many good references are available. Look into the ISO 17799 standards until the new updates in ISO 27000 are completed. Or consider the ISO 13335 standard on IT Security Management.

Another good reference for security guidance is the Control Objectives for Information and Related Technology (CobiT). CobiT is an internationally applicable and accepted IT governance and control framework for aligning IT with business objectives, delivering value, and managing associated risks. Available through the IT Governance Institute (ITGI), CobiT was first published in April 1996, and version 4.0 was published in May 2006. CobiT 4.1 is the current version. CobiT provides a reference framework for IT management and users, as well as IT audit, control, and security practitioners. Its policy guidance can help an organization implement effective governance throughout IT, and get the most value from IT investments.

There is a difference between business continuance and disaster recovery planning. Although often used interchangeably, they are not the same thing. Think of business continuance as the ability of an organization to provide continued services and support for itself and its customers while maintaining its viability before, during, and after a business continuity event. This is fundamentally a proactive exercise.

Disaster recovery, on the other hand, is a reactive exercise. It is a set of activities undertaken to eliminate or reduce the negative effects of foreseeable interruptions of mission-critical business processes, and to mitigate the deleterious effects of unforeseeable interruptions. In short, how does an organization recover from an event that prevents the continuous operation of the business?

Business continuity and disaster response and recovery generally get accomplished if and when there are any leftover resources to direct to a solution. Ill-planned, incomplete solutions to business continuity and disaster recovery planning (BC/DRP) just invite other disasters. Only through strategic thinking and organized processes can organizations gain the upper hand.

Security professionals will advise that a security policy is probably the most important item to start with when considering information security. Other measures may seem imperative; however, merely deploying security measures such as a firewall or intrusion prevention system is not enough. A security policy ensures that everyone in an organization understands their responsibilities. To this end the security policy must support the company mission and be viewed by all as an asset to the company in the same way that research and development is an asset. Too often, information security, when added as an afterthought, and not planned out with company goals in mind, is seen only as a necessary evil.

Too often, information security, when added as an afterthought, and not planned out with company goals in mind, is seen only as a necessary evil.

Regulatory compliance is also driving many businesses to consider implementing new, or updating existing Information Security programs.

Regulatory compliance has existed as long as there have been governments. In our lifetime, regulatory compliance has included such things as driver's licenses, taxes, and passports for international travel. Some of the newer, better known regulations today include Sarbanes-Oxley (http://www.sarbanes-oxley.com/), Gramm-Leach-Bliley (http://www.ftc.gov/privacy/privacyinitiatives/glbact.html), HIPAA (http://www.hhs.gov/ocr/hipaa/), and the U.S. Patriot Act (http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162:). The type of business determines which regulations the business must comply with.

Despite the potential upcoming rollback on Sarbanes-Oxley rules, a new regulation took effect December 1, 2006. The Federal Rules of Civil

Procedure will require most businesses to retain electronic records—emails, instant messages, and text documents—and be able to retrieve them in economically feasible ways. The rules also require IT managers within those companies to be able to show how electronic records are stored and what mechanisms are used to retrieve them, as well as when and how those records are deleted.

Unfortunately, most companies are not prepared to comply with these new rules. A recent study by the Enterpise Strategy Group (ESG) notes that 90 percent of organizations with more than 20,000 employees have experienced an electronic discovery within the past 12 months. However, another study by Cohasset Associates notes that almost half of all organizations have no email retention policy! Companies must start preparing such policies.

In summary, there are two principal questions that companies should address when trying to address a business challenge. The first is how to address the challenge. This is a technological discussion. The second is where to address the challenge.

As to the first question, how, there are a myriad of technologies that will be used for business continuance and disaster recovery, each worthy of a separate article. Such concepts include VPNs, encryption, authentication, and storage. For example, should a company implement a DAS, NAS, SAN, or CAS, and why? Should a company use a Fiber Channel protocol, perhaps FC/IP? Should the organization consider iSCSI or Ethernet?

Considering the second aspect, companies should determine where solutions should be implemented. There are three choices here. The company can either place some technology on its own site, an on-premises solution. Or the company can place the technology "in the cloud", an off-premises solution. The third option is a combination of the two.

As always, I appreciate hearing from you. Feel free to email me at mark@hill.com, as well as check out our blog, wiki, and PodSnacks for more insight on business continuance and other topics. Until then, remember that knowledge matters.

Mark Steinberg
Hill Associates, Inc.
Director of Business Development
Senior Member Technical Staff
CISSP
mark@hill.com

There are two principal questions that companies should address when trying to address a business challenge. The first is how to address the challenge... The second is where to address the challenge.

New Regulations

Some of the major initiatives requiring businesses to upgrade IT infrastructures are:

- HIPAA, which deals with the portability and security of a patient's medical data.
- Sarbanes-Oxley, which mandates that both a company's CEO and CFO sign off on pertinent financial reports.
- U.S. Patriot Act, which requires strict adherence by financial services organizations to anti-terrorism and anti-money laundering regulations.
- Gramm-Leach-Bliley, which regulates how financial institutions use private customer data.
- Federal Rules of Civil Procedure, as amended, which impose new requirements on record retention in the event of litigation.
- E-SIGN (Electronic Signatures in Global and National Commerce Act), which makes a transaction's electronic contracts and signatures legal and binding.

john cushman

AT&T BusinessDirect®

As the new Vice President for eSales & Service, I am delighted to be assuming responsibility for the AT&T BusinessDirect® portal. As you may know, this portal has received numerous awards and accolades for being the most outstanding network-management and customer-service portal in the telecommunications industry.

Two of the capabilities that have been unmatched in the industry include AT&T BusinessDirect Map, which provides a geographical representation of a customer's network, along with point-and-click network-management capabilities, and AT&T BusinessDirect Mobile, our new remote-access capabilities for AT&T eMaintenance.

As proud as we are of these accomplishments, we also continue to move forward with additional portal enhancements. Primary among these are our considerable integration efforts that will allow our customers to enjoy the same customer experience regardless of whether they were previously with SBC, BellSouth, Cingular, or AT&T.

At the same time, we continue with the energetic evolution of our industry-leading tools. Specifically, we will continue to extend our mobile capabilities so that customers really can manage their networks and accounts from virtually anywhere. And we will continue to enhance our collaborative communication tools so that customers can communicate with us in the most efficient and convenient ways.

