2007

Campus Communications Systems: Converging Technologies

The Association for Communications Technology Professionals in Higher Education

Campus Communication Systems:

Converging Technologies

The Association for Communications Technology Professionals in Higher Education

Special thanks to Verizon Business for sponsorship of this book.

$15 ACUTA Members
$25 Nonmembers
$2 Shipping & Handling

Campus Communications Systems: Converging Technologies

The Association for Communications Technology
Professionals in Higher Education
152 W. Zandale Dr., Ste. 200 · Lexington, KY 40444 USA
www.acuta.org

Special Thanks

Special thanks to the 2005–2006 and 2006–2007 ACUTA Board of Directors and Publications Committee Members who planned, directed, and contributed to this book.

2006–2007 Board of Directors

President
Carmine Piscopo, RCDD, Providence College

President-Elect
Walt Magnussen, PhD, Texas A&M University

Secretary/Treasurer
Riny Ledgerwood, San Diego State University

Immediate Past President
Patricia Todus, Northwestern University

Directors-at-Large
Harvey "Buck" Buchanan, Florida State University
John Bradley, Rensselaer Polytechnic Inst. (retired)
Randal J. Hayes, University of Northern Iowa
Corinne Hoch, Columbia University
Diane McNamara, Union College

2005–2006 Board of Directors

President
Patricia Todus, Northwestern University

President-Elect
Carmine Piscopo, RCDD, Providence College

Secretary/Treasurer
Riny Ledgerwood, San Diego State University

Immediate Past President
Tamara J. Closs, Duke University

Directors-at-Large
Phillip Beidelman, WTC
George Denbow, The University of Texas at Austin
Randal J. Hayes, University of Northern Iowa
Corinne Hoch, Columbia University
Diane McNamara, Union College

Publications Committee 2006–2007
Ron Kovac, PhD, Ball State University, Chair
Lee Badman, Syracuse University
William A. Brichta, Delaware Valley College
Janice Bundy, University of California, Los Angeles
Rick Cunningham, PAETEC Communications
George Denbow, University of Texas, Austin
Peggy Fischel, Middlebury College
Les Shaw, University of Maine
Dave Wirth, Princeton University

Ex Officio
Carmine Piscopo, RCDD, Providence College
Jeri Semer, CAE, ACUTA Executive Director

Board Liaison
John Bradley, Rensselaer Polytechnic Inst. (retired)

Staff Liaison
Pat Scott, ACUTA Communications Manager

Publications Committee 2005–2006
Walt Magnussen, PhD, Texas A&M University, Chair
Linda Bogden-Stubbs, SUNY Upstate Medical University
Rick Cunningham, PAETEC Communications
Peggy Fischel, Middlebury College
Ron Kovac, PhD, Ball State University
Dale Lee, Biola University
Paul Petroski, University of Maryland, Baltimore
Carole Sedlock, University of Toledo
Cindy Shortt, University of Texas Health Science Center at San Antonio

Ex Officio
Patricia Todus, Northwestern University
Jeri Semer, CAE, ACUTA Executive Director

Board Liaison
Randal J. Hayes, University of Northern Iowa

Staff Liaison
Pat Scott, ACUTA Communications Manager

Published by
ACUTA: The Association for Communications Technology Professionals in Higher Education
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

PHONE 859/278-3338
FAX 859/278-3268
E-MAIL pscott@acuta.org

Executive Director
Jeri A. Semer, CAE, Executive Director

Editor-in-Chief
Pat Scott, Communications Manager

http://www.acuta.org

Table of Contents

Foreword 4
Walt Magnussen, Ph.D.

Preface 5
Ron Kovac, Ph.D.

1 The Technology Landscape: Historical Overview 6
Walt Magnussen, Ph.D.

2 Emerging Trends and Technologies 15
Joanne Kossuth

3 Network Security 32
Beth Chancellor

4 Security and Disaster Planning and Management 49
Marjorie Windelberg, Ph.D.

5 Student Services in a University Setting 67
Walt Magnussen, Ph.D.

6 Administrative Services 79
David E. O'Neill

7 The Business Side of Information Technology 95
George Denbow

8 The Role of Consultants 114
David C. Metz

Glossary 122
Michelle Narcavage

Foreword

This book is a rewrite of *Campus Telecommunications Systems: Managing Change*, a book that was written by ACUTA in 1995. In the past decade, our industry has experienced a thousand-fold increase in data rates as we migrated from 10 megabit links (10 million bits per second) to 10 gigabit links (10 billion bits per second), we have seen the National Telecommunications Policy completely revamped; we have seen the combination of voice, data, and video onto one network; and we have seen many of our service providers merge into larger corporations able to offer more diverse services. When this book was last written, ACUTA meant telecommunications, convergence was a mathematical term, triple play was a baseball term, and terms such as iPod, DoS, and QoS did not exist.

This book is designed to be a communications primer to be used by new entrants into the field of communications in higher education and by veteran communications professionals who want additional information in areas other than their field of expertise. There are reference books and text books available on every topic discussed in this book if a more in-depth explanation is desired.

Individual chapters were authored by communications professionals from various member campuses. This allowed the authors to share their years of experience (more years than many of us would care to admit to) with the community at large. On behalf of all of the authors, I would like to let you know how much fun that we all had in writing this material, and we sincerely hope that you will enjoy reading it as much as we have writing it.

Special thanks go to the ACUTA Board of Directors for their vision in making this a strategic project, to Jeri Semer, ACUTA Executive Director, for her guidance and support in pushing this project forward, to the Publications Committee members who made this happen,to the authors who took much of their own time to make this a reality, and, of course, to Ron Kovac, Ph.D., from Ball State University, who served as editor-in-chief of this undertaking.

I would like to thank Verizon for their generous support in underwriting the expense of this version of the book.

Last but not least, I would like to thank Pat Scott, the ACUTA Communications Manager, for her efforts in keeping everyone on task. She is truly one of the most dedicated professionals that I have ever had the pleasure to work with.

Perhaps in another 10 years we can sit down once again and look back at all that has happened and may happen. Until then, we hope that you will find the information presented here both beneficial and enlightening.

Walt Magnussen, Ph.D.
Director for Telecommunications, Texas A&M University
ACUTA President-Elect 2006-2007
Chair, ACUTA Publications Committee, 2005-2006

Preface

The following book was written with one purpose in mind; To help ICT personnel in higher education solve their problems. To do this we realized that what must first happen is for personnel in this field to be brought up to a certain base level of knowledge. This is the starting point for this book—to provide a comprehensive overview of the ICT issues and areas in higher education. For beginning personnel in this field, there is a large learning curve, and the whole book will be of merit to their career success. For seasoned personnel in this field, there is always more learning to be done, and certain chapters within will assist you.

Unlike many of the books in the ICT field, this book looks at how technology, business, human factors, and the regulatory environment have blended. There are certainly enough books published that concentrate on each of these fields, especially technology, but not enough that wrap it together into a well-thought-out management perspective. Don't fear this book, as it is not a technically complex book but one that uses technology to solve problems.

An additional unique aspect of this book is from the environment of colleges and universities in the United States. In the ACUTA tradition and mission, this book was written to help ICT personnel who work for colleges and universities. This is one of the strong assets of this book, as all the authors, case studies, examples and situations are taken from colleges and universities. Certainly higher education has unique problems and situations they must deal with, and this book does an excellent job of portraying those unique situations.

For beginning staff members in the ICT field, we strongly suggest you read this book fully to gain a scope for the various functions of ICT within your college or university. Although each staff member may not deal with all the areas of this book, each staff member must understand the whole in order to be fully productive. For the seasoned professional, this book can help to reinforce your understanding while also providing a quick encapsulation of areas that one doesn't normally deal with. Whatever your background or seasoning in the ICT field, we hope that this book provides a unique perspective and helps you to solve the dilemmas and problems that you run across in your position. Enjoy and use the information within.

Ron J. Kovac, Ph.D., Editor
Professor/Consultant
Center for Information and Communication Sciences, Ball State University
Chair, ACUTA Publications Committee, 2006-2007

CHAPTER 1

The Technology Landscape: Historical Overview

Walt Magnussen, Ph.D.

Walt Magnussen, Ph.D., is the Director of Telecommunications at Texas A&M University. In addition to serving as 2007-08 President of ACUTA, he co-chairs the VoIP SIG for Internet2; directs the Internet2 Technology Evaluation Center (ITEC), a VoIP Research Center at Texas A&M University; and chairs the Operational Subcommittee for the State of Texas Telecommunications Planning and Oversight Council (TPOC). He has his bachelors and masters degrees from the University of Minnesota and his Ph.D. from Texas A&M University.

■ General Review

The Only Constant Is Change

In the past 10 years, we have seen our niche in the campus change in a fashion that is more revolutionary than evolutionary. We have gone through a metamorphosis from being the telephone department that supported plain old telephone service (POTS) to being a part of the information technology department, supporting a wide range of collaborative communications applications. At the same time, the way in which we are viewed has migrated from that of a utility to more of a strategic resource.

This metamorphosis is driven partially by technological change and partially by regulatory change but mostly by changing demands placed upon us by the students, faculty, staff, and administration of the campuses we represent. Services that we support are required in the delivery of distance education, research collaboration, information sharing, and entertainment. The importance of what we do is attested to by the fact that at most of our institutions, the chief information officer (CIO) has been elevated to a vice president position.

Many of us in the industry started out providing only dialtone and long-distance services. Today, in many cases, our service portfolios include not only the traditional services but also cable television services (including pay-per-view), cellular services (voice, data, and video), two-way radio systems, card-access systems (including biometric), off-campus broadband (e.g., DSL and cable modem), energy-management communications systems, wireless data communi-

cations, music-sharing services, video and audio streaming (iPod servers), Web sharing, and a host of other services. Whereas a decade ago, many of these each required their own network, today they are all migrating to IP- or network-based transport.

Faculty, students, and researchers who are recruited to our campuses arrive with high expectations. Ten years ago, only the telephone network was expected to be available 99.999 percent of the time (called "five nines reliability"). Now, all services are expected to come close to the same level of reliability. Our departments are typically among the first to be called onto the scene any time there is an emergency, and the planning of all new facilities involves significant involvement from our offices. We are no longer an afterthought.

This elevation in status does not, however, come without a cost: The systems that we maintain require an increased level in technological expertise. The rapid change in technology often makes our systems obsolete even before we have amortized them. The regulatory environment in which we operate is very confusing and vague. And we are often asked to do more and more but with the same amount of resources. Fortunately, there are organizations, such as ACUTA and others, that let us share resources, knowledge, and, in times of crisis, even staff with one another. The hurricane season of 2005 was a testimony to this fact.

Recurring Themes and Trends in University Telecommunications

The students we support represent some of the brightest and sharpest minds in the world, which is a mixed blessing. As a result, some of the services we deal with (telephones and cable television in dorms) are planned and delivered by our offices, while others (peer-to-peer music and rogue wireless WiFi access points in dorms) require that we react to them. Regardless of the case, the open nature of academic institutions that has become a part of our history will ensure that we will always be on the leading edge of technology.

The one certainty for communications in higher education is that nothing is forever. Our campuses went through a time when the only telephones present in the dorms were in the common areas. Then we were asked to provide a telephone in each room. In recent years, we have been removing these individual phones as students replace them with cellular telephones. The story was the same with student long distance. On the data side, we wired dumb terminal centers, then replaced them with microcomputer centers, which are now being replaced with wireless access for student-owned laptops anywhere on campus. Many of the services that are being provided today were not even thought of 10 years ago, and it is almost certain that the next 10 years will bring even more change.

The way professors teach is a large part of what is pushing technological changes on campus. One recent trend is the development of multimedia-enabled

classrooms. Chalkboards have been replaced with podiums that include control panels allowing for access to DVD players, laptop displays, cable television access, and even lighting control. Student desks are often provided with electric power for laptop computers. And, of course, everything is equipped with high-speed wireless Internet access. Often, students can watch the lecture live in the classroom, from their laptops on their broadband connections at home, or streamed late that night after work.

The delivery of services has almost gone entirely online as well. Life on campus for the student used to involve waiting in line to register for class, waiting in line to fill out financial aid forms, and going to the library to check out a journal to write a paper that they then printed up and handed to a professor. Now all of these transactions are delivered over communications networks anywhere and anytime that is convenient for the student. The delivery of Web-based services has not only made life easier for the student, but it has also provided significant savings in hours for the staff who deliver these services.

Business Aspects Important to University Telecom

The business aspect of what we do continues to be complex. As communications becomes more critical, a larger percentage of our institution's budget is dedicated to what we do. Typically, our staffing levels are increasing faster than most other departments on campus, our bandwidth requirements are growing at a rate that doubles almost every 24 months, and technology is being made obsolete every 3 or 4 years by rapidly improving standards and capabilities.

One business skill that is important to today's communications professional is the ability to forecast industry directions and customer needs. Many of the services we provide are contracted out to service providers that provide financial incentives for long-term contracts. Although this may be beneficial if the price of services goes up, the costs of many of the services that we purchase are actually being driven down by competition. In some cases, services that we are obligated to because of long-term contracts could become obsolete if technology provides a better way of doing things. To make forecasting even more difficult, in general, competition has been driving prices downward, but there is now a fear that recent mergers and acquisitions may reverse that trend.

A second important skill is the ability to accurately partition the costs of service components and establish a cost-recovery system that allows each component to stand alone. This can be difficult when many of the components are closely related. There has been a tendency in our industry to allow cost components to subsidize each other. With the rapid amount of change discussed earlier, however, it is possible that the subsidizing service component could be replaced by some other technology (e.g., long-distance resale in the dorms being

replaced by cellular telephones), which creates a funding deficit for the subsidized service.

■ Current Factors

Current Business Initiatives

When EDUCAUSE, a professional association of higher-education CIOs, released its 2006 survey of the top 10 issues facing campus technology professionals, six were directly and four indirectly related to what we do. The six issues directly related (show here with their position in the top 10) are

1. Security and identity management
2. IT funding
4. Disaster recovery/business continuity
6. Infrastructure
7. Strategic planning
8. Governance, organization, and leadership

Two of these deserve special comment. The second issue on this list, IT funding, begs one of the larger issues we face: determining the right combination of insourcing, out-tasking, and outsourcing. As the services that we are expected to deliver become not only more numerous but also more diverse, it becomes increasingly difficult for our own staff alone to provide support. This has resulted in an increased dependency on out-tasking (having business partners deliver a component of a specific service) and outsourcing (depending on the business partner to provide the entire service). The result is that we are more dependent on our vendors to provide the services that our customers demand. The good news is that vendors have stepped up to the plate with the advent of business-to-business (B2B) applications. Examples include Web portals that allow our customer-service representatives to enter and track their own orders in the vendor's order-entry systems and online billing systems that allow our accounting departments to look at bills online in real time.