Taken together, all of these efforts and a consistent customer-centric focus will undoubtedly lead us to further successes. I look forward to working alongside you in this exciting time.

John Cushman
Vice President
AT&T eSales & Service

We will continue to extend our mobile capabilities so that customers really can manage their networks and accounts from virtually anywhere.

AT&T BusinessDirect® Tops All Competitors

For the third consecutive year AT&T has been recognized by a leading industry research firm as providing customers with the strongest online support and service experience in the industry through its Web portal, AT&T BusinessDirect.

AT&T BusinessDirect was once again ranked as the best e-portal in service categories deemed critical to enterprise customers in an annual survey of leading carriers providing wired and wireless services conducted by the Yankee Group.

AT&T BusinessDirect combines service management and support reporting tools into a single, secure extranet site that provides users with increased visibility and cost control over their network performance and investments. Each month, hundreds of thousands of AT&T business customers conduct more

than 3 million transactions—ranging from ordering services, to maintenance requests, to billing inquiries—using AT&T BusinessDirect. The number of BusinessDirect customer transactions increased 12 percent in 2006, and AT&T expects use of the service will continue to grow even higher in 2007.

The Yankee Group study, which was completed in December 2006 and published in May 2007, compared ordering, maintenance, billing and network management functionality in the portals of five Tier-1 service providers. In addition, the study concluded that AT&T had the strongest enterprise portal across all of these areas with the widest range of product coverage, functionality and integration to the enterprise.

"Web-based self-care emerged as an invaluable tool for providing enterprise customers with more information and choices for how to manage their carrier-based services," said said Paul Hughes, Vice President of Enabling Technologies Service Provider Group at Yankee Group. "This is the third consecutive year that AT&T continues to be the industry leader for online customer service and support with AT&T BusinessDirect. AT&T stood out in 2006 by demonstrating leadership in the integration of mobile devices into the Web portal. Other carriers should follow its lead."

We want to hear from you!

If you have ideas for future articles, or if you'd like to contribute, please contact editor Elaine Tipping at elaine.tipping@att.com, or contact your liaison manager.

READ THE WORLD OVER

Editor Elaine Tipping researching *france telecom* for future *UPDATE* articles.

The AT&T Ethernet Portfolio includes a diverse set of products allowing customers to match their network requirements to the right technology, price and service performance.

Ethernet has been readily adopted as a transport solution worldwide. It has become the premier LAN technology—used in 98% of US LANs. It's simple, familiar, low-cost, ubiquitous, scalable, and bandwidth rich.

The AT&T Ethernet Portfolio includes a diverse set of products allowing customers to match their network requirements to the right technology, price and service performance. The portfolio spans products designed for small business customers to the largest corporate customer hungry for bandwidth. Although some of the services may have different names in different states, they can be broadly categorized as shown below. This article provides a simple overview of the comprehensive AT&T portfolio of Ethernet services designed to meet the full breadth of performance, reliability and bandwidth for customers' changing business demands.

This depiction of the AT&T Ethernet product continuum shows the bandwidth range for the various Ethernet services. The Ethernet services are categorized by the number of buildings connected and bandwidth requirements.

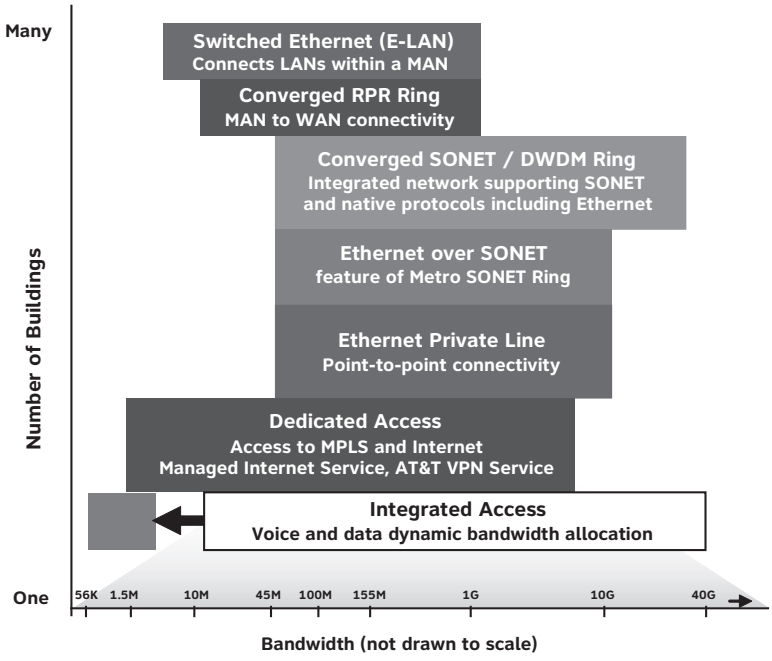
Switched Ethernet (E-LAN)

Opt-E-MAN®

Opt-E-MAN Service is a switched Ethernet service that connects a customer's LANs within the same metropolitan area. Opt-E-MAN service provides a fully managed and scalable optical service and uses Multiprotocol Label Switching (MPLS) in the core network architecture. This service provides flexible bandwidth options, from 5 Megabits per second (Mbps) to 1 Gigabit per second (Gbps), for growing Ethernet application needs. Multiple locations can communicate with each other using a switched Ethernet solution that supports many types of business applications.

Opt-E-MAN service supports many transport data configurations (point-to-point, point-to-multipoint, multipoint-to-multipoint). It uses physical and virtual connections to satisfy specific business requirements. Ethernet Virtual

The AT&T Ethernet Portfolio



Connections (EVCs) are used to transmit Ethernet LAN frames that run over optical fiber to your intraLATA network. The EVCs also transmit to the Internet or a network-based Virtual Private Network (VPN) service. The fiber transport connects to network terminating equipment at your location, and connects to the service using a router, bridge, or switch.

Availability: Offered in CA, NV, TX, KS, MO, IL, IN, OH, MI, WI, CT

Customized Switched Metro Ethernet

Customized Switched Metro Ethernet (CSME) Service is a switched Ethernet service that connects a customer's Local Area Networks (LANs) within the same metropolitan area (intraLATA) to create a Metropolitan Area Network (MAN). CSME is available in a wide range of metropolitan areas and provides scalable optical service at speeds of 10 Mbps, 100 Mbps, or 1 Gbps.

CSME is a fiber-based Layer-2 switched service providing a broadcast domain network and does not offer grades of service in its core architecture. Like Opt-E-MAN, however, it supports many transport data configurations (point-to-point, point-to-multipoint, multipoint-to-multipoint). It uses physical and virtual connections to satisfy specific business requirements.

CSME connects the Ethernet cloud and establishes logical EVCs traversing the public network to transparently connect to customer locations. CSME uses fiber optics and Ethernet to provide a Virtual Private Network. Network connections are made with a router, bridge or switch. A customer can connect to locations within a MAN as if they were segments on the same LAN.

Availability: Offered in CA, NV, TX, KS, MO, OK, AR, IL, IN, OH, MI, WI

AT&T Ethernet Switched Service—MAN

AT&T ESS—MAN is an Ethernet Virtual Private Network supporting any-to-any high bandwidth LAN connectivity between customer locations in a metropolitan area allowing for a hub and spoke, partial meshed or fully meshed logical customer network configuration.

Availability: Offered nationwide

Metro Ethernet Service

Metro Ethernet is a high speed packet transport that is based on Ethernet transmission parameters. Metro Ethernet Service provides various transport capabilities that range from 2 Mbps through 1 Gbps. Three switched services are offered—Basic, Premium and Virtual. Basic Service offers high bandwidth service at the most economical price point. Premium and Virtual Metro Ethernet services provide enhanced capabilities and features that are designed to support any customer application; key features include committed bandwidth, bursting capabilities, traffic prioritization for delay-sensitive traffic, Customer Network Management, and Service Level Agreements (SLA) to support Quality of Service (QoS). Switched Metro Ethernet Service supports hub-and-spoke or fully meshed logical customer network configurations.

SMARTRing® and LightGate® service can be used as the underlying transport for Metro Ethernet service.

Availability: Offered in AL, FL, GA, KY, LA, MS, NC, SC, TN

Converged Resilient Packet Ring (RPR)

AT&T Ultravailable® Managed Opt-E-Ring℠ Service

The AT&T Ultravailable Managed Opt-E-Ring Service uses the power of resilient packet ring technology to interconnect your customer's data centers and business sites in a Metropolitan Area Network (MAN) environment with the ability to extend the MAN into the WAN with cost-effective, scalable, rapidly provisioned, fully managed and highly reliable service. This service is designed and engineered to provide the highest possible levels of availability, assuring fail-safe, continuous operations and access to mission-critical information. Speeds range from 10 Mbps to 1 Gbps and the service supports any-to-any connectivity.

Availability: Offered nationwide

Converged Sonet/DWDM Ring

AT&T Ultravailable® Network Service

Ultravailable Network Service (UVN) is a fully managed, custom DWDM/SONET-based solution for interconnecting data centers or business sites in a highly

Continued on page 10

The Ethernet VPN network design is enabled by Ethernet switching technology supporting connectivity speeds from 50 Mbps to 1000 Mbps.

Continued from page 9

reliable and secure metropolitan area network (MAN) environment. This highly secure fiber optic MAN provides the communication path between the premise and the AT&T POP/LNS node(s), or any third party fiber provider's node.

This service enables different types of data protocols to be carried over an optical channel and transmitted through protected equipment. The AT&T diversely routed fiber network helps to protect payload traffic in the event of a fiber cut or equipment failure. UVN provides a fully-managed alternative to dark fiber and a comprehensive network solution, in addition to:

- Diverse connections to AT&T Points of Presence
- Secure private communications network
- Protocol independent service channels
- No single point of failure
- Scalable design to meet changing infrastructure requirements

Available in Bandwidth/Speeds: OC-3, OC-12, OC-48 and OC-192

Supported protocols include Native IT (ESCON, FICON, GigE, D1, FDD1);1 & 2GB Fiber Channel; DS-1 / DS-3; OC-3, OC-12, OC-48, and OC-192 bandwidths; Fast Ethernet; Gigabit Ethernet, 10 Gigabit Ethernet, ISC; D1 Video; ETR; and SONET.

Availability: Offered nationwide

Ultravailable® Service Option2

Ultravailable Service Option2 offers all the same speeds and features as Ultravailable Network, with standard configurations, management services and Service Level Agreements. However, there are specific engineering rules that must be met in order to comply with Ultravailable Service Option2, such as: no more than six nodes or more than 120 miles on total circumstance; configured as planned with minimal changes; and not to exceed more than 4 wavelengths.

Ultravailable Service Option2 is targeted to:

- Mid-size enterprise customers
- Clients with traditional OC48 & OC192 ACCU-Ring requirements needing additional bandwidth and services
- Existing ACCU-Ring customers who require DWDM or other services not currently offered on ACCU-Ring such as FICON, ESCON, etc

Availability: Offered nationwide

Multi-Service Optical Network

MON Ring—Multi-Service Optical Network—is a flexible, high-bandwidth service that supports a broad range of protocols and network modification without changing equipment. MON Ring offers the outstanding bandwidth and flexibility of Dense Wavelength Division Multiplexing (DWDM) technology plus the security of fiber sustainability.

MON Ring lets you use multiple protocols and connect to multiple sites. If you are currently using several data interfaces over a variety of networks, you can combine multiple data signals and transport them over one network. MON Ring service allows you to maintain a simpler, more efficient, and easily expandable network using high-speed circuits.

MON Ring provides DWDM capability over a single pair of fibers in two directions. Therefore, you can increase capacity without limiting required data interfaces. MON Ring is suitable for such demanding applications as mainframe or data center mirroring, data center connectivity, storage area network connections, and disaster recovery. This flexible, multi-service platform delivers up to 32 wavelengths of bandwidth through the power of DWDM and offers 10 Gbps per wavelength scalability.