Another issue that affects us significantly is the eighth item on the EDUCAUSE list, which includes organization. The convergence of services has changed where we report (formerly to business services or utilities departments, now to IT departments) and how we are funded (or what we fund). This impact is clearly evident in ACUTA membership, which has migrated from an organization of *telecommunications* professionals in 1995, when the previous edition of this book was written, to an organization of *communications technology* professionals today. As this shift indicates, the industry's focus has evolved from

telecommunications to communications technology that includes voice, data, and video.

Brief Statistics: What Has Changed and by How Much?

It is not only communications within higher education that is changing, but also the nature of higher education itself. These changes include a rapid increase in enrollment, more emphasis on distance education, and a desired change in the degree programs.

The U.S. Department of Education predicts an increase in higher-education enrollment from 17.3 million students in 2004 to 19.9 million students in 2015 (http://nces.ed.gov/pubs2006/2006084.pdf). Although a 19 percent increase may not seem overwhelming, we must put this number in perspective. The largest universities in the United States today have an average enrollment of about 50,000 students. The projected increase of 2.6 million students would be the same as adding another 52 of our largest institutions. The impact upon the basic infrastructure of adding 2.6 million students is staggering.

Another study by the U.S. Department of Education (http://nces.ed.gov/surveys/peqis/publications/2000013/#seven) showed that the number of distance-education courses taken had doubled between 1995 and 1997. Assuming that this trend either continues or accelerates, universities' dependence upon brick and mortar will decrease, and their dependence on communications technology will increase.

A third study and subsequent book titled *The Gathering Storm* makes a convincing argument that the future of the U.S. economy has become dependent upon having the most-educated workforce in the world. The study reports that about 85 percent of our current increase in GNP is due to technological changes. The unfortunate reality is that we are falling behind in the critical areas of science and engineering. Our once-staggering lead in math and science has diminished as other countries continue to graduate many more students in these areas than does the United States. The study also reports that only 6 percent of Americans are currently enrolled in engineering-related fields, whereas Europe has 12 percent enrollment; Singapore, 20 percent; and China, 40 percent. The study argues that the United States will need to significantly increase our enrollment in science and engineering, which are typically more dependent upon technology than other programs, if we are to maintain our global leadership position.

Regulatory and Legal Issues and Actions

The regulatory and legal environment in which we currently exist can best be described as confusing. In the history of telecommunications, three actions have

made a significant change in the way we all communicate: the FCC act of 1932, the Modified Final Judgment of 1982, and the 1996 Federal Telecommunications Act. This last act promised to provide competition in the local loop by allowing facilities resellers (competitive local exchange carriers, or CLECs) to enter the market by unbundling services (requiring the owners of facilities to sell service components rather than the full service). It pushed for the deployment of wireless services, and it provided incentives for the incumbent local exchange carriers (ILECs) to open up their markets to competitors. A decade into the process, what has actually occurred is that unbundling of advanced services (such as ADSL broadband) has gone by the wayside, wireless technology has proven to be costly to deploy, and ILEC mergers have reduced the number of service providers. All of this is causing legislators to consider yet another major rewrite. These sorts of changes make long-term strategic planning difficult yet necessary.

Other significant regulatory issues include the following:

- Recording Industry Association of America (RIAA) actions: The 1990s brought about technology that allowed students to share music and movies with each other using peer-to-peer technology that runs over the Internet. This sharing is considered to be a violation of copyright law if done without the artist's permission. Universities are expected to monitor and limit these activities and to provide the names of students involved if there are violations of these laws.

- Universal Service Fund: In 1932, the Federal Communications Act established the concept of universal service, the premise of which was that everyone would have access to basic communication services, regardless of the cost of serving an area. Initially, this subsidy was provided by urban subsidizing rural areas and long-distance subsidizing local services. With the advent of competition and technology changes, however, the federal government is forced to look for other ways of funding the ever-increasing Universal Service Fund.

- Converged services: Until a relatively short while ago, cable television companies were responsible for providing entertainment television services, and telephone companies provided dialtone. Although more recently there has been competition over who should be the Internet service provider, the two operated under completely different sets of regulatory rules. Today, telephone companies are adding entertainment television to their dialtone and Internet offerings, while cable companies are beginning to roll out voice over IP (VoIP) on their existing Internet and entertainment television services. These converged services—or the triple play (voice, data, and video), as they have become known—are breaking many of the regulatory processes that currently exist. It is quite likely that additional legislation will be required to address the major issues brought about by convergence, including franchising cable television offerings at either the state or the federal level (they are currently franchised at the local level); determining

which services have to pay which fees, such as the Universal Service Fund; and determining who sets 911 delivery policy (it is currently set at the state level for landline and cellular, but at the federal level for VoIP).

- Net neutrality: This issue involves the ability of a service provider (ISP or carrier) to be able to charge a separate fee for information providers (such as universities) that provide large amounts of content that require special treatment to work well, such as streaming video.

These issues and others will be discussed in more detail in subsequent chapters.

■ Trends and Issues

Unique Issues Facing Telecom

Telecommunications services have become a strategic resource at colleges and universities today. Students expect advanced services in the classrooms, in the dorms, and at the libraries and cafeterias. In other words, anywhere, anytime high-speed broadband Internet access is demanded—not just expected—on campuses. Three areas that make this a challenge to achieve are (1) rapid change in the technology that delivers these services, (2) constant change in service providers, and (3) increasing importance of security.

1. Rapid change in the technology that delivers these services. The speeds and feeds that are required to keep up with the ever-increasing demand for service force obsolescence of our technology. From the basic infrastructure, such as the copper and fiber, to the transmission equipment, large investments are typically only lasting from 4 to 10 years. Many campuses invested millions of dollars in multimode fiber-optic cable plant, only to overlay the plant with single-mode fiber in order to support speeds in excess of 1 gigabit (1 billion bits per second). We delivered Category 5 cable plant to the desktop (or bed), only to replace it with Category 6 or 7. And we finished up the IEEE 802.11b wireless deployments just in time to start planning the 11a and 11g deployments. We replaced Ethernet hubs with basic Ethernet switches, only to find out that we would need advanced Ethernet switches that support separate VLANs, traffic prioritization, and power for VoIP devices. Our wide-area ATM and SONET-based infrastructure was replaced by MPLS and Ethernet-based devices, and so on. The result of all of this is that our service costing models now have a significant capital replacement component in order to keep up with the rapid change.

2. Constant change in service providers. The 1996 Telecommunications Act promised more competition in telecommunications. This competition was going to come from resale of services, intermodal competition (e.g., a telephone

company competing with a cable company), and new facility-based companies (e.g., wireless delivery). Although there were early success stories, the early 2000s saw many failures not only of newly established firms but also of many larger, older firms that were either in bankruptcy or facing it. At the 10th anniversary of the 1996 act, we saw mergers and acquisitions at an unprecedented rate. SBC had merged with AT&T and was in the process of bringing in BellSouth. Verizon had merged with MCI; Level3, with Wiltel; and there were others. In the wireless arena, we have gone from seven major national carriers to three. The positive aspect of these mergers is that the merged forces are financially stable and are able to offer services that are more diverse than those offered premerger. The potential downside is that the reduced competition may have a tendency to drive prices up, although this remains to be seen.

3. Increasing importance of security. Due to many unfortunate incidents in recent years, we have been forced to secure our networks at unprecedented levels. Academia has traditionally been wide open. That openness is a part of the freedom-of-thought process that makes our institutions the envy of the world. The advent of denial-of-service attacks, identity theft, spam, and other disruptive activities have forced us to secure our wireless infrastructure, thus increasing the complexity of connecting; install fire walls, which are costly to manage; and install spam filters, which eliminate undesired e-mail but also slow down desired e-mail and virtual private networks (VPNs) that authenticate and encrypt traffic from off campus but add overhead and reduce throughput. It appears that the direction for most campuses is toward an identity-management system—you log onto the network, and it knows who you are and where you are at all times. Although this resembles the "Big Brother" vision of the future, it may be required not only to meet future law enforcement requirements but also to protect our networks enough so that students, faculty, and staff can work in a safe and secure manner.

International Issues that May Have Impact

Just as our economy has become a global one, our education system has also become global. International education and research have provided both challenges and opportunities in the communications fields. Many universities have established branch campuses in other countries, have sent visiting lecturers and researchers to work with faculty at other schools, and have invited researchers and faculty to visit their schools. There have been three ways in which our field has helped facilitate this:

1. Wireless communications: With the advent of international standards in the wireless space, it is now common for faculty to use their same cellular instrument and telephone number while traveling on any continent. GSM and other similar

services, in conjunction with solid international roaming agreements, have made travel much easier than in the past.

2. International broadband access: Once office or faculty members arrive in a foreign country, they will likely find that a reasonable broadband access line is available. In fact, broadband is more likely to be available in other parts of the world than in the United States. A 2004 study by the International Telecommunication Union (ITU) (www.itu.int/ITU-D/ict/statistics/at_glance/top20_broad_2004.html) placed the United States at 16th in the world in terms of broadband penetration, with about 12 percent deployment. This is about half of the 24 percent for the Republic of Korea and 22 percent for the Republic of China.

3. International research networks: A third contributing factor to the globalization of education is international research networks like Internet2. Over the past 10 years, higher-education institutions have worked together to build the Internet2 network—a 10-gigabit network with connections in Europe, Asia, and North America, as well as a significance in South America. This network provides links for videoconferencing, VoIP, and other collaborative applications, making communicating with much of the world no more or less complicated than communicating with a neighboring university.

■ Summary: What Is Our Role Today?

As mentioned, communications and IT in general have become strategic resources for most of our higher-learning institutions. In effect, we are the enablers of education. We are uniquely positioned to take advantage of new and emerging technologies, but we are also in a position to help direct what new technologies will be used tomorrow. By working closely with faculty who are researching next-generation technologies, participating in standards-setting groups, and working with our future engineers (today's students), we can have an impact on the new and exciting advancements that our children and grandchildren will one day experience.

CHAPTER 2

Emerging Trends and Technologies

Joanne Kossuth

Joanne is currently the CIO and Associate Vice President for Development at the F.W. Olin College of Engineering. She has been associated with the college since its startup in 1999. Joanne is also the current Chair of the NERCOMP (North East Regional Computer Program) Board and serves on the Educause Program Committee. She has a B.S. in Pyschology from College of the Holy Cross and an M.S. in Management froom Lesley University.

Telecommunications networks used to be described as simply a data network or a phone network. Today's telecommunications network is much more complex and pervasive. Network-based applications such as e-mail, instant messaging (IM), video, and VoIP refer to a communications network, not simply a voice or data network. As technology continues to increase in speed, diversity, and convergence of devices, which trends will have an even more intense impact as we move into the future?

Trends

Prosumerism

One new trend is often referred to as "prosumerism." Today, many high-tech products that at one time would have debuted in the workplace are now first introduced into the home or recreational levels by tech-savvy consumers. These consumers then bring the technology to the workplace, where they demonstrate to colleagues how it has a positive impact on both their productivity and the quality of their work. These employees are driving the adoption of technology in the workplace, as opposed to the workplace driving technology requirements.

One factor in the adoption of technology is the expectation of employees that connectivity will be ubiquitous and will involve a variety of devices (of their personal choice) that can handle multiple types of media and provide instantaneous communication one-to-one, one-to-many, or many-to-one. Examples of these devices include cell phones, personal digital assistants (PDAs), personal DVD players, and combination devices, such as cell phone cameras. The commonalities of the devices are that they are all inexpensive, personalized, and advertised as secure.[1]

The proliferation of these devices necessitates discussion of a number of issues that have a significant impact on the enterprise's operation. Both the increasing speed of product obsolescence and the level of customer expectations lead the list of issues. Interoperability concerns (or standards)—along with human factors, such as interface design—are becoming increasingly important as individuals, rather than institutions, decide which device to buy and which type of service plan to execute. Privacy and security concerns surrounding the physical devices, as well as the data, are popular topics of conversation for just about everyone. The one thing that seems certain is that managing these aspects of technology will not get any easier for quite a while. Legislative and governance complexities, along with the lack of standards and the ongoing mergers and acquisitions/consolidations, dictate that the telecommunications environment will remain increasingly complex and volatile.

Convergence

Multiple definitions of *convergence* abound. Convergence can be defined in terms of services, hardware, networks, and even points of view. In terms of technology, the convergence of multiple services over one network is a trend that is accelerating. Cabling for one network, operating one network, decreasing the complexity and number of skill sets required to run the network, and increasing service and reliability are just some of the reasons for this trend.

Many institutions are running voice, video, data, building controls, security and surveillance, cable television (CATV), and music over one network infrastructure. The ability to run multilayered services on one network requires that the equipment be capable of providing quality-of-service (QoS) designations. One way to handle QoS is to tag traffic differently and to then use those tags to prioritize the traffic. For instance, voice can be prioritized to always go through, video second, and data third, based on the requirements of the packet transfers and the impact on the end user. For example, audio is a very sensitive area. If there is any "jitter" in the phone conversation or words get scrambled or dropped, then the user is much more likely to have an unsatisfactory experience than someone sending data in which packets have to be resent and recompiled and resent again, but still end up in their entirety at their appropriate destination.

Another important consideration in converged networks is the virtual local area network (VLAN). A VLAN, or virtual LAN, is a local area network (LAN) with a definition that maps workstations on a basis other than geographic location (for example, by department, type of user, or primary application). The mapping is often based on application or use—such as a VoIP VLAN, building security VLAN, video VLAN, or chemistry department VLAN—to provide more granular management and application of policies. As more and more services run

over one network infrastructure, the separation and manageability—and thus the security—of the various services and access to them can be provided within the same device, minimizing both hardware and support costs.

The convergence of devices, concurrent with a drop in prices and the continuing miniaturization of components, provides consumers and businesses with intriguing combinations of services. For example, DVD players support CDs and MP3s. Binoculars have zoom lenses, act as digital cameras, and have slots for memory cards. Cell phones double as cameras, MP3 players, calendars/PDAs, and e-mail devices. Home computers now run the family entertainment network, which connects to VCRs, DVD players, stereos, and CATV and allows for storage on a PC or another device for later playback and/or personalization of content via editing or other augmentation.