Availability: Offered in CA, NV, TX, KS, MO, OK, AR, IL, IN, OH, MI, WI, CT

Metro SONET Ring

AT&T ACCU-Ring® Network Access Service

AT&T ACCU-Ring Network Access Service is a private Synchronous Optical Network (SONET) ring that provides dedicated high-speed access for consolidation of your customer's traffic. ACCU-Ring provides a two-way digital channel for transmission of synchronous, asynchronous and Time Division Multiplex (TDM) signals via a private dual-fiber, self-healing SONET ring that

The AT&T diversely routed fiber network helps to protect payload traffic in the event of a fiber cut or equipment failure.

assures the highest reliability for uninterrupted communications. It consolidates all traffic including AT&T all-distance traffic—voice, data and video. Standard service channels of 1.5 Mbps (DS1), 45 Mbps (DS3), 155 Mbps (OC-3/OC-3c), 622 Mbps (OC-12c) and 2.5 Gbps (OC-48c) and Ethernet service channels of 50 Mbps, 150 Mbps, 300 Mbps, 600 Mbps and 1 Gbps are supported. Performance is monitored 24/7 by the ACCU-Ring Service Center and managed end-to-end by AT&T. ACCU-Ring provides bandwidth for ring capacities of 155 Mbps (OC-3), 622 Mbps (OC-12), 2.5 Gbps (OC-48) and 9.95 Gbps (OC-192). If the ring is used to carry local voice, PRI or local data circuits Dedicated SONET Ring Service should be used.

Availability: Offered nationwide

Dedicated SONET Ring Service (DSRS)

Synchronous Optical Network (SONET) is an optical fiber ring network backbone that accommodates additional capacity as needs increase. SONET enables bundling of network connections, such as multiple DS1 and DS3 circuits and native Ethernet, on one continuous optical fiber structure and connection of existing protocols to it. SONET ring service employs bi-directional line-switched ring (BLSR) configuration to provide inherent protection on the bandwidth between nodes. Such a configuration enables transport of bandwidth-intensive applications between specific locations and use of SONET ring(s) without concerns over service outages. SONET ring structure has the power and capacity to fully integrate WAN traffic, making it an economical, reliable, enterprise-wide solution. SONET transports Ethernet, data, video, and voice traffic between customers' locations and AT&T central offices on a single, fail-safe platform. SONET can sustain as much as 10 Gbps of traffic providing the bandwidth to support all communications. A SONET ring or point-to-point service can be used in place of any analog private line, DS0, fractional DS1, DS1, and DS3 circuits.

Availability: Offered in CA, NV, TX, KS, MO, OK, AR, IL, IN, OH, MI, WI, CT

SMARTRing®

SMARTRing service is a SONET based, self-healing ring network in which the entire capacity is dedicated to a single customer. SMARTRing is designed to transport DS1, DS3, STS-1, OC-3, OC-12, OC-48, 10 Mbps, 100 Mbps, 1,000 Mbps circuits and Fractional Gig E speeds of 50 Mbps, 150 Mbps, 300 Mbps, 450 Mbps and 600 Mbps between customer-designated locations. SMARTRing service offers customers with high levels of traffic in a metropolitan area an industrial strength transport product. The host ring for SMARTRing can be OC-3 (155 Mbps), OC-12 (622 Mbps), OC-48 (2488 Mbps) or OC-192 (9953 Mbps or 10 G). Ethernet is offered as a point to point between two locations on the ring, as a multi-point service using Virtual Packet Ring (VPR) to establish the accessible bandwidth between multiple points on the Ring, or as a connection to Metro Ethernet service.

Availability: Offered in AL, FL, GA, KY, LA, MS, NC, SC, TN

Ethernet Private Line

GigaMAN®

GigaMAN Service is a dedicated, fiber-optic, point-to-point gigabit Ethernet service that links local area networks within a metropolitan or regional area. GigaMAN Service transmits data at up to 1 Gbps—22 times faster than DS3 service—across the street or across town. GigaMAN service uses the same transmission protocol as LANs to take full advantage of enterprise LAN speeds while transmitting data between sites. GigaMAN service connects existing gigabit Ethernet switches with dedicated, single-mode fibers.

Availability: Offered in CA, NV, TX, KS, MO, OK, AR, IL, IN, OH, MI, WI, CT

DecaMAN℠

DecaMAN Service is a fiber-optic point-to-point transport service that connects a 10 Gbps Ethernet signal within the same Local Access and Transport Area (LATA). DecaMAN supports point-to-point configurations to transmit serial data at a discrete bit rate of 9.95 Gbps WAN PHY and 10.3125 Gbps LAN PHY Ethernet physical layer

SONET can sustain as much as 10 Gbps of traffic providing the bandwidth to support all communications

Continued on page 12

Continued from page 11

rate. DecaMAN is based on the IEEE 10-gigabit Ethernet standard (802.3ae), which contains two interface options: WAN PHY and LAN PHY. AT&T can provide either interface option on a particular DecaMAN circuit. Because DecaMAN can interface natively to 10 Gigabit Ethernet based equipment, no special equipment or protocol conversion is required to achieve high capacity and efficient data transport. DecaMAN is built on a robust, Wave Division Multiplexing (WDM) network for maximum availability and fiber use, while delivering outstanding performance.

Availability: Offered in CA, NV, TX, KS, MO, OK, AR, IL, IN, OH, MI, WI, CT

EPLS-MAN

Ethernet Private Line Service—Metropolitan Area Network (EPLS-MAN) is a point-to-point, fixed-bandwidth Ethernet transport service that connects local area networks (LAN) or locations to other locations within a metropolitan area. EPLS-MAN provides interface rates of 50 Mbps to 1 Gbps. With EPLS-MAN, you can gain access to high bandwidth by using the same Ethernet protocol as your current LAN application. The service transmits your data through the network using Ethernet-over-SONET encapsulation. EPLS-MAN is similar to local private line service except EPLS-MAN provides a layer-2 Ethernet interface, while local private line provides a layer-1 SONET interface.

Availability: Offered nationwide

EPLS-WAN

Ethernet Private Line Service-Wide Area Network (EPLS-WAN) is a point-to-point, fixed-bandwidth Ethernet service that provides inter-city, full-duplex data transport over combined-access and long-haul (core) networks. EPLS-WAN provides interface rates of 50 Mbps to 1 Gbps.

With EPLS-WAN, you can gain access to high bandwidth by using the same Ethernet protocol as LAN applications. Once on the AT&T long-haul network, Ethernet packets travel over a SONET transport network, which assures low latency and fast recovery from failure—typically within 50 milliseconds.

Once on the AT&T long-haul network, Ethernet packets travel over a SONET transport network, which assures low latency and fast recovery from failure—typically within 50 milliseconds.

Availability: Offered nationwide

LightGate®

LightGate is a dedicated point-to-point SONET service that supports bandwidth from DS3 up to OC-192. Ethernet can be provisioned as point-to-point (CO to CO) between two LightGate Systems (CO to Prem, Prem to CO), and connect to SMARTRing, Wavelength or Metro Ethernet service. LightGate is designed to transport DS1, DS3, STS-1, OC-3, OC-12, OC-48, 10 Mbps, 100 Mbps, 1,000 Mbps circuits and Fractional Gig E speeds of 50 Mbps, 150 Mbps, 300 Mbps, 450 Mbps and 600 Mbps between customer-designated locations.

Availability: Offered in AL, FL, GA, KY, LA, MS, NC, SC, TN

Wavelength Service

Wavelength Channel offers two tariffed solutions for point-to-point connectivity. The FCC Tariff offering is Wavelength Channel Service and is offered as individual channels or as Dedicated Systems. Dedicated Systems offer specific Wavelength Channel capacities:

- Dedicated System 1 = 4 unprotected Channels
- Dedicated System 2 = 8 unprotected Channels
- Dedicated System 3 = 16 unprotected Channels
- Dedicated System 4 = 32 unprotected Channels

The Private Line (State Tariff) offering is Wavelength Service Basic Arrangement. Both services offer a point-to-point transport between the customer premises and the Serving Wire Center over a shared Dense Wavelength Division Multiplexing (DWDM) infrastructure.

Wavelength Dedicated Ring Service provides dedicated bandwidth over dedicated point-to-point facilities in a ring topology service configuration. Wavelength channel speeds begin with 1.25 Gbps Transparent Transport to OC-192 Wavelength Transport, Gigabit Ethernet and Fast Ethernet, and Fibre Channel. All wavelength services offer channel protection on a channel by

channel basis. Channels can be unprotected which offer two diversely routed channels with the customer providing the switching (Client Protection), or Network Protection with AT&T providing the switching and route diversity.

Availability: Offered in AL, FL, GA, KY, LA, MS, NC, SC, TN

Dedicated Access

AT&T Managed Internet Service

Managed Internet Service is an Internet access service that combines a high-speed, dedicated connection with consolidated application management. It lets the customer reliably access information resources and communicate with Internet users worldwide. Managed Internet Service (MIS) includes proactive, 24x7 network monitoring, enhanced network security features, and maintenance of the communications link between locations and the AT&T network.

MIS is available in three service types. MIS with Managed Router provides managed Internet access, including on-site router, Channel Service Unit/Data Service Unit (CSU/DSU), and diagnostic modem management. MIS (with Customer Managed Router) and International MIS (I-MIS) provide managed Internet access but allow customers to provide and manage their own on-site equipment. MIS uses an access circuit to connect a LAN to the AT&T fully redundant, highly reliable MPLS IP backbone network. The Internet traffic travels over this network to destinations around the globe. AT&T proactively manages all network components, including access circuit, router, and firewall, to monitor network security and performance.

Availability: Offered nationwide

AT&T VPN Service

AT&T VPN is a network-based IP VPN solution that is enabled by Multiprotocol Label Switching (MPLS). AT&T VPN is the evolutionary successor to the IP services which began with IPFR/ATM. AT&T VPN service enables customers to build an application aware, network-based Multiprotocol Label Switching virtual private network to link locations and efficiently transmit applications such as voice, data, and video over a single connection. Customers can choose the access method to AT&T VPN. ATM, Dedicated Private Line, Frame Relay and SDSL (where available) may all be used to connect to an MPLS port. In addition AT&T plans to add an Ethernet MPLS port option.

AT&T VPN simplifies and will over time consolidate capabilities from the company's currently separate MPLS-based VPN services—IPeFR/ATM, PNT, EVPN and NVPN—into a single VPN service. This will enable AT&T to offer a world class global network-based MPLS VPN with options to add on the features that customers want, when they want them, without having to migrate between different VPN services. AT&T VPN currently has transport capabilities and in the future will include integrated options like managed CSU and managed routers.

Availability: Offered nationwide

Integrated Access

Integrated Network Connection Service

AT&T Integrated Network Connection Service provides dynamic bandwidth allocation for voice and data services, allowing more traffic to be carried on fewer high-speed access lines. The service supports AT&T Frame Relay and ATM as a data access method to extend the AT&T voice and high-speed packet networks to a customer's premises.

Availability: Offered nationwide

With the largest Ethernet footprint in North America, AT&T Ethernet Services are where customers need them. Service is available in a variety of bandwidths and configurations that can be expanded and changed with ease, to meet business application needs. For more information about these products contact your Liaison Manager.

Tom David
Liaison Manager
td1898@att.com

AT&T Integrated Network Connection Service provides dynamic bandwidth allocation for voice and data services, allowing more traffic to be carried on fewer high-speed access lines.

nancy grover

Get a Mac?

Apple recently made its browser, Safari, available for Windows users. Eight security holes were discovered in the first day. Yes I know it was a beta version, but it raised eyebrows nonetheless. Maybe it was a lack of testing, or maybe there were flaws because the product was out of Apple's closed, protected environment, or maybe it was the Windows platform. Whatever the reasons, the situation brought an age-old question back to the forefront. Is a Mac really more secure than a PC?

Whatever the reasons, the situation brought an age-old question back to the forefront. Is a Mac really more secure than a PC?

If you watch the Mac vs. PC ads you may come away thinking the Mac is completely secure, and PC's should only be handled with latex gloves and surgical masks. But just how realistic is that? To answer theses questions, I called upon my nine years of Unix security experience, and the expertise of four friends to add insight on this hotly debated topic: Dennis Ritchie, father of Unix, and a Unix and Planet 9 on PC user; Bill Cheswick, creator of the firewall, and a BSD Unix and Mac user; H D Moore, security researcher, white-hat hacker extraordinaire, and user of Linux; and Dan Tentler, a local systems architect, San Diego Bar Camp organizer, and Mac, PC and Linux user. Interestingly enough, we came to a similar conclusion.