Session initiation protocol (SIP) and personalization devices, such as the MCS 5100 by Nortel, allow for integration of corporate IM, live chat, videoconferencing, shared files, and whiteboards, as well as routing of calls to various devices (PC, cell phone, home phone, VoIP device) based on the caller's identity and role. Bluetooth, a personal area communication protocol, integrates with wireless to transmit data within 30 feet and beyond via other device connections. For example, Bluetooth headsets are often used with cell phones and/or allowing various appliances to share information. Who knows what will be next. What we do know is that the trends of convergence of services, miniaturization, increasing speed and functionality for less cost, and emergence of nanotechnologies will strain our imaginations.

Mobility

Along with the convergence of network hardware and services and the increasing pervasiveness and drive into the workforce of personalized technologies, mobility is an evolving trend. Mobility refers to the ability to work or play anytime, anywhere, anyhow. Implied in mobility is continuous access to a set of resources. That set of resources might comprise network applications, local or remote files, collaborative institutional documents and tools, archived e-mail, or digitized, copyrighted content.

The form factor for mobility is still a work in progress, although the cell phone seems to be leading the race. Some refer to laptops as portable and cell phones and PDAs as truly mobile. This debate over form factor will continue, however, as laptops get smaller and lighter, tablets evolve, and cell phones and PDAs support pocket versions of Microsoft Office and sport expandable or slideable keyboards.

One thing that is clear is that the push for mobility has increased the reach of the enterprise and drives the use of VPNs, which provide an encrypted connection between the device in use and the network on which the resources reside. VPNs require the installation and support of platform-specific software (Macintosh, Microsoft, and Linux). In addition, VPN connections have an overhead due to encryption and the sending and acknowledgment of packets. These issues have led to an increase in the sale of secure socket layer (SSL) VPNs, which are clientless, are run through a Web browser using https, and are thought of as being easier to support (no software to install), usable on any Web-enabled device, and less affected by overhead. However, overhead can become an issue, even with SSL VPNs, when there is a large amount of traffic. This traffic can be mitigated by the use of an SSL accelerator, which off-loads the SSL traffic to a stand-alone device (though some switches and routers are now building these capabilities onto blades in these devices) to speed up the connections and the transactions.

Wireless Technologies

Of course, mobility would not be the overarching trend it is today without the development of the wireless spectrum in the local area network (LAN), metropolitan area network (MAN), and wide area network (WAN) space. Both higher-education and corporate campuses are deploying wireless technologies at an amazing rate. But even this rate is not quick enough for many constituent groups who deploy their own access points and routers and who have the potential to disrupt network services such as DHCP and DNS.

Wireless technologies are continuing to develop, including the advent of thin access points that are connected to switches (and that are soon to be integrated into the switches in wiring closets through blades for wireless services). These switches provide centralized management, policy development, authentication, and other standard network services typically associated with switched equipment. Wireless products also come equipped with sophisticated planning and deployment tools to determine the best coverage. Wireless mesh networks, such as those deployed by Nortel, the University of Arkansas, and MIT, provide for outside access points to create a mesh network by communicating with each other, providing redundant and self-healing routes, and so on. Point-to-point wireless (line of sight) is used to connect building-to-building on campuses and, in some cases, campus-to-campus, providing relatively inexpensive connectivity where funding prevented it in the past.

As more services move onto the wireless LAN, quality of service becomes a particular challenge, especially where the wireless traffic crosses the wired Ethernet infrastructure. One popular approach is to deploy multiband network

infrastructure, setting aside the 5 GHz 802.11a spectrum for critical data applications and the 2.4 GHz 802.11b spectrum for voice applications. In the meantime, IEEE is supporting the enhancement of various standards with QoS support (802.11 standard), and the WiFi Alliance has released its WiFi Multimedia (WMM) specification. Until the standards are accepted, however, the best protection for scalability is to design the wireless network with a multiband structure and a dense deployment of access points.[2]

Soon to come in the wireless space is the potential for other self-like seeking, routing, and healing devices and systems. One example of this concept are airplanes that identify themselves, communicate continuously, update each other, and thus reduce the reliance on air traffic control systems.

Peer-to-peer technologies and connections that allow for on-the-fly sharing of resources without centralized service support is another application of smart, self-seeking technologies. Although security and copyright concerns abound with regard to technologies such as Napster, Limestone, and others, these technologies are flourishing. Other peer-to-peer sharing technologies utilize unused CPU cycles to create grids where job tasks can be shared and results compiled in less time than the work of one supercomputer.

The next generation of wireless services is already here. WiMAX is a standards-based technology that provides high-throughput broadband connections over long distances. Typical uses include "last mile" broadband connectivity, hotspots and cellular backhaul, and high-speed connectivity for business. Although the cost is still on the expensive side, this technology presents a viable alternative to DSL and perhaps 3G. WiMAX is seen as true wide-area wireless that combines cell phones with WiFi speeds, enabling all sorts of services currently tied to local area networks.[3]

3G systems provide access via one or more radio links to a range of telecommunication services that are supported by fixed telecommunication networks. [4] Other mobile-specific services, as well as a range of mobile device types for fixed or mobile use, may also be supported. These can all be linked to terrestrial- and/or satellite-based networks. Vendors such as Verizon[5], Cingular[6], and Sprint[7] currently offer such services. 3G provides throughput of 200–500 kbps and is on a road map for 1 Mbps.[8]

Another area of next-generation wireless systems set to emerge is that of VoIP over WiFi (802.11b, a, g). VoIP handheld devices are the result of partnerships between network companies, such as Nortel and Cisco, and handset manufacturers, such as Nokia and Motorola. These devices can currently handle voice over

the wireless IP network. The next challenge is for these devices to be handed off to carriers such as Verizon, SMC, and other local telephone companies so that the devices can take advantage of carrier networks, be they CDMA, GSM, or IP.

Outsourcing

As technology demands increase the breadth of the portfolio that must be managed, the trend of selective outsourcing and using managed service providers is on the rise. What types of services are being outsourced? Security, network management, help desk, and application development are just a few.

According to Gartner (a research and IT consulting company), managed security services is one of the fastest-growing segments of the security marketplace. In 2002, Gartner reported that by 2005, 60 percent of enterprises would outsource the monitoring of at least one network boundary security technology.[9] Other services that will follow once relationships are established around boundary security will likely be VPN and firewall management, vulnerability scanning and intrusion detection, and security monitoring and response. Because authentication and identity management are truly the "keys to the kingdom," they are likely to remain in house until a much later date.

The two major drivers of the outsourcing trend are cost and staffing. Managed security services can typically spread investments in analysts, equipment, and facilities over a number of clients and a period of time, thus reducing cost per client. In addition, there is a shortage of qualified information security personnel, which raises the costs of recruitment, compensation, and retention. This shortage cycles back to the companies, requiring from them a very high initial investment in security—thus enhancing their appreciation of an outsourced solution.[10]

Network management is another area in which outsourcing is making inroads. While outsourcing, in general, has received a great deal of press with regard to larger corporations, network management outsourcing has been growing, particularly among midsized companies. These companies do not usually have the IT resources available to continually optimize and update their network applications. Due to the demands of growing the business, these same companies do not have the funding to dedicate to maintaining a competitive, cutting-edged technology infrastructure.

The major stumbling block for many midsized companies is the loss of control and visibility with regard to their infrastructure. As a solution to this, outsourced firms are now providing for this knowledge management and

accountability through tools such as real-time reporting and management. This adaptability has increased their success in the midsized market.[11]

One example of a successful outsource is at Los Angeles–based AECOM (Architecture, Engineering, Consulting, Operations, and Maintenance) Services Group. By company mandate, the one-person network team was not going to grow. The only way to keep expanding and supporting the network in order to support the 17,000 employees and multiple worldwide subsidiaries was to outsource network management and other tasks.[12]

Any successful outsourcing takes into account the vendor's stability and track record. It is necessary to investigate the outsourcer's ability to provide incident assessment and response, whether the topic is security or network management. Another important area to understand is how the outsourced functions integrate into broader IT management systems and facilitate the operation of the overall IT operation.

Experts believe that the potential pitfalls of outsourcing network management center around "naive expectations that the outsourcer will automatically solve all of your problems. Clearly understand your requirements of the outsourcer and its capabilities, and be very explicit about them. Negotiation of the terms and conditions of the outsourcing agreement will be crucial."[13] Given the escalating trend of selective outsourcing of higher-level tasks, setting the correct expectations and understanding the management of risks are two important skill sets for technologists as we move into the future.

The help desk was one of the first areas to experience the outsourcing phenomenon. Ciber[14] is one example of a company that specializes in this area. A major driver of this trend is the cost of recruiting, training, and retaining staff, especially as the scope of IT application support has grown to encompass all areas of a business. Because specialists tend to be more expensive than generalists, one track is to outsource common application support, such as Microsoft Office applications, while another is to outsource specialized application support. Yet another is to outsource the entire help desk support operation.

The outsourcing of application development has been in place for some time. Case study examples can be found at http://pm.ittoolbox.com/documents/document.asp?i=768. A major driver in this area of outsourcing relates to specialized skill set requirements for shorter periods of time or more diverse skill sets at a reduced cost.

Regardless of the specific tasks that are outsourced, a number of areas need attention for the partnership to run smoothly. These include establishing relevant metrics for customer satisfaction that are meaningful and actionable; reexamin-

ing all parameters of the relationship and developing plans on at least an annual basis; understanding typical attrition levels to keep churn to a minimum; maintaining flexibility; and establishing a seat at the table with the service provider so there are no surprises, since your customer is still your customer.[15]

Web Services

As employers have looked to IT to do more with less, another major trend involves Web services, particularly self-service variations, such as online registration and bill-paying. Web services are characterized by an easy-to-use interface, intuitive icons, and an ability to track every transaction from start to finish, anytime or anywhere. Amazon.com is a pioneer in this field. From their tabbed search tools to their shopping carts and account management to their e-mail updates and tracking interfaces, Amazon has made shopping online fast, efficient, and simple.

A number of factors are driving the Web services paradigm into all aspects of business, including education, banking, healthcare, benefits, and investments. These factors include enhanced 24/7/365 availability of services, reduced cost of support personnel, the ability to collect immediate feedback and tailor end-user experiences to better meet customer needs, and the ability to integrate synchronous chat and even videoconference capabilities with these services.

In higher education, self-service manifests itself in integrated, one-stop-shopping student service centers, as well as in Web-based portals that provide services based on the role(s) of the person accessing the information. For example, candidates for admission have different needs for information than do staff, faculty, current students, or alumni. For each of these constituencies, the ability to personalize the information and to easily search for relevant information is extremely critical. Candidates want to know what campus life is like for students. Students need to be able to register; view schedules, grades, transcripts, and bills; submit coursework; and dynamically interact with their peers and colleagues. Faculty need to be able to advise students, submit grades, view transcripts, host synchronous chats and asynchronous discussion threads, and quickly disseminate information to their students. Alumni need to stay in touch with the institution, make donations, purchase college-branded merchandise, and keep in touch with classmates. Staff need to be able to check the status of their last paycheck, update benefit information, work with budget and actual financial information, change their personal information, and disseminate information to colleagues at other institutions.

Implementations have demonstrated that to make the Web services offered by portals the first place that various constituencies go for information, additional

daily-use services, such as e-mail, calendaring, contact management, weather, and stock links, must be integrated into these offerings. This is especially true for portals that link to course management systems. Course management systems provide access to syllabi, office hours, assignments, and content that complements the textbooks (course cartridges) as well as specific faculty-developed content (e.g., learning objects). Some institutions have developed their course management systems to such an extent that faculty host online courses and degree programs through the use of both synchronous and asynchronous tools, such as live video feeds and archived PowerPoint presentations.

Another driving force in the provision of Web services is the quest to derive business intelligence from all the data that are collected on a regular basis. In this quest, data are often collected to help determine the alignment of IT with the goals of the business, institution, or company. Among the methods used to collect this information are feedback forms, surveys and polls, and tracking such webpage statistics as browser used, page hit, page rehit, and length of time spent on each page/item/visit.

This type of data collection results in rapidly increasing storage and reporting requirements. In addition, in the corporate sphere, the activity in mergers and acquisitions is creating pedabytes of information that must be turned into useful knowledge about the new entity. In higher education, the growing body of online collaborative knowledge and the increasingly transitory nature of the student population are creating similar requirements.

In all of these examples, the vast majority of employees and other constituency groups are not familiar with query-based reporting tools such as Crystal Reports and Cognos. In addition, in many instances, these groups are using mobile, small form factor devices that are not friendly to large displays of data. Therefore, tools such as data marts and dashboards are increasing in popularity, because they provide high-level, easily readable, easily identifiable information that can quickly be viewed at the portal or other Web interface.

This level of transparency of data and large scope of dissemination requires that databases be well protected in terms of security and access policies. It also requires that security be considered and built into all levels of portable and mobile devices to the extent possible. Finally, training of all users of mission-critical data needs to focus on safe, secure use of these handy, time-efficient tools. Accountability in the form of continuous audits and verifications of equipment, as well as audits of access to information, are musts in this day and age of federal and state oversight and regulation.

Digitalization

Online courses take advantage of another current trend—digitalization. Digitalization refers to the process of putting paper and text into electronic formats both for purposes of archiving and for ease of access and dissemination. Many institutions that do not currently offer online courses still take advantage of digitalization for e-reserves (setting aside documents or texts for specific courses, which formerly required students to travel to the library to obtain the information or to use an interlibrary loan process) or for accessing online journals in electronic—as opposed to print—format. This system reduces the space requirement for libraries and provides access for all types of remote constituencies, such as faculty on leave, commuting students, and others. As a side note, the majority of this type of access requires that VPNs (a trend that was discussed previously) be in place to verify the legitimacy of access to online resources and to comply with the current licensing requirements that are based on valid IP address ranges.

More and more content is being put into electronic format, as demonstrated by the arrangement between Google and Stanford University, Harvard University, the University of Michigan, the University of Oxford, and the New York Public Library to make millions of books from their collections electronically available.[16] The challenge becomes one of content and knowledge management. The correct tagging of metadata and input of search keywords is critical to the success of any digitalization project. For content to be used effectively, the end users must be able to find applicable content quickly and efficiently. End users must also be educated about or literate in the origins of the information and the degree of reliability they should place on the information. They should also understand how to acknowledge the material in their own works.