But first, a little background.

Viruses

This may come as a surprise, but the first computer virus released into the wild was something called Elk Cloner, and its target was Apple II machines. That was in 1982. Brain, the first PC virus, followed four years later. Two years after that, it was Macintosh's turn, when it was hit with the MacMag and Scores. Since then, Windows has been the ultimate target of the virus writers.

Worms

The first worm was the Morris worm and it infected Sun and BSD Unix systems. After a few years of targeting Unix, the worm writers have been concentrating almost exclusively on Windows machines; although, a minor worm dubbed Oompa Loompa did hit Mac OS X systems just last year.

Security Patches

On the second Tuesday of every month Microsoft releases new security patches. There is usually a press release and lots of media attention, which makes it seem that Microsoft is the only company experiencing security flaws. But they aren't alone. Since January, Apple has also been issuing patches each month, but without the fanfare. As part of May's security bulletins, Microsoft corrected 19 vulnerabilities; Apple fixed 12.

Closed system

Apple and Windows both use proprietary operating systems that prevent others from having access to their code. But Apple takes it one step further by controlling the whole experience, from the hardware and software to the peripherals. This allows Apple systems to work in that seamless fashion its users rave about, but at the same time, it limits choices. Microsoft, on the other hand, allows an extensive choice of software, hardware and peripherals to work with its operating systems. And this can affect security.

Dennis thinks Microsoft systems have a lot of security problems. "But," he adds, "I suspect an even bigger thing is that the common MS applications like mail, browsers, spreadsheets and the like are a bit too eager or willing to execute code or scripts that might come from elsewhere."

Bill adds, "The closed hardware of the Apple means they don't have to deal with drivers from every hardware vendor on the planet, as Windows and even Linux tries to do. A lot of Windows' grief comes from the sheer number of drivers they have to deal with."

Out-of-the-box security

Is security better on one system over

the other if you take it take it straight out of the box, plug it in and use it? H D Moore says they both have issues. "Out of the box, a Mac OS X system is exploitable through mDNS. Once you apply patches, turn off services, and switch to a more secure web browser, it might be more secure than a Windows system. Out of the box, a Windows XP SP2 system is exploitable through a variety of flaws. A brand new OEM Vista system is also exploitable right out of the box, if you use the default browser to go online."

And Bill found a number of default UDP listeners on his Mac that he doesn't like the looks of, "Of course, a lot of Internet troubles don't come from running services, but are invited in. Safari, iChat, and Mail are obvious possible weak points."

And Dan had this to say: "With Windows, if you want to protect yourself you have to buy antivirus software on a subscription basis, you have to buy anti-spyware and anti-malware software to keep the pop-ups and zombies away. More software needs to be purchased to address local firewalling issues because the Windows firewall is not as effective as I'd like it to be."

So, is a Mac more secure?

H D says either system can be locked down, but it really comes down to a numbers game on which system is most likely to be attacked. "I believe Macs are less likely to be compromised by a random bot-herder or script kiddie, but that doesn't mean they are any less exploitable. If anything, the Mac OS X operating system falls behind Windows when it comes to OS-level security features. Among other things the heap management code in Windows XP SP2 and Windows Vista are much more robust than on OS X, making classic heap overflows slightly more difficult."

Bill adds, "There is a lot of discussion about how secure a Mac is. It is mostly opinion and conjecture. Macs have been largely below the radar, and therefore not subjected to many attacks from the professional attackers who count their successes in the number of machines compromised. So Macs have not been through much of a wringer. Being below the radar is a fine defense, and means that Macs are unlikely to be major targets until they have a much larger market share."

Dennis agrees, "Microsoft systems are more common and hence a richer target. The MAC-OS approach is I think on the whole better, but probably it's mainly that there is a lot more Microsoft code, and Microsoft systems out there."

And H D sums it all up: "Until Apple's market share increases, spyware and malware writers have no incentive to target Mac users. If critical mass is reached and it becomes profitable to exploit Mac systems, the perceived 'security' of Mac OS X will plummet as more home users have their systems hijacked."

Securing your system

What it all comes down to is this—there is no such thing as an operating system impervious to security risks, especially when it comes to malware. And that includes both the Mac and the PC. But once both systems are securely configured, the consensus is they can pretty much stand shoulder to shoulder.

Dan likens securing an Apple to securing a Unix machine: "What it boils down to is control. If a user is familiar with how to secure a computer, they can easily secure an Apple."

As for Windows security, it may not be as difficult as you think. Like Unix and Apple, it's a matter of turning off unused services and sharing, choosing a secure browser and locking it down even more.

And as with all systems, keeping current with security updates for the OS and security software, and employing safe computing practices are imperative. To help with this task, both Apple and Microsoft offer their users comprehensive security guides on their sites.

Mac OS X Security Configuration Guide—
http://images.apple.com/server/pdfs/Tiger_Security_Config_021507.pdf

Windows XP Security Guide—
http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx

So no matter what type of user you are, secure your system, and be careful. You never know what's lurking out there, and who will be the next target.

Nancy Grover
Regional Manager
AT&T Corporate Information Security

What it all comes down to is this—there is no such thing as an operating system impervious to security risks . . .

CALNET 2

AT&T and the State designed the CALNET 2 contracts to meet agencies' existing tele-communication requirements and to support the infrastructure for future business applications.

The State of California Department of Technology Services has contracted with AT&T to provide public agencies with a comprehensive collection of integrated enterprise network services. AT&T and the State designed the CALNET 2 contracts to meet agencies' existing telecommunication requirements and to support the infrastructure for future business applications.

The contract includes a complete suite of integrated enterprise network services and equipment. All public sector agencies can use CALNET 2. This includes the State as well as any public or local government agency that is nonprofit and entirely tax supported or has an eligible joint powers agreement.

Below is a partial list of the services available with CALNET 2.

Voice Services

- Business Lines
- Calling Cards
- Centrex – Basic, Area-wide plus Enhanced
- Interactive Voice Response (port and network based)
- Long Distance Calling
- Operator Services
- Specialized Call Routing
- Toll Free Services
- Voicemail
- 900 Service

Data Services

- Asynchronous Transfer Mode (ATM) – local, statewide, nationwide
- Dedicated Data Circuits – local, statewide, nationwide
- DSL Virtual Private Network
- Agency Hosted DSL
- Fax Broadcast
- Frame Relay – local, statewide, nationwide
- Gigabit Ethernet Metropolitan Area Network Services (GigaMAN, Opt-E-MAN, etc).

Integrated Services

- Advanced Intelligent Network
- Synchronous Optical Network (SONET) Services
- Enterprise Messaging Service (EMS) Unified Messaging
- Fiber Ring and Access Services
- Virtual Private Network (AVPN)
- Multiprotocol Label Switching (MPLS) Services
- Compucall and Computer Telephone Integration (CTI)

Conferencing Services

- Audio Conferencing (multiple types)
- Video Conferencing (multiple types)
- Web Conferencing (multiple types)

Call Center Services

- Automated Attendant and Call Router
- Automatic Call Distribution (ACD) including Management Information Service (MIS)
- Network-Based Call Center

Equipment

- Complete range of data equipment
- Complete cable and wiring services

For more information, and to view a copy of the contract, visit: www.CALNETii-info.com.

2007 Segmentation Overview

By uniting industry leaders with broad product portfolios, diverse customers, and complementary strengths, AT&T is positioned to be an end-to-end solution provider for companies nationwide and around the globe. The Business Customer Segmentation model allows AT&T to continue to maximize combined strengths and provide outstanding service to customers.

Enterprise Business Services (EBS):

EBS is a multi-national/national sales organization that supports large and medium businesses with national/ international distribution and/or locations both domestically and internationally.

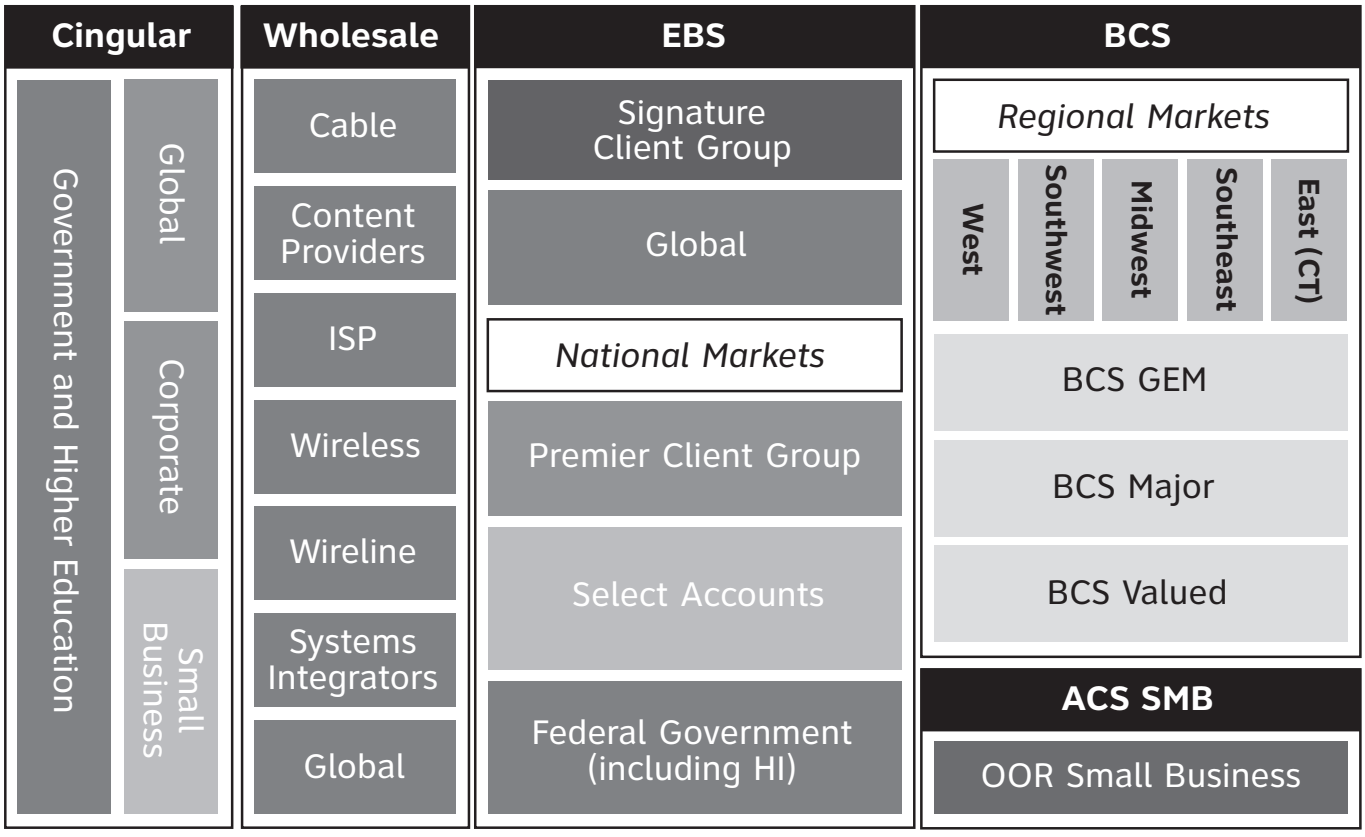
Business Communications Services (BCS) Regional Markets:

BCS Builds on a strong 22-state foot print through five regional sales organizations (East, Midwest, Southwest, Southeast, West).

Wholesale Markets:

Delivers end-to-end telecommunications solutions (for both resale and internal use) to service providers on a global, regional and local basis.

AT&T Business Segmentation Summary



jerry hinek

J.K. Rowling and Information Security

I've enjoyed each of the first six Harry Potter books, and as I write this article in the month of June, I look forward to my chance to read the final book in the series, *Harry Potter and the Deathly Hallows*, due to be published Saturday, July 21. Along with most of the world, I have no access to the story in the book before it's published, and I don't know what will befall Harry as this series ends.

Author J. K. Rowling uses information security to enhance her considerable wealth. She's not just an author, she's a business woman, and information security is part of her business plan. Her writing skills have brought her from welfare to riches; she used information security to maximize that success.

J. K. Rowling has written seven best-selling novels. Pre-orders for the seventh made it a best-seller the day it was published. Information security comes into play in the pre-publication processes. While it's no secret that Harry will again confront Lord Voldemort, the story of that confrontation and its conclusion are secret. People have to pay to read the book.