Content and knowledge management is also applicable to the information created, collected, and stored at each individual institution. Numerous systems, both proprietary and open source, have recently entered the market. Examples include CrownPeak, Interwoven, Google, Mindbridge, Percussion, Druple, and Ektron. Although the products are still young in terms of development, they offer useful tools that assist in managing the knowledge of higher-education institutions. Based on surveys and proposal experience, the following features are considered critical in any content management system:

- Web-based interface
- User-friendly editor
- Integration with Microsoft Office/Adobe/Macromedia
- Accessibility guidelines
- Links and link checking
- Navigation and usability

- Application speed
- Metadata, taxonomy, indexing, and search
- Extranet capabilities
- Personalization
- Image and multimedia file library
- Page preview
- Expiration of content
- Page history, version, archive, and restore controls[17]

Social Engineering

While there is a lot of noise about the "death of libraries as we know them" due to the influence of electronic resources, higher-education institutions are still building libraries as social and learning common spaces. These areas take on particular meaning as the higher-education community focuses on tools that encourage community, creativity, and collaboration. All of these tools depend on a network infrastructure—wired or wireless, though wireless is usually preferred due to its informal and ad hoc nature. The social engineering trend includes development of social networks such as Friendster (www.friendster.com), LiveJournal (www.livejournal.com), and Facebook (www.thefacebook.com). With these tools, participants register and provide information about themselves and who they know (friends). Their friends are then invited to join, and participants soon have many friends through their network of friends (e.g., "I know Joe. Joe knows you. So I know you." and so on).

Other collaborative tools, such as wikis (group-editable Web pages) and blogs, are primarily used for developing and supporting information that is useful to group work. These tools can also have a side social benefit. Wikis tend to be open-source tools (taking advantage of the younger generation's proficiency with PHP) and allow for the instantaneous posting of content. Additional content can then be contributed by anyone else. These tools allow users to log work as well as to back up recent versions, which provides cover for any instances of hacking or defacing that might take place. Popular examples of these collaborative tools include Moinmoin (http://moinmoin.wikiwikiweb.de), EditMe (www.editme.com), and TWiki (http://twiki.org). Colleges and universities are trying to capitalize on the social engineering trend by using wikis as a feedback mechanism for candidates and campus visitors or as a way for current students to communicate with potential applicants.

Blogging

Blogging, another recent trend, refers to writing an online journal or reflection of daily experiences. Blogs can be general or dedicated to a specific topic. A number of corporations are now attempting to capture the positive benefits of blogging by having one or more of their employees blog either about products or about the company in general to assist with the marketing effort. In these cases, the trick is to protect the company's valuable intellectual product and secrets while providing a better communication mechanism for customers.

Higher-education administrators are also attempting to take advantage of such a direct channel to the consumer. Students can blog about the college or university experience to attract applicants; admission counselors can blog about the admissions process and their experiences on the road; students can blog about semester/year-away experiences; campus experts can blog about their areas of research; and so on. Blogs are in addition to the now-standard whiteboards, chats, IM (texting), and discussion forums that are often included in course management systems and offered by most ISP packages.

Radio Frequency Identification

Radio frequency identification (RFID) is projected to break out in the coming months. As these radio tags become less expensive, they will work their way throughout the supply chain and reform it just as Amazon reformed online shopping. With radio tags scheduled to be adopted by Wal-Mart, which is insisting that their suppliers adopt them as well, the potential impact is huge. In higher education, RFID tags have been used for a while now to identify and manage library collections. *The Chronicle of Higher Education* reports that more than 300 libraries currently utilize RFID but are very careful to store the least amount of information possible on the tags for fear of privacy issues.[18]

As RFID adoption increases, the tags will change the way that fixed assets are tracked, research supplies are identified and managed, standard supplies are ordered and tracked, products are developed, research stages are identified and tracked, and more. In addition, these tags will make their way into our private lives (as well as auxiliary services) when they are used to track origin of and expiration dates on everything from food products, vaccinations, and medications to health records, vending products, and so on.

RFID will also allow for even more efficiencies in the product supply chain and for additional Web-based self-service productivity. For example, when you order an item online, the system will wirelessly communicate with the warehouse to determine whether product inventory is held. If the product is held, the tags will identify themselves such that the oldest-viable product will automatically be

placed on the belt to the shipping department, where it will gain additional information, such as the date shipped and a tracking number. That tracking number will then report itself every step of the way (via e-mail or another communication that you select) until it is at your doorstep. Once at your doorstep, the product will then function normally until the expiration date, at which time it will automatically notify you whether the product is still on your shelf. The obvious challenges of this system relate to the development of policies, procedures, and standards that can be accepted industries-wide in order to facilitate ubiquitous services.

Awareness and acceptance of RFID technology has been growing in the public sector.[19] RFID is beginning to make inroads in higher education in areas other then the library. For example, universities in China are using PicoTag labels for student identification cards. The primary reason for this RFID deployment is to prevent fraud, as China has a difficult time authenticating student ID cards. Railways, in particular, had an issue, since Chinese students are entitled to discounted train travel. RFID readers deployed at the nation's four main railway stations allow students to have their status quickly verified by means of the smart label attached to their ID card. According to Didier Serra, vice president of sales at Inside Contactless, which is based in Aix en Provence, France, the ID card's ISO 15693–compliant chip, which can hold up to 2 KB of data, operates at 13.56 MHz at a distance of up to 1.5 meters when read by a long-range reader and antenna. At present, the smart label stores only a student's identification data. The next step will be to store all the diploma and degree information on the tag.[20]

Cases of successful RFID implementations can be found in industry-specific journals and in the *RFID Journal.* Some examples include the following:

- Jacobi Medical Center's RFID-enabled patient ID system not only enhances patient care and staff working conditions, but it is also expected to save a million dollars per year.
- Hampton, a supplier of locks and lighting to Wal-Mart, deploys RFID "at minimal cost" and achieves such benefits as faster invoice payment and the ability to know which goods are lost or stolen.
- Hong Kong airport's RFID luggage-handling system is expected to lower labor costs, increase capacity, and improve security.
- El Paso County deployed RFID to keep tabs on its IT equipment. Due to the county's vast size, it expects to recoup its investment soon.[21]

■ What Can We Look for in the Future?

Looking at the technology landscape today and the steps that have brought us where we are, certain trends and directions seem inevitable.

- RFID and more RFID: As RFID tags get less expensive, the more information they can carry, the more they will be relied on to track everything from product to intellectual property to important personal papers. Start thinking about how your institution would handle this, and begin to build consensus around policy and procedure.
- The importance of identity management and federated identity as the push for hardware to become truly nomadic increases: Why shouldn't everyone have a profile that is stored in a central repository, and why couldn't that profile then be logged into any cell phone or PDA or laptop, even a borrowed one? Biometrics will continue to develop and will emerge as a viable tool for managing identity, particularly as more and more personally identifiable data is stored in large-scale databases to develop profiles. This will be core to developing the seamless, ubiquitous user experience of the next generation.
- An increasing focus on regulation and compliance as computer technologies infiltrate even more aspects of our lives: When a trend becomes large and there is potential revenue generation or potential privacy violation inherent in the technologies, the current tendency for action on the part of both state and federal government entities will not go away.
- The increasing importance of policies and standards as organizations and institutions adopt emerging technologies at a rapid pace: With the advent of prosumerism and the rapid pace of development, most pilots of various technologies are turning into deployments faster than you can say "1, 2, 3." Be prepared for this. Test and retest within your IT organization. Draft policies, standards, and procedures before the user pilot, or you will not have anything to fall back on when that superuser discovers a "really cool" application that you and your group had never thought of.
- More improvement in voice and handwriting recognition—especially in areas of scripting, graphics, equations, and multilingual vocabulary training—and in integration with digitalization—especially as tablets and their derivatives seek to attain greater market share: Breakout applications in healthcare and in some K–12 classroom applications are already driving these changes.
- A continued focus on security at all levels: The focus on the security of software, hardware, and devices will increase. Network hardware vendors, such as Nortel, are partnering with virus protection vendors, such as Symantec, to provide security that is built into chipsets for every product on their road map.

They are also partnering with IBM to research and develop these technologies into blade servers.

- The continuing improvement of human interface design: The major disappointment since the 1980s has been why intuitiveness has not yet been built into products, although we have seen increased use of robotics in everyday life. Consider examples such as the docking station-seeking Roomba to the robotics-enhanced prosthesis.

■ Surviving the Challenges

What is the significance of these trends for the communications technology professional? The main significance is that yet another trend is emerging: the development of the consummate technology professional. Technological skills are no longer sufficient requirements for success in an IT career. In addition, IT professionals must have skills in communication, business, relationship building, negotiation, alignment, human resource management, fiscal management, strategic planning, and presentation—not to mention a sense of humor.[22] According to a Tech Spotlight series on CIOs, in addition to this list, leadership and management, as well as an understanding of and an ability to build organization and culture, are also required.[23]

Thornton May, a renowned futurist and faculty associate of the Center for Advancing Business through Information Technology (CABIT) at the W. P. Carey School of Business at Arizona State University, states these skill sets in terms of contexts. At an Interop CIO Bootcamp, he presented the following as requisite skill sets:

- Manage massively complex, never-meant-to-be-integrated technology
- Demonstrate to increasingly hostile, risk-sensitized stakeholders how to comply with an expanding array of ambiguous regulations
- Perpetuate 24/7, global, multiple-device access to online information assets in the face of escalating security threats
- Educate time-challenged executive teams about IT costs, functions, and value creation for their line-of-business responsibilities
- Align IT investment with business strategy to help shape the overall executive agenda and enable the enterprise to understand the "art of the possible," attracting appropriate resources to that opportunity[24]

Summary

In summary, to rise to the challenges and career path of a CIO, you must arm yourself with the skill sets that will be demanded by the next generation of employees who are the driving force of adopting today's emerging technologies. The technical skills are just one portion of the skill set. You'll also need to be skilled in management, visioning, and team-building, plus have the flexibility and agility required to deal with the unknown. Predications of technology will only be able to go so far and be so accurate. The ability to harness those predications and technologies into an implementable plan for the benefit of the enterprise—be it corporate or higher education—will be essential.

Finally, it is not necessary to reinvent the wheel with regard to emerging technologies. It is imperative that you understand the strengths, weaknesses, and risk tolerance of your IT organization and your institution. Best practices in emerging technologies exist and are often documented on other institutional websites and presented at conferences. Leveraging the applicable work of others and focusing on the value of that work to your organization will allow you to do more with less and keep a percentage of the work focused on emerging technologies and their potential value to provide the most seamless, integrated, and rich customer experience, regardless of the industry application.

Notes

1 Lindeman, J., and Bulk, F. "Herding Highly Mobile Cats." Network Computing Summer 2005 Expert Series, Mobile and Wireless.

2 Molta, D."WLANS Put to the Quality Test." Network Computing Summer 2005 Expert Series, Mobile and Wireless (http://www.nwc.com/go/expert.jhtml).

3 Dornan, A. "The WiMAX Anticlimax." Network Computing Summer 2005 Expert Series, Mobile and Wireless (http://www.nwc.com/go/expert.jhtml).

4 http://www.fcc.gov/3G/

5 http://www.verizonwireless.com/b2c/mobileoptions/broadband/index.jsp

6 http://www.cingular.com/midtolarge/solutions

7 Mobile Pipeline Staff, http://informationweek.com/story/showArticle.jhtml?articleID=164900167, June 16, 2005.

8 Rysavy, P. "Wide-Area Wireless Evolves." Network Computing Summer 2005 Expert Series, Mobile and Wireless (http://www.nwc.com/go/expert.jhtml).

9 Pescatore, J. "Managed Security Services Provider Magic Quadrant." *Gartner Research Note,* February 1, 2002.

10 Allen, J., Gabbard, D., and May, C., http://www.cert.org/security-improvement/modules/omss/index.html, January 21, 2003.

11 Nash, T., http://www.networkmagazineindia.com/200410/vendorvoice01.shtml, October 2004.

12 Schwartz, M., http://www.esj.com/security/article.aspx?EditorialsID=1123, September 22, 2004.

13 O' Donnell, G., http://www.unisys.com/services/network__services/insights/outside__opinions/opinions.htm?insightsID=23230, June 2003.

14 http://www.ciber.com/index_var.cfm?pageid=/services_solutions/outsource/main.cfm?id=cs-out-helpdesk

15 Bailor, C. "5 Elements to Consider After You've Outsourced." *Customer Relationship Management,* July 2005.

16 Palmer, B. Stanford Report (http://news-service.stanford.edu/news/2005/january12/google-0112.html), January 12, 2005.

17 Porco, C., http://www.intranetjournal.com/articles/200502/ij_02_18_05a.html, February 18, 2005.

18 Carlson, S. "Talking Tags." *Chronicle of Higher Education* (Information Technology Section) 50(48): A29.

19 Press Release. "Consumer Awareness and Attitudes About RFID Are Stabilizing.htm." *Market Wire,* June 21, 2005 (http://press.arrivenet.com/tec/article.php/656967.html).

20 Collins, J. "Smart Labels for Higher Education.htm." *RFID Journal,* May 24, 2003 (http://www.rfidjournal.com/article/articleview/666/1/32/).

21 http://www.rfidjournal.com/article/archive/4/htm

22 CIO Executive Research Center, "The Changing Role of the Chief Information Officer." October 1, 1999 (http://www.cio.com),

23 PWC Advisory, "The New CIO: From Techie to Tie." *Tech Spotlight* 33 (May 2005), (http://www.pwc.com/extweb/pwcpublications.nsf/docid/D5489234F50FF32A85256FF2000FE226).

24 May, T. CIO Bootcamp Seminar, presented at Interop, May 1, 2005.

CHAPTER 3

Network Security

Beth Chancellor

Beth Chancellor is Associate CIO at the University of Missouri, Columbia. She received her B.S. in Management from William Woods University. Her 19-year career at the University of Missouri has been in management and administration, covering traditional telecommunications, networking, and information security.

The Internet has provided a venue that enables higher-education institutions to become truly global. Higher-education electronic networks promote relationships with prospective and current students, faculty, staff, research consumers, patients, alumni, grantors, vendors, and benefactors. Unfortunately, networks also provide access to global troublemakers and outright criminals who want to disrupt, exploit, or steal electronic information resources.

As with any area of security, network security programs should be developed to respond to the risk while simultaneously balancing access with usability. We can guarantee the security of our networks simply by not letting anyone on them, but that would obviously be counter to their purpose. The fact remains that the more secure a network is, the less "open" it is, which for some equates to it being less usable. This is especially true in college and university settings where, in the past, networks have been extremely open.