From Rowling's writing of the book until its publication, information has been concealed and released in ways to get the most people to buy the book. As July 21 approached, keeping the secret became more difficult as the process ramped up for the climactic availability of the book. More and more people had to be trusted with the secret.

The cornerstones of information security are confidentiality, integrity and availability. Let's take a look at how they are key to J.K. Rowling's business plan.

Harry Potter and the Deathly Hallows is a secret shared by a small but growing number of people: the author, the editor, some typesetters and translators, perhaps a few others.

No doubt only J. K. Rowling has the right to discuss anything in the book before July 21. She has given a few clues, mostly to build anticipation, but has not given anything away. As time gets closer to publication date, more and more people have access to the story; after all, millions of copies will be printed and shipped to book stores, online booksellers and fulfillment houses all over the world. Online booksellers have taken advance orders for the book and will ship it so that it arrives at customers homes on July 21.

How can all this be kept secret? Rowling and her publisher have had to demand secrecy as a condition for a share of the profits. This doesn't mean simply that I can't get the printer to tell me what's in the book, it means that everyone involved in the publication process must take care that unauthorized persons can't discover the secrets of the book.

Rowling's draft had to arrive securely at her editor's office. The editor had to keep the draft away from everyone else during the review and revision process.

People making the master copies had to be informed of the confidentiality requirements. Printers had to keep their plants secure, allowing only authorized employees to participate in the printing process.

The computers that store the text of the books as part of the process must be secured to keep out intruders. Perhaps the books are stored encrypted on a computer's disk drives.

Printed books have to be stored securely. Perhaps there are biometric controls that limit access. I don't know the details, but the book would not be a secret without imbedding secrecy into the whole process.

The cornerstones of information security are confidentiality, integrity and availability.

On July 21 all the confidentiality ended.

In this context, integrity means that the book that I buy on July 21 has to have exactly what J. K. Rowling wrote, as she wrote it. Integrity is a quality control issue. If someone were able to change the ending, delete chapters or rearrange paragraphs, the book wouldn't be as good and wouldn't have its value.

At first it's just up to Rowling to make sure her text isn't corrupted or destroyed in any way. Copies or backups are essential to this process just as they are with business records.

Each person who becomes involved in producing the book for publication also has to safeguard the integrity of the book. Other than the author, only the official editor should have any business modifying or updating the text. Only the official artist should have any right to create or change the graphics used throughout. Printers can not rearrange text or graphics to save paper or to cut production costs. The book comes first.

Naturally as this goes through the process, integrity becomes less of an item of concern. Once the book is in print, it can't be modified. If it's printed correctly it's Rowling's book.

On July 20 those books had to be in the possession of retailers but unavailable to the public and on July 21 they had to be easily accessible to everyone who wanted a copy. For weeks and months afterwards the copies have to be available, although the numbers will decline.

Rowling is a writer, yes, but she's also watching out for the security and success of her business, which is selling books. She started out on welfare as a single parent. She planned out the full series of seven books before she began to write the first, and she has planned out the process of publishing her books in a way that made her greater profits. She's now a billionaire.

Information security is not a peripheral aspect to your job, career or profession. It's most likely a very important part of the process that ensures you keep getting paid for your talents.

Jerry Hinek, CISSP
Senior Business Security Manager
AT&T Information Services

Information security is not a peripheral aspect to your job, career or profession. It's most likely a very important part of the process that ensures you keep getting paid for your talents.

FROM THE ARCHIVES

Photo Courtesy of SBC Archives and History Center, San Antonio, TX

Operators saluting flag at the Chicago, Illinois, Harrison office (1911)

Helpful Numbers and Web Sites

Area Code Information
http://areacode-info.com/

Area Code Look Up
http://www.my-areacode.com/

AT&T Account Manager (registration required)
http://www.att.com/accountmanager

AT&T BusinessDirect®
1-800-221-0000 Hot Line
http://www.att.com/businessdirect

AT&T Corporate Contact List
http://sbc.com/contactus

AT&T Customer Support
http://sbc.com/help

AT&T Local Service (repair desk)
1-800-829-1011

AT&T Product Information
http://ask.sbc.com

Billing Inquiry – West
1-800-891-1800

California Public Utilities Commission (CPUC)
http://www.cpuc.ca.gov

Carrier Verification
1-700-555-4141 – Long Distance
1-805-700-4141 – Local

DSL
1-877-722-3755

E-Bill
1-888-700-5422

FOCUS
http://www.thefocus.org

Internet Safety
http://sbc.com/safety

Knowledge Network
http://www.kn.pacbell.com/products/discounts.html

Local Calling Area Mapping
http://localcalling.sbc.com/LCA/lca_input.jsp

Managed Internet Service
1-888-613-6330

North American Numbering Plan Administration
http://www.nanpa.com/

Priority Repair
1-800-332-1321

Repair
611

Up2Speed Newsletter
http://sbc.com/up2speed

AT&T Consultant/Vendor Sales Group

Kari Aguinaldo, CVSG Leader
795 Folsom St Rm 517-O2
San Francisco, CA 94107
415-644-7118
email: kw6875@att.com

Mike Aaron, Liaison Manager
795 Folsom St Rm 517-P3
San Francisco, CA 94107
415-644-7129
email: ma2519@att.com
Area codes: 209, 408, 415, 510, 559, 650, 707, 831, 916, 925

Eric Aguirre, Data Administrator
email: ea3515@att.com

Consultant/Vendor Sales Group Hot Line
1-800-552-5299

Tom David, Liaison Manager
200 Center St Promenade Rm 735
Anaheim, CA 92805
949-855-5055
email: td1898@att.com
Area codes: 619, 714, 760, 858, 909, 949, 951

Lowayne Shieh, Liaison Manager
1150 South Olive St Rm 1600
Los Angeles, CA 90015
213-743-5759
email: ls1869@att.com
Area codes: 213, 310, 323, 424, 562, 626, 661, 805, 818

Vendor Consultant Service Center (VCSC)
1-800-773-3318

LOA
Fax 1-877-778-4141 / 4133

AT&T West Alliance Channel (registration required)
https://west.alliance.att.com

at&t
Your world. Delivered.℠