This chapter deals with the topic of network security—specifically policies, processes, and technologies that work together to ensure that systems are protected and networks are reliable and usable.

■ Defining the Services: Voice, Data, and Video

Voice Networks

Voice networks have operated under a fairly limited number of security threats for many years, although physical security has always been a concern. Breaches in physical security include unauthorized wiretaps or other malicious activities. Fortunately, the circuit-switched environment provides little opportunity for breaches in physical security.

Security concerns in the circuit-switched environment began to rise with the development of modem technologies in the 1960s and 1970s. *Modem* is a contraction for modulator/demodulator. Specifically, it refers to a device in which one can use plain old telephone service (POTS) lines to transmit data communications. For its time, the modem was revolutionary. It allowed up to 56 kbps of data traffic to be transmitted over the regular phone system. Today, the term *modem* is used for any device that translates information from one medium to another—for example, a DSL modem, a cable modem, and others.

Telecom and network managers had few methods for stopping the installation of modems, which provided access (often insecure) to the systems and networks to which they were attached. Dial-up access continues to be a concern, and now VoIP technologies have facilitated the movement of voice calls from circuit-switched networks onto data networks, exposing such traffic to all the security concerns that come with data-networking technologies.

Video Networks

Video networks (typically closed circuit) have also faced few security threats, with most security efforts focusing on the prevention of cable television (CATV) theft. While closed-circuit video systems are still quite prevalent, the transmission of video content is increasingly accomplished through data networks. Videoconferencing, video streaming, movies, and programming typically handled by CATV providers are all being transitioned into an "anytime, anywhere" delivery method via data networks.

Data Networks

Data networks are made up of LANs, MANs, and WANs. There are also a variety of components and services—switches, hubs, routers, wireless access points, remote access servers (RAS), cable modems, digital subscribe lines (DSL), T1s, and so on—all of which must be secured from many different threats. In addition, other services, such as domain name services (DNS), are required for a network to function properly. These services run on servers that pose their own set of security risks.

DNS makes the Internet more user friendly. When we want to go to a site, we key the URL (e.g., www.acuta.org) into our browser. Unfortunately, the computer does not know where that site is, as computers can only go to sites identified by their IP address (e.g., 192.3.5.200). The DNS translates what we humans enter (www.acuta.org) into the IP address so the computer can make the connection. Although a very useful service, DNS does pose its own series of difficulties.

Data networks are increasingly carrying more than what is normally referred to as "data" traffic. For example, VoIP is becoming prevalent and does not carry with it a tolerance for disruptions. Interception of voice communications on the data network, while not fundamentally different from other types of traffic, will be viewed by users as an invasion of privacy and may seem more serious than the disruption or loss of a data transmission. Video services are also becoming prevalent on IP networks. Given this convergence of services on the data network, the rest of this chapter will focus primarily on data network security.

■ Identifying Threats and Assessing Risk

According to Internet World Stats (www.internetworldstats.com), the number of security threats is growing at an alarming rate. This increase plus a growing cracker (malicious hacker) community and many other factors, place all networks at risk.

Network administrators are being confronted with a variety of threats, including viruses, worms, and unauthorized intruders. These threats can pose a significant risk to the network and, more seriously, to desktop computers and servers (referred to jointly as systems or hosts) on the network. In fact, insecure hosts and insecure applications pose the biggest risk to networks and to other hosts on the network.

Similar to viruses that affect the human body, computer viruses enter the computer and self-replicate to infect the whole computer. Typically, these viruses also carry a destructive factor that erases a portion of the hard drive, copies passwords, and/or destroys data. Viruses are confined to one computer until, deliberately or inadvertently, a user passes them along to another computer.

Unlike viruses, worms have the capability to transmit themselves between computers. Using the file transmission capabilities of the computer and the Internet, worms often spread themselves to other computers using the address book of the infected computer. Once on a computer, worms may also have destructive properties that destroy data.

Some sources say that spyware has surpassed viruses as the number one threat to computers today. Spyware is any program that installs itself uninvited on a hard drive, collects personal information about the user and his or her computer habits, then sends that information, unauthorized, to a third party. Spyware gets into a system by stealth. It may come bundled with another program and automatically install along with the other software. Or it may enter the system through the advertising used in some free software, such as peer-to-peer programs like Kazaa and Morpheus. This second type of spyware is known as adware. A visit to certain websites that install cookies on your hard drive may also

open a door for spyware, or someone may install spyware on your computer maliciously.

Symptoms of a network security breach or of a compromised system can include loss or manipulation of data, applications that become unusable, loss of Internet access, and the "spewing" of information causing what is known as a denial of service (DOS) attack, which can clog the network and render it unusable.

Network *hardening* is the concept and process of securing a network. To meet network hardening goals, an organization must first understand the threats, vulnerabilities, and, thus, the risks that need to be mitigated.

Assessing the risk associated with known (or unknown) threats requires a thorough review, or audit, of your current network security environment. What business and academic systems attached to the network are critical to the institution? What would happen if one of those systems were compromised? Legal requirements, such as the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) act, must also be considered when determining what to protect. Assessing risk also requires identifying weaknesses of the network itself, not just the risks posted by hosts. These assessment factors are complicated by the fact that the systems in need of protection are broadly distributed throughout a campus and are typically managed by individuals with a variety of responsibilities and skill sets.

In trying to assess risk, network administrators should ask questions such as the following:

- How many network IDs are active, and how many should legitimately be active?
- Does the institution mandate strong passwords for network and system access?
- Where does critical, sensitive, and legally protected information reside?
- Are there limitations on who can gain access to critical systems?
- Are older systems segregated from the rest of the network?
- Is the information being transmitted on the network secure (encrypted)?
- Would anyone know if a system had been compromised?
- Do desktop configuration and security policies and standards exist?
- How can policies and processes be applied to address network security issues?
- How much technology can we afford, and how can it be utilized most effectively?

So how can an institution use the answers to these types of questions to prioritize security goals? A tool that is often used in assessing risk and setting priorities is a matrix or XY grid. Start by selecting a particular vulnerability or threat, such as the introduction and spread of an e-mail virus. Use one axis of the grid to set a level of likelihood that the event will happen and the other axis to apply an impact rating. The likelihood rating is an educated assessment based on what's going on in the industry and the current state of an institution's security efforts on the topic in question—in this case, e-mail security. The impact rating, also somewhat subjective, takes into account factors such as the institution's reputation, loss of productivity, and the amount of staff time needed to fix the problem. Although both ratings may seem subjective, information available from industry experts and other institutions can be helpful in applying a dose of reality to the ratings selected.

Once completed, how can the matrix be used? In theory, the items that are high in likelihood and high in impact should be the areas on which you focus. However, it may not be reasonable to focus only on those items. There may be low-likelihood or low-impact threats that are "low-hanging fruit," meaning they can be addressed with little time and effort. Always deal with quick wins whenever possible. There may also be high-likelihood, high-impact issues that are cost prohibitive, or have more than one possible solution, or become bogged down in politics. While they pose high risk, it could take time to deal with some obvious priorities.

The matrix should be updated frequently. In addition to information presented in the matrix, use the concept of hardening, or "defense-in-depth," to make network security decisions. Defense-in-depth focuses on removing factors that increase risk and on adding controls to decrease risk throughout the network.

■ Network Security: Nontechnical Strategies

Staffing

Improving network security requires making staffing a priority. Outsourcing network services, management, and security is an option for some institutions, but it can be costly. Even when outsourcing is an option, vendors are usually not capable of handling all network security needs. Therefore, it is important to hire sufficient, competent network staff and to train and arm them with tools that focus specifically on security.

The number of staff required depends on a variety of factors. For example, an institution's size can affect the number of staff. Larger institutions may be able to

hire staff who focus only on network and other security issues. Smaller institutions may need to add security responsibilities into existing network administration titles. Regardless of how it is accomplished, it is important that the entire institution be aware that network security (and security in general) is a priority.

Another factor is the institution's functional program diversity. All higher-education institutions will probably have to comply with FERPA and GLB, but not all institutions have medical endeavors that throw HIPAA into the mix. Likewise, not all institutions are research intensive, with vast vaults of highly sensitive and confidential data. However, many do utilize e-commerce systems and thus may have credit card information that needs to be kept secure. The more functionally diverse an institution is, the more types of systems need to be secured and the more laws must be complied with.

Centralization

In most higher-education institutions, there is a tension between centralized and decentralized network services. In a campus setting, decentralized network services—and thus decentralized network security—make the availability, reliability, and security of a network nearly impossible to attain. Network management, policies, compliance, best practices, and standards can be optimized when centrally deployed. While it is not mandatory to centralize network and system administration, institutions do stand a better chance of success in a centralized network environment.

Standards, Policies, and Processes

Like centralization, standardization is a difficult "sell" in higher education, especially when it comes to information technology. Standardization, however, may be the single biggest factor leading to efficient, effective security practices. Desktop management, server administration, strong password standards, account management policies, and so forth—all of these require standard policies and processes in order to be effective. It is simply more efficient, more enforceable, and thus more secure for an institution to deal with development and implementation of standards, policies and processes at one time.

• Privacy and Confidentiality

Privacy concerns may be especially high in a university setting where academic autonomy and freedom of exploration and expression are highly valued. These values and expectations apply to electronic transmissions as much as they do to speech and publications. Combined with the widely publicized security breaches

in the private and public sectors, users are increasingly concerned about these issues.

It is critical that security staff be trained in privacy and confidentiality issues. Training on these topics should at least include appropriate use of logs and files, retention and disposal processes, handling requests for information from others within the institution and from law enforcement, handling subpoenas, and FERPA. Technical staff should acknowledge their responsibilities associated with their privileged access. As an example, many institutions require technical staff to sign statements of understanding to drive home the importance of this issue.

Institutions should also have a policy that requires the expedient disclosure of any security breach involving the release or theft of personal or financial information. Not only do institutions have an obligation to inform individuals when their information has been inadvertently released, but institutions will also find that the public reacts better when they "come clean."

• Documentation

Documentation should be developed for all security-related processes and techniques. Areas that require documentation include testing procedures and results, decision papers related to selection of a particular technology, bids and bid evaluations, implementation and configuration criteria, and so forth. Documentation will assist an organization in ensuring that decisions are well thought out and that security initiatives are in-line with institutional priorities.

Documenting an institution's network security strategy is important for a variety of reasons. First, it provides a clear understanding of the philosophy used in developing, implementing, and managing security goals, thus setting the tone for the entire institution. Second, it provides foundation and direction for network administrators. Third, auditors use the documentation to identify problems and weaknesses in an institution's network security posture. Even if auditors find weaknesses (and they will find them), the documentation lets them know that network security is taken seriously.

• Testing, Change Management, and Quality Assurance

As with anything IT related, technologies and tools used in network security must be tested (and documented) before being implemented. Many network organizations have a test lab that is as close to a replica of the production environment as is financially possible. If such an environment exists, it should be used to its fullest to test network security technologies and configurations before implementing them.

If a test lab is not available, it is usually feasible to apply security solutions to a smaller segment of the campus population for a test. This smaller segment can be by building, by a range of IP addresses, by network segment, and so on. Applying

security features to smaller segments of the network before applying them universally is a good way to test results without disrupting the entire organization.

Other IT professionals responsible for managing servers, desktop computers, and so on can also assist in identifying potential problems with technology implementations. Engage them in network security discussions and test solutions against their systems. Experts in other IT areas can identify negative effects that network security solutions might have on other systems. Ultimately, all new solutions or changes to existing solutions must go through a change management process to ensure that changes are known about and endorsed by the rest of the IT community.

Once solutions have been tested and endorsed, it is important that more than one network technician be involved in implementing the solution to ensure quality assurance. There are a significant number of settings, configurations, and techniques used to implement technology security solutions. Always use a second set of eyes to ensure that technologies are being executed in the agreed-upon method.

• Account Management

Networks connect computer systems. These computer systems have operating systems that require mechanisms to allow (or prohibit) access to distributed resources. Use of those mechanisms requires users to first be authenticated (proving they are who they say they are) and then authorized to access a particular resource. Account management ensures that authentication and authorization are limited only to those who should have access. Unneeded user accounts and inappropriately assigned access are significant, and often overlooked, security risks.

Authentication, authorization, and accounting, which are often thought of as the three As, are the fundamental foundations for network security.

Authentication: A process or tool that verifies you are who you say you are. Typically, what you know (passwords), what you have (a picture ID), or who you are (biometrics) provide authentication.

Authorization: Once you prove who you are, what are you allowed to do? Authorization allows the user to have access to certain systems (payroll, student accounts, etc.) at certain or all times of the day.

Accounting: Now that you have proven who you are and were given permission to do things, what actually did you do while logged on? A critical and third leg of the security stool, accounting monitors user attempts to go where they shouldn't and watches for suspicious behavior and activity.

Account management can be a difficult, time-consuming, and thankless task, especially for central IT shops that manage accounts and access to resources for the entire campus population. To be effective, account management calls for very specific sets of policies and processes. Organizations have a multitude of systems that should go through rigorous and frequent account cleanup processes. While some universities have true single-sign-on systems, many do not. Instead, a fairly common environment is known as a single-account realm. Users have an ID (sometimes referred to as a network ID) and password, but authenticating once allows access only to a few systems. Often, users have to authenticate at least twice to access a specific system. Examples of the types of systems and resources that should have an account management process include:

- Directory services (such as Microsoft's Active Directory)
- E-mail systems
- File, print, and web servers
- Application servers
- Enterprise resource planning (ERP) systems
- Identification systems (ID cards)
- Voicemail systems
- Long-distance authorization codes
- Remote access accounts
- Distribution lists
- Resource accounts

You should begin an effective account management program by frist centralizing the account management administration process for as many systems and services as possible.

Second, establish campuswide policies for eligibility for and elimination of accounts. A single policy that identifies the overall account management goals and the organization responsible for the program should be sufficient at the institutional level. The responsible organization can then develop additional policies and processes that provide details of the program, such as defining account eligibility, frequency of account deletion cycles, communication processes, and more.

Third, constantly communicate. Notify users and their departments (if applicable) of impending account deletions. Communicate more than once with the affected user well in advance of the deletion date. Also, be sure to provide a method through which users can obtain an exception or an extension. This can be accomplished by setting account expiration dates or by requiring a sponsor-

ship of (technically) ineligible accounts from a person of authority. Maintaining exception lists can be cumbersome, but providing flexibility will make the whole concept of account management more palatable to the campus community.

Finally, publish the policies and processes to the entire campus community. Everyone will be more aware of what to expect when accounts are being deleted. Also, in a decentralized environment, campus departments might just use those processes to ensure that the systems they maintain are free of unnecessary accounts.

Do not undervalue the account management team. Individuals who are involved in account management experience many on-the-job situations that, over time, make them very good at what they do. They learn what to expect from users, how to communicate, when to make exceptions, and when to escalate problems appropriately. They are not clerks. They have to understand how to access a variety of systems and can potentially do harm to those systems if they don't know what they are doing. They may need to perform database query commands and system commands on a variety of systems, including directory services, telecommunications systems, file systems, and others. Good account management staff are invaluable to your organization's efforts to secure IT and telecom resources.

Compliance and Auditing

To ensure that policies and procedures are being followed, compliance and auditing are critical. It is impossible to guarantee that everyone follows the policies, processes, and technical techniques established to ensure network security. Compliance and auditing are not limited to the network itself. Insecure servers (also known as hosts) are a constant threat to both the network and other hosts. Compliance must take into account all systems and services that can affect the network and those devices attached to it.

Security audits can take several forms. One type is an unrequested or unannounced audit that measures compliance and identify weaknesses. This type of audit is typically intended to satisfy administrative mandates and regulatory or legal requirements. Another type of audit is an assessment, which is usually requested by an organization. The assessment audit identifies weaknesses, tests the strength of security measures already implemented, and sets priorities for the future. This audit should be conducted by a qualified vendor and should be customized to fit an institution's needs. Assessment audits can be expensive, so it is imperative that you develop a clear and detailed "statement of work." Audits can also be performed internally, typically by your own IT or administrative staff, to test compliance with policies, processes, and best practices. These internal audits can be very beneficial in preparing for the inevitable external audits.

Auditing can be complicated and stressful. It is a process best learned through actual experience. Those responsible for network security (and information security, in general) should work proactively with auditors and others within the institution (including legal counsel) to understand the areas that auditors are concerned with and the compliance issues they intend to examine.

■ Network Security Technologies

Access Controls

Access controls are technologies and policy methods used to restrict the use of your network. Controlling access to a network surely means better security. Like all things security related, however, the trick is how to balance security with usability—or, in this case, access.

A variety of technologies can be used to implement access controls. The best approach, before selecting a technology or set of technologies, is to step back and take a broad look at the user community—where they are, how they access the network, and what they need to access. Unfortunately, most networks do not get to start with a clean slate. Networks usually have a preexisting network environment that cannot simply start over and utilize the best of all access-control technologies. Instead, network administrators must constantly keep up with what's going on in the access-control technology world and meld existing products with new ones.

Firewalls

A network firewall is an access-control appliance designed to protect a private network from the Internet. The firewall allows systems inside (or behind) to access information or resources on the Internet (the outside) while preventing users on the Internet from accessing information on the inside. This separation is handled by establishing a demilitarized zone (DMZ), sometimes called a neutral zone, between a private network and the Internet.

Network administrators implement firewalls based on a carefully planned access-control policy that manages the flow of data or connections between networks. Firewalls use several different methods, such as packet filtering, to allow or disallow the flow of data. They also provide many additional features and functionality, including extensive logging and reporting.

In addition to protecting a network from the Internet, firewalls can be used to divide an existing network into two or more segments. Network segmentation is an effective way to provide more-or-less restrictive access to and from the

Internet and between the network zones. Segmentation is similar to establishing several "gated communities" within a network, allowing access between those communities only to authorized users and only after the data flows have been inspected.

Universities have multiple systems with highly sensitive data, often scattered throughout a campus, that need to be protected. These systems hold research data, patient data (protected by HIPAA), student data (protected by FERPA), financial aid data (protected by GLB), credit card data (E-commerce), and so on. Multiple firewalls (or multiple virtual firewalls) allow network administrators to establish different levels of security, as necessary, to protect systems and data.

Firewalls can be expensive. Enterprise firewalls with sufficient features and throughput to handle medium to large campus environments range from $50,000 to $100,000. Firewalls are in-line and, therefore, present a single point of failure. Firewall redundancy doubles the costs. Maintenance costs add between 10 percent and 20 percent of the cost of the equipment, in addition to staff salaries and training.

Virtual Private Network (VPN)

A VPN is an access-control system that connects remote users to a private network through an insecure public network (i.e., the Internet). VPN technology was originally developed to allow access to home office networks via the Internet, thus eliminating costly private-line connections. A VPN may connect two or more networks, or it may connect individual users to a network. A VPN can provide both data encryption and user authentication.

A VPN can also be used to allow access by specific users to specific resources. VPN groups, for example, can be established to allow a limited number of system administrators access to a particular server or set of servers, thus simultaneously ensuring encryption and access control. In this scenario, it doesn't matter whether the system administrator is using the Internet or whether he or she is in the office on the enterprise network. A VPN appliance doesn't really care where you are, as long as you have the necessary credentials to get from point A to point B.

VPN appliances, like firewalls, can be expensive. An enterprise-class VPN system may cost between $20,000 and $30,000. VPN appliances can be used for a variety of purposes and can be placed in more than one location on a network. Depending on their use and where they are placed, they may or may not present a single point of failure.

Intrusion Detection System (IDS)

An IDS can be a valuable and important part of a network security program. There are two types of IDSs: host based and network based. Host-based systems are implemented by installing a client (or an agent) on a server that acts as an incident-reporting agent. A network-based IDS monitors network data flows to identify suspicious or malicious activity.

An IDS identifies both unauthorized actions on a network and attempts to gain unauthorized access to systems. It can also identify a variety of other malicious activities, such as viral infections. On the negative side, an IDS can be extremely time consuming and difficult to manage. Network staff can become inundated with data. In addition, because an IDS can collect confidential data, policies must be developed to address confidentiality and retention issues.

IDSs were initially designed to detect and report intrusions in log files. They are similar smoke alarms: When a smoke alarm goes off in a building, everyone knows to leave the building. However, they don't know which alarm went off or what set it off. Specially trained firefighters must ascertain where the fire is and how to put it out—or whether there really was a fire. Sophisticated fire alarm systems can actually pinpoint a fire and activate a fire-suppression system (akin to an intrusion prevention system) that can automatically put out the fire. Similarly, well-trained staff and a well-honed IDS can simplify use and minimize false positives.

An IDS works by monitoring a network and then reporting activities based on anomalies or "signatures." Several free tools are available, including a variety of network scanning tools, sniffers, and file-integrity programs. These tools can capture and report intrusions and create logs, which then need to be analyzed for intrusions or checked for altered files. An effective IDS uses a variety of programs specifically tuned to provide efficient identification of attackers and other network breaches. An IDS can also be used to proactively identify vulnerabilities in systems that are attached to a network, such as out-of-date operating systems or uninstalled patches.

Some commercial IDS systems are becoming popular. These systems can jump-start an intrusion detection program, providing out-of-box functionality, vendor support, and regular software and signature updates. There are also vendor-provided intrusion detection services. If intrusion detection is a worthwhile investment, outsourcing is an option that merits consideration.

Because an IDS is not an in-line system, it does not pose a risk to the network if it is compromised or it fails. Unfortunately, most uses of IDS are reactive, allowing only the most experienced network technicians to actually prevent an attack. That's where intrusion prevention comes in.

Intrusion Prevention System (IPS)

Today's network environment is increasingly complex. The number and sophistication of crackers grows every day, as do the number of vulnerabilities. The time to react to a known exploit has shrunk to a few days, and most of us agree that "zero day" reaction times are inevitable. Network administrators will be forced to utilize proactive methods to identify and stop intrusions.

IPSs have emerged as full-fledged enterprise network systems only in the past few years. They are not typically developed by internal staff using free software. Instead, they are commercial systems developed to take advantage of the information historically gathered by IDSs. They use that information to automatically prevent an intrusion in a specific and predictable manner.

Comprehensive intrusion detection/prevention appliances can prevent network attacks and stop a variety of other threats, including worms, spyware, keyloggers, and other malicious applications. They provide extensive auditing and logging functions with canned and customizable reports. To keep up with the changing intrusion landscape, the vendor frequently provides signature and feature updates. Like most network technologies, IPSs are expensive, running typically $30,000 to $50,000 per unit.

Honeypots

Honeypots are intrusion detection and prevention systems rolled into one. They provide a decoy to lure potential attackers and thus keep them away from systems you want to protect. Once a system is attacked, network administrators can use the information to obtain details about the hacker and his or her techniques. Honeypots can also slow an attacker, minimizing the negative impact on a network.

Honeypots have only been around for a few years. In 2003, there was a great deal of activity within the network and security industries about possible legal issues associated with honeypots. There were suggestions that honeypots intercepted communications, which is illegal, or were a form of entrapment. Although no court cases have firmly established this, subsequent information from a variety of sources (including technology industries, law enforcement, and legal opinions) agree that honeypots are legal methods used to protect networks and other resources.

■ Wireless Networking

The most common form of wireless networking for the enterprise utilizes network devices called access points (APs) that use the IEEE 802.11 standard, commonly referred to as WiFi (wireless fidelity). There are currently three variations of the 802.11 standard: a, b, and g. When implementing, or considering implementing, wireless networking, remember that although all forms of wireless technologies provide mobility, they do not provide the bandwidth or the level of reliability and security that wired networks provide. Wireless networks pose unique security problems, such as vulnerability to interception. However, methods for securing your wireless network are available.

Steps to Wireless Security

The first step to securing a wireless network is to control the network and the airspace. Policies should prohibit the installation of unauthorized APs on your university's network. Without such a policy (and even with it), you will experience constant interference between the campus's official wireless network and rogue APs. In addition to interference problems, unauthorized APs may also allow unauthorized users to gain access to your network.

In addition to rogue APs, WiFi technologies pose significant technological security problems. WiFi's built-in security method calls for encryption through Wireless Encryption Protocol (WEP), which encrypts the transmission between an end user's computer and the AP. WEP itself is somewhat easy to crack due to flaws in the protocol design.1 Some wireless technologies provide management tools to update all APs with a new WEP key through a single command. Others require that the keys be set one at a time. While not hacker-proof, WEP should be implemented on all APs until stronger encryption schemes like WPA (WiFi Protected Access) are widely available.

If WEP is your primary method for wireless security, rotating the key frequently can increase security. It is difficult, however, to rotate a WEP key for an entire campus. After the WEP keys are changed, all authorized wireless subscribers must configure their network interface cards (NICs) to match the new key. In addition, end users have to be told what the new key is, posing a security problem of its own. WEP should never be the sole method of security in a wireless network.

Network Keys

Similar to metal keys on your key chain, network keys allow only those holding the keys to interpret the transmission. You can't enter your locked car without the

key (or keycode), nor can you read your e-mail without a network key. Keys are broken down into two broad categories: symmetric keys and asymmetric keys. Symmetric keys require both parties (sender and receiver) to hold the same key, and each key has an equal amount of the encryption. Asymmetric keys require both parties (sender and receiver) to hold *related,* but not exactly similar, keys.

802.1X: The Best Method

Other standards and technologies are available for increasing wireless network security, including authentication systems, VPNs, and firewalls. The most effective method of all options, however, uses the IEEE 802.1X standard (commonly referred to as 1X). The 1X standard offers an effective method for melding authentication and dynamic WEP keys. When 1X is implemented, users must authenticate with a network ID. Once authenticated, the wireless NIC transparently receives a new WEP key, allowing for hidden, frequent, and simple rotation of WEP keys.

The downsides to 802.1X are the required use of a client, called a "supplicant," and the requirement to authenticate. Obviously, a separate client poses significant support issues. In addition, the use of 1X requires that everyone accessing the wireless network have an ID and password. All campuses have "guests" who have been able to access networks. With 1X, network administrators will have to provide a method to enable guests to access the network.

Encryption

Encryption, based on the science of cryptology, is an important part of securing data transmissions. It is accomplished by exchanging ciphers(s), or "keys," between two communicating devices. Keys enable one device to encipher a transmission and the recipient device to decipher the transmission, and vice-versa. A network, however, can be designed to disallow some forms of insecure protocols, such as telnet and file transfer protocol (FTP), while allowing other forms of secure transmissions, such as pretty good privacy (PGP) and secure shell (SSH), thus forcing encrypted or other forms of secure communications.

There are a variety of encryption methods. The two major types are symmetric and asymmetric. Symmetric encryption enables communications devices to share the same key. Asymmetric encryption uses a pair of keys, one pubic and one private, to encrypt and decrypt communications. Asymmetric technology is the basis of secure certificates, which are used to secure Web traffic, like that associated with e-commerce.

Similar to encryption is hashing, which involves taking a key element on a computer, such as a password, and subjecting it to a particular mathematical

algorithm to change its content. To regain the original content, the same hash value must be applied. Hashing is quite often used in internal computer storage of information and sometimes in data transmission.

■ Summary

Network security does not focus only on keeping the "bad guys out." Rather, it is a comprehensive program that manages a whole list of issues, including protecting from threats inside and outside, managing access to resources, and ensuring that sensitive data transmissions are encrypted. Network security can be very costly. Organizations may have to make trade-offs between network service improvements and security needs.

In higher education, security breaches can take many forms. The changing of grades, loss or manipulation of data, loss of access to critical systems and services, unintended release of personal information, including financial information—all of these breaches can cause irreparable harm to individuals and to an institution. Network security is not a matter of "Can you afford it?"; it's a matter of "You can't afford to not afford it."

Organizations never know when they are secure; they only know when they aren't. It is imperative that higher-education institutions make information security a high priority, both in attitude and in funding. Network security is not a one-time cost. Threats and vulnerabilities change on a regular basis, requiring an ongoing source of funding. Institutions that make security a priority can make significant progress in protecting their IT resources.

Note

1 Albanese, J., and Sonnenreich, W. *Network Security.* (New York: McGraw Hill, 2004).

CHAPTER 4

Security and Disaster Planning and Management

Marjorie Windelberg, Ph.D.

Marjorie Windelberg, Ph.D., served as CIO at Gannon University and Hillsborough Community College from 1994 to 1999. In 2003 and 2004, she served as the program manager for the National Do Not Call Registry. She currently consults to the federal government on information assurance best practices and teaches graduate courses on information security management, business continuity, and homeland security for the University of Maryland University College.

Security, disaster planning, and management are three practices that can protect an institution's critical functions, information assets, and people. These practices help safeguard an institution's mission-critical functions, reputation, and financial interests. The practices discussed in this chapter provide a template that can be adapted to an institution's specific circumstances, such as its critical functions, the amount of protection needed, and the resources available for security and disaster management.

To study security and disaster planning and management we begin with the foundations of program management and risk analysis, then cover physical security, and close with disaster planning and management.

■ Program Management

Program management involves developing policies and plans that reflect an institution's needs, making the business case for those plans by (1) analyzing costs and benefits, (2) providing oversight to ensure that the plans are carried out and meet the established performance measures, and (3) reporting to senior management. What are the major elements of program management for security and disaster planning and management?

Governance and Planning

Sponsorship, commitment, and visible support by senior management, as well as by a governance committee, are important for starting and sustaining efforts for security and disaster planning. At the governance level, an institution will define

requirements for security and business continuity and develop strategies for both areas. Those responsible for developing security and business continuity plans will also assess the resources needed. Senior management will need to commit funding and people to implement the plans.

Incident response is another important part of these plans. No matter how much effort goes into preventing incidents, an institution should have thought through what to do when something negative happens. Incident response assigns roles and defines their responsibilities. It also outlines procedures for response and recovery. For example, in instances of a network or system breach, procedures should detail how to protect evidence, preserve the chain of custody, and document actions taken. Another good practice is to hold postincident reviews and use the information from the reviews to plan security improvements or to help prevent disasters. Provisions should also be made for training response teams and for regular testing of response procedures.

As with any plan, once it is approved, the project must be managed to ensure that deliverables are met within the timelines and budget constraints. Ongoing program management for security and disaster plans includes training for staff, regular testing, and periodic reviews of and updates to the plans.

Policies

For network and computing security, acceptable-use (or ethical computing) policies have long been a necessity. An acceptable-use policy typically covers behavior and utilization of computing, telecommunications, and network resources, as well as respect for intellectual property. The areas covered have continued to expand—first into e-mail and cell phones, and more recently into connecting home or personally owned computers to campus networks, instant messaging, use of peer-to-peer software, and blogging. A well-designed policy not only describes what behaviors are off-limits but also prescribes consequences for violating the policy.

Personnel policies are also important. An institution should have, and follow, policies and procedures regarding termination of employees and prompt revocation of access privileges. When hiring staff for IT responsibilities, it may also be wise to conduct background checks and require them to sign off on rules of behavior. Training, along with the allocation of resources for training, is essential for both IT staff and users. End users should be expected to be aware of security policies, to avoid behaviors that increase risks, and to report to appropriate authorities incidents and possible vulnerabilities. Promoting security awareness among end users encompasses both technical and nontechnical issues, including configuring software firewalls and recognizing social-engineering tactics.

All of these practices pertain to internal staff, and some to end users. Another area to address involves third-party vendors and suppliers. Contracts with outside vendors and suppliers should include personnel security policies, such as requiring third parties to sign in and out of restricted areas or to be escorted while in those areas. There should also be a policy that covers interfaces with external systems for exchanging data.

■ Risk Analysis

Risk analysis helps an institution determine which functions and information assets are critical and how they might be vulnerable. On the basis of that information, an institution can decide what steps need to be taken to reduce risks and prevent or minimize security incidents and disasters.

Identify and Prioritize What Is Critical and Sensitive

The first step is to identify and prioritize the critical functions and assets. As part of the identification process, it helps to map the functions and assets to telecommunications and data-processing systems; to people; and, for physical security, to spaces, including network and data centers, telecom rooms, network pathways, and even storage areas.

Prioritizing functions and assets is typically based on criticality and sensitivity. A governance committee is often responsible for determining how critical functions and assets are to the institution's mission. Questions associated with criticality should also be addressed, such as How long can a department operate without access? and How will they function in the meantime? Criteria for evaluating the sensitivity of information assets include the degree of privacy that needs to be maintained and the value of intellectual property. Information assets may be compromised in terms of confidentiality (e.g., exposure of personally identifiable information) or in terms of integrity (e.g., modification or destruction of institutional records or research data).

Describe Threats, Vulnerabilities, and Countermeasures

Identifying threats and vulnerabilities, as well as documenting existing countermeasures or safeguards to address threats and vulnerabilities, constitute the next steps in a risk assessment. Vulnerabilities include absent, flawed, or weak safeguards—whether in design, implementation, or operation—that can be exploited. There are different types of vulnerabilities, ranging from the ineffective policies or procedures to complicated technical measures, such as firewalls and intrusion detection.

Threats may be natural (e.g., fire or weather related) or environmental (e.g., loss of power or air conditioning). One type of incident, such as a hurricane or earthquake, may result in secondary problems, such as power outages or fire.

Humans can pose a myriad of threats, both physical and logical, that affect the confidentiality, integrity, and availability of information. At times, human threats are accidental (as in, "Oops, I deleted the wrong file.") or caused by negligence, such as not patching or not keeping antivirus software up to date. Deliberate acts are more costly and can be committed by insiders or outsiders, or even by outsiders working with the help of insiders. Attacks such as network intrusions or disruption of network or system services may be remotely launched—either manually or automated via scripts. Even social engineering to obtain personal information or system information is typically conducted remotely. Other threat activities are carried out in person: reconnaissance, such as checking access doors; disruption or access by tampering with a network's physical infrastructure; theft of equipment or even documentation; and even social engineering by piggybacking on someone else's access to restricted areas.

Existing controls and countermeasures should be inventoried and their capabilities analyzed. There are different models for categorizing the controls and countermeasures. One model analyzes them in terms of prevention (e.g., firewalls, awareness training), detection (smoke detectors, audit trails, and logs), and response and recovery (account lockout after three failed login attempts, restore procedures). Another model classifies them by objective: confidentiality (access controls, proper disposal methods), integrity (data entry verification, monitoring for rootkits), and availability (off-site storage of backups, fail-over). A third model, found in guidelines from the National Institute of Standards (NIST), classifies controls as managerial (plans, policies, standards, and assigned responsibilities), operational (documented procedures, testing, design, and architecture—whether physical or logical), and technical (identity management tools, locks, encryption).

The analysis should also determine the effectiveness and adequacy of the controls. Do water sensors really work, and does somebody react to the alarm? Can the backups be restored on the equipment designated to be used during recovery? Are existing policies sufficient?

Putting together information from the analysis of threats and vulnerabilities, as well as of controls and countermeasures that are in place, provides a picture of an institution's current state of readiness to deal with incidents.

Conduct an Impact Analysis

A security incident or a disaster—or even the lack of controls—will have an impact not only on an institution's ability to carry out its key functions but also

on its financial resources and reputation. For example, a natural disaster can cause enrollment to drop in the following semester, or researchers may be denied grants if a major security breach has occurred. Assessing the impact on reputation is usually in terms of a qualitative scale, such as high, medium, and low or a rating of 1 to 10. Financial impacts may also be rated qualitatively, whether in ballpark figures or according to some formula. The financial impact analysis should take into account the costs of response and recovery; the costs of downtime, if any; potential legal or liability costs; public relations factors; and more.

The other element of an impact analysis is the likelihood or probability that a certain incident will occur. For a fast-track analysis, rating the probability as high, medium, or low may suffice. For a more quantitative approach, the probability can be based on the likely frequency of an incident—the range might be from 100 times a day to once every 300 years.

Develop a Risk-Mitigation Plan and the Business Case

By this point, an institution should have an understanding of what its greatest risks are. Risk mitigation involves putting in place new controls, improving existing controls, or accepting the risk (and documenting that fact). In the opinion of David Osborne and Peter Hutchinson, authors of *The Price of Government,* "Zero tolerance for risk is the wrong objective—and it is far too expensive." The proposed controls should be evaluated along several vectors: Are they appropriate to the value of the information asset and commensurate with the level of threat? Is the control feasible in terms of effectiveness, funding, technology availability, or staff resources and capabilities? Another factor is the impact of the control itself. For example, one type of control may consume more bandwidth and slow response times; another control may impose more procedures or reduce people's flexibility or freedom in using systems.

Another part of the business case for controls is the cost. Documenting standards and following them are a fairly inexpensive form of controls. Technical controls, such as an intrusion prevention system or a disaster recovery site, are bigger expenses and will require financial analysis in order to justify them to senior management. One approach is to compute the 5-year cost of ownership and break it down to an annual or even per-person cost. The value of this approach is that it forces accounting for both the initial cost and the operating costs. Another method is to calculate the return on investment (ROI) by dividing the cost of the control by the cost of the risk. A third method is annual loss expectancy (ALE), which is computed as the value of the information asset multiplied by the exposure factor multiplied by the annualized rate of occurrence.

While certain controls may represent a substantial expense, they may also address multiple risks. Thus, it is useful to use a matrix to summarize the controls and the risks they address and show the positive overlaps. In addition, a project plan for implementing the controls needs to be developed. As with any good project plan, the risk-mitigation plan needs to list the tasks, define who is responsible for each, state when the tasks need to be completed, and identify the resources needed for each task.

Establish Risk Metrics

The findings from the initial risk analysis should form a baseline for future comparison. An institution should also define critical success factors, or desirable outcomes that measure the success of the solutions implemented. One example from the security arena is reducing the amount of time staff spend dealing with infected systems; another might be setting the standard that no one host can give intruders complete access to the network if that host is compromised. On the disaster side, an example of a measurable outcome is that within 24 hours of the complete destruction of the phone system, 15 percent of normal inbound and outbound call volumes are being handled.

■ Physical Security

Physical security involves protecting those physical assets that support communication technologies for voice, data, and video, along with the information they contain or transport. The incidents to be protected against may be caused either deliberately or unintentionally, whether through an accident or negligence.

Assets

The assets to be protected are varied. First on the list for controlled and limited access are telecommunications spaces—the rooms and closets that house equipment and cabling. Under ideal circumstances, telecom rooms and closets are dedicated spaces, but sometimes they are shared with other campus departments or may even contain co-located equipment owned by external third parties. Other areas include the pathways and spaces for both inside and outside cabling and for termination, including conduits, vaults, manholes, steam tunnels, junction boxes, pedestals, and the demarc. All of these should be designed to prevent tampering or accidents.

Telecommunications equipment, which is usually housed in equipment rooms (or closets), derives most, but not all, of its protection from the space it occupies. This is not true, however, of wireless equipment, such as access points,

free space optical equipment, or satellite dishes. End devices, such as a console, or client devices used a terminal also need to be safeguarded against unauthorized access or even against physical reconnaissance tactics, such as watching an administrator key in passwords. Other assets to protect include the electrical and HVAC supporting systems.

Finally, documentation, files, and records pertaining to telecommunications systems should be physically secured, whether on paper, disk, or tape. It is good practice to label system documentation as confidential and keep it in a locked drawer or cabinet. In addition, paper records or printouts with sensitive information should be shredded, and disks and tapes should be destroyed or degaussed when they are discarded.

Standards, Procedures, and Technical Controls

Protecting assets, detecting breaches of physical security, and responding to incidents are achieved through a combination of managerial and operational controls, such as standards and procedures, along with technical controls. Clearly documented standards and procedures are a requirement for passing a compliance audit. For physical spaces, a good external source of standards is found in the construction industry's MasterFormat™ 2004. The MasterFormat document contains three divisions pertaining to telecommunications: (25) Integrated Automation, (27) Communications, and (28) Electronic Safety and Security. Other standards and procedures already mentioned include controls on documentation and media and their proper disposal.

Physical design and architecture is another aspect that must be controlled. Placing a network operations center with biology or chemistry labs on the floor above is an invitation to problems. Similarly, although laying loose network cabling above ceiling tiles may make life easy for technicians, it also accommodates those intent upon mischief. Designing multiple layers of controls and diversifying controls do not guarantee against loss, though these measures do help prevent losing everything at once. For example, uninterruptible power supplies take over during brief power outages, but generators serve as a safeguard for extended power outages.

Technical controls support both prevention and detection of incidents. Locks prevent access to critical and sensitive areas. Access can be gained by using keys, cards, PINs, or scramble codes. Biometrics (e.g., handprint, fingerprint, voiceprint, or iris or retinal scanning) constitutes another method, though it tends to be more expensive. Regardless of the type of lock, questions to consider include whether the lock maintains a log of who has entered the area and whether the control device needs electrical power or network connections to function.

Detection through technical controls encompasses monitoring and alarming. Monitoring methods include cameras, motion detectors, door status, and glass-breakage detectors. Particularly with respect to security cameras, the technologies for recording and reviewing the video images need to be considered. In all cases, procedures should be in place for regular review of the logs and reports from monitoring, including sign-off that the review has taken place.

While the monitoring devices detect an intrusion or violation of normal status, the alarm provides notification that an incident has occurred. When designing an alarm system, consideration should be given to the system of notification, who is to be notified, and procedures for response and escalation.

Reviewing, testing, and auditing of the controls should be done on a regular basis to uncover weaknesses and gaps. For example, procedures should be reviewed to determine whether they are being followed and whether they still make sense. Alarms should be tested periodically to ensure that they work.

Finally, part of the ongoing responsibilities of IT and telecom management is to ensure maintenance of the standards and procedures and to budget for maintenance and upgrade of technical controls.

■ Disaster Planning

Disaster planning (which means planning how you will respond to a disaster, not planning a disaster, of course) helps an institution ensure that its mission-critical functions can survive a disaster. This section discusses the concepts of disaster and business continuity, responsibilities of disaster planning, disaster activities (detection, recovery, and restoration, as well as the use of alternate sites and operations centers), postdisaster concerns, response teams, testing and training, and maintaining the disaster plan.

Definitions

Terminology with various connotations is applied to planning and management of major incidents that physically disrupt an institution's operations.

- *Disaster recovery management* has an implied objective of returning services and functions to their previous state.
- *Disaster management* is broader than just recovery and includes preparations, prevention, and the option to replace the previous state with new and improved facilities and systems.

- *Business continuity management* also has the purpose of avoiding or mitigating risks and attempts to ensure that mission-critical operations carry on in spite of a disaster.

A *disaster* is an event that causes serious loss or destruction. The Federal Information Processing Standard (FIPS) 199 defines standards for rating incidents; for example, a high rating can be assigned if an incident would result in "severe degradation or loss of mission to an extent or duration that the organization is not able to perform one or more of its primary functions" or if there is major damage to assets, major financial loss, or catastrophic harm to individuals. Events that are disruptive but minor (a brief power outage) are outside the scope of disaster planning and management. Instead, these should be addressed through regular operational plans.

When faced with a disaster, an organization proceeds through a series of stages. First, the incident is detected, and, if feasible, those on the scene may try to contain and/or assess the damage. They also notify appropriate authorities. Based on the damage assessment, an authorized person may declare a disaster and activate the disaster plan. Notification is sent to the people responsible for responding to the disaster, who then carry out continuity of operations and recovery procedures. When services are restored, an authorized person can declare that the disaster is over. Afterward, it is a good idea to debrief those involved and capture lessons learned that can be used in improving the disaster plan.

Considerations

It is important to understand that despite the best planning, disasters can occur and events will not unfold exactly according to the scenarios in the disaster plan. This does not mean, however, that it is not worth having a disaster plan.

A good plan should be workable and should incorporate sufficient preparations to respond to disasters. It is also important to appreciate that the plan is a living document that requires regular maintenance—there will be changes to priorities, risks, tolerance levels for risks, and systems. Testing the plan can reveal the need for changes.

Disaster Planning Responsibilities

The group responsible for developing a disaster plan should be chartered and empowered by senior management. The group, along with its sponsor, must define the objectives and requirements for disaster planning and make an upfront decision regarding the scope of its planning activities. Disaster plans may be

restricted to centralized IT services, or they may cover decentralized IT functions as well.

Those responsible for the plan also need to identify and prioritize mission-critical functions and the systems that support them. For mission-critical functions, the group should discuss methods for recovery and alternative handling, including manual processing. Knowing the options currently available—fail-over, off-site capabilities, even insurance—is helpful. It is also advisable to discuss and document whether any activities can be suspended or at least postponed (and for how long).

The disaster planning group needs to define the scenarios and events that will be considered disasters and categorize these as major, moderate, or minor. Considerations include the impact of the event on aspects, such as health and safety, core mission functions, and finances. Another factor to consider is the anticipated length of the incident and the time to recover. The focus should be on major and moderate disasters, not minor ones. The group should also define authority levels for declaring various kinds of disasters.

Membership in the disaster planning group will extend beyond IT and telecom. Participation, if not full membership, is needed from such departments as facilities, safety and security, human resources, finance, public relations, and even legal counsel, as well as key users representing mission-critical functions. The disaster planning group will also need to coordinate and plan with external organizations, such as local public safety officials, vendors, and any third party that has interfaces for exchanging data with the institution. As a preliminary, the institution should have service-level agreements regarding these interfaces, and these agreements should incorporate provisions for security and disaster planning and testing.

Internal departments and external organizations should not only be involved in creating the plan but also into actually preparing activities. Finance, for example, should create accounting codes for disaster expenses and set aside contingency funds. Purchasing should set up open or blanket purchase orders for replacement equipment and recovery and restoration services (nonequipment examples include cleanup, data recovery, paper recovery, furniture and supplies) and put in place pre-loss contracts with vendors for supplying the equipment within a specified time. Human resources should revise policies to accommodate preauthorization for overtime and overtime compensation or travel to off-site recovery centers. Public relations should develop communications plans to deal with various audiences, including students, faculty and staff, the media, the community, parents, alumni, government agencies, and other interested parties. Other preparatory activities involve management, such as designating authority

to override normal policies, procedures, and standards and working out escalation procedures for resolving problems and conflicts.

The disaster planning group also needs to review existing documentation. A thorough review would cover the following elements:

- Physical layouts of spaces, rooms, and closets
- Physical access controls (keys, cards, alarm codes), who has access, and who is allowed access
- Power diagrams
- HVAC, fire detection, and suppression
- Pathways and conduits
- Cabling diagrams and records
- Telecommunications systems configurations
- Hardware and software inventories, licenses and software keys, passwords, configurations, and the amount of disk space, memory, CPU, and bandwidth needed
- Dependencies among systems and applications
- Procedures for installation, configuration, testing, and other recovery activities
- Inventories of supplies, such as cabling, forms and printing paper, manual checks, and so on
- Information about alternate site(s) and operations center(s)
- Copies of contracts
- Contact information for disaster response team members
- Skill set inventory for disaster response team members
- Contact information for utilities, professional resources, vendors, and suppliers for telecommunications and IT, office equipment and supplies, reclamation and cleaning, and other services
- Contact information for local fire and safety and other authorities (e.g., FBI, National Guard)
- Contact information for public relations
- Insurance policies

Any identified gaps in the information should be addressed. Some of this information will be included in the plan, while other parts of it should remain separate. The planning group will need to determine how much detail to gather while planning and what to include in the planning document.

The published plan should also include a revision history of the plan; statements on the purpose, objectives, and scope of the plan; information on how to use the plan; standards for updating the plan; definitions; and assumptions. Assumptions explain how functions and systems were prioritized, recap information from risk and business impact analyses, and describe funding levels. Following the assumptions, the plan might include a list of topics that will be addressed in future versions. The published plan should also describe the disaster team organization, their training, and the testing of the plan. The plan should also address the various stages of a disaster and detail the procedures (required and optional) for each stage, along with who is responsible for performing particular tasks, the specific outcome needed, and how long a task should take.

When the plan is complete, the disaster planning group must determine how to distribute it and to whom, and they must control that distribution. Often, the copies of the plan are numbered. There should be procedures to recover copies of the plan from anyone who terminates employment or whose job responsibilities change.

Detection and Initial Response

Measures or controls for detecting an event or incident may be in place. It may be as simple as someone being present and knowing the criteria for determining a possible incident, or it may involve monitoring systems and alarms. Procedures (and training) should emphasize that the health and safety of personnel takes priority over responding to the event. The procedures should include instructions for evacuation, determining that everyone has evacuated, assembly at a predesignated location, and conducting a head count.

Sometimes, automated response mechanisms have been implemented to minimize the impact of an event. To ensure safety, emergency door releases may be activated. For counteracting primary or secondary effects of a disaster event, automated response mechanisms include FMS 200 fire suppression or sprinklers, smart UPS shutdown, or even automatic air-conditioning shutdown. Manual intervention may also be required—for example, staff may disconnect lines and cables, cover equipment with hoods, or use a fire extinguisher.

Notification of appropriate personnel is another part of the initial response. Authorized personnel will conduct and/or collect assessments of the situation and decide whether to declare a disaster. As part of the disaster declaration, the authority in control will need to determine which incident response teams are needed and invoke the necessary recovery options. If the disaster is severe enough, the options might include recovery at an alternate site, use of manual processing, and contacting vendors for cleanup and replacement of equipment, supplies, and furniture.

Alternate Sites and Operations Centers

An off-site location for temporary recovery and alternate processing is becoming an imperative. An institution with multiple campuses can operate and maintain its own facility. The distance to the facility needs to be evaluated in terms of the risks faced. Earthquakes and hurricanes can affect fairly large areas, whereas disruption by fire or an act of terrorism may be more localized. Other options for alternate sites include reciprocal agreements with another organization or contracting for a commercial recovery center's services. Travel and lodging must also be taken into consideration when selecting an alternate site.

A primary operations center and a backup operations center (also known as a command or control center) should also be established; one of these may be in the alternate site. The operations center is where the disaster management team is headquartered. If the alternate site and/or the primary and backup operations centers do not exist, then the disaster plan group should require plans and funding to establish them.

Many factors need to be considered when selecting and equipping operations centers and alternate sites. Communications requirements include data network connections with sufficient bandwidth, voice network connections, phones, cell phones, radios, conference bridges, and extras, such as cables and chargers for the cell phones and radios.

Workspaces should be furnished with desks or tables, chairs, computers and printers, power strips, electrical cords, and office supplies. Whiteboards and flipcharts are useful for tracking issues and for conducting brainstorming sessions to solve problems. Copies of the disaster plan and other documentation should also be on hand. Other useful supplies include extra flashlights and batteries, cameras or recorders to document conditions, taping supplies, and labels. Work gloves and masks and even deep-water boots might need to be kept on hand.

Securing the alternate area physically and controlling access should be easy. A generator should be available as an alternate power supply. The area should have sufficient parking space, though it is also wise to plan for alternate transportation methods, such as shuttle buses or vans. There should also be sufficient restroom facilities, and access to showers is a nice extra.

For the comfort of those working, the area should have a stock of nonperishable foods, water, and beverages. Having blankets and pillows, and even cots, on hand is a good idea. An alternative is to prearrange lodging with a nearby hotel or motel. If there is sufficient space, separate areas for sleeping and for breaks are desirable. A break room might be supplied with magazines, books, games, music, videos, or other entertainment.

Recovery and Restoration

The disaster planning group's responsibilities include evaluating alternatives for recovery and restoration and selecting preferred alternatives using such criteria as service to key constituencies, cost effectiveness, and ease of implementation. Alternatives to processes, assets, and people should be assessed and determined. For example, if the billing system is affected, can manual bills be produced, or can the processing be done on a smaller server? Each person involved in recovery and restoration should have an identified alternate. The alternate may not have the same skill set as the primary, but with good documentation and training, he or she should be able to perform the minimum necessary tasks. Smaller institutions, for example, may have just one database administrator, but a system administrator may be able to fill in if necessary. The disaster planning group should also have identified primary and secondary locations for recovery and operations control.

The standards developed by the disaster planning group also include the minimum acceptable recovery configurations for each process and system and the minimum and maximum time frames for recovering each process and system. At a higher level, this means there should be defined operational requirements for mission-critical functions, communications, and applications. As an example, for a key administrative department, the requirement might be that after a disaster, 25 percent of calls can be routed to a different number during the first two days, while 25 percent of outbound calling can be suspended until after the end of the disaster.

In general, recovery—the continuity of operations—proceeds as restoration to full services is undertaken. The restoration may be to the same state as before, using the same equipment and software, or it may be an opportunity to move to new architectures, new technologies, or new procedures.

Communication of status is important during recovery and restoration. Status reports should focus on major elements. For example, it is easy to convey the status through color codes, such as red to indicate that something is not functioning, yellow for partial functionality, and green for normal functionality. The estimated time to resolve each element should also be reported. Finally, it helps the morale of all involved to avoid dwelling on the problems encountered, focusing instead on progress made.

End of Disaster

Criteria for determining that a disaster is over and that services have been sufficiently restored, as well as who is authorized to make that call, will have been established by the disaster planning group.

In the postdisaster phase, organizations should conduct an analysis of the impact of the event and its costs, and assess how well various activities were handled. From this assessment, a list of lessons learned can be developed, and the disaster plan itself can be updated and improved.

Disaster Response Team Organization

The organizational structure and membership of disaster response teams will vary from institution to institution and will often depend on the size of the institution. In any case, one principle is to designate an alternate for each role or responsibility identified. If there is enough depth to the organization, it a good idea to have multiple people for a single role or responsibility and assign them to work no more than 12-hour shifts. This allows one person to take rest breaks while the other one continues recovery work.

Typically, a designated disaster coordinator ensures that the necessary teams and staff members are on hand and are following the procedures and checklists. The coordinator monitors the progress of the recovery and communicates to management not only the status but also requests for resources (financial or personnel). He or she also escalates any serious problems or decisions. If some staff are at an off-site alternate location, there should be an off-site coordinator who reports to the general disaster coordinator.

Technical team responsibilities include network and telecommunications systems and infrastructure, data systems administration, database administration, applications software, operations, and end-user systems. There should also be a team responsible for testing and quality assurance. Again, at smaller institutions, one individual may be responsible for multiple activities. An important support role is someone to log activities as the technical staff are working. This person can help ensure that the checklists are completed and that the times to complete activities are logged. Just as important, this person can record improvised solutions or other nonstandard actions, in case it is necessary to undo them later or to learn from them later. Other support roles cover handling logistics, such as travel to the alternate site, obtaining supplies and food, and taking messages. Another team with a complementary role will include insurance representatives and internal audit personnel to conduct a more thorough damage assessment.

When major physical damage occurs, a facilities team will be needed for cleaning, construction, electrical work, and HVAC maintenance.

At a higher level will be a disaster management team, usually composed of executives and senior managers of the institution. As part of the plan, the disaster planning group must define the scope of decision-making authority of the disaster coordinator versus the disaster management team. The management

team must remain accessible for strategic decisions and is responsible for approving unplanned expenditures and obtaining additional resources for the hands-on teams. This team also resolves conflicts over resources and priorities. Although the team will receive reports from the working teams, members should be educated to not disturb the teams by demanding information. A preestablished schedule of when reports will be delivered helps limit their questions. The management team handles all official communications to the rest of the institution, the community, and the media. They also coordinate with community authorities, including fire and safety. Finally, the management team should support the morale of the working teams.

Disaster Response Team Logistics and Support

Each team member should be preequipped with a copy of the disaster plan and contact lists. A smart idea is to keep this information in a disaster backpack that also contains favorite snacks, pens and paper, a flashlight, an extra cell phone battery, and even a change of clothes.

The disaster planning group should also have determined which people will be granted access to buildings and spaces during the response. Team members' ID badges may have a special marking that denotes their status. If so, the disaster planning group should make arrangements with law enforcement (campus, local, and even National Guard) to accept this form of identification.

Another planning activity is to develop methods for getting team members to their designated work locations if the disaster has made roads difficult to travel or even impassable.

Testing and Training

The disaster plan should specify schedules for conducting testing and training activities. Objectives for testing are to

- prove the feasibility of the response and recovery strategies;
- locate and correct shortcomings in the disaster plan, such as the accuracy and completeness of procedures; and
- determine the state of readiness of alternate sites, operations centers, supplies, and so forth.

Testing thus feeds into updating the plan. It also serves as one method of training for disaster response teams. The main purpose of training is to help team members understand the plan and to acquire the habit of following the procedures. Another purpose is to develop teamwork and a culture of information sharing.

Various testing and training strategies can be used, including doing a walk-through or simulation, staging a mock disaster, or activating a portion of the plan, such as notification or switching to the alternate site. Another method of testing is to conduct an audit of equipment, furnishings, and supplies in the operations center or to determine whether cabling records are up to date.

Initially, testing should be limited in scope. Over time, however, each key aspect of the plan should be tested. Testing is normally thought of in terms of the response and recovery aspects of the disaster plan, but testing should also encompass disaster prevention and detection measures, such as smoke or water detectors. As systems and interfaces are newly implemented or undergo major upgrades, disaster testing should be part of the quality assurance process to certify them.

As the disaster plan matures, testing should become more challenging and complex. Whereas early testing should be announced in advance, unannounced tests can be conducted as teams become more practiced. Tests should be designed to include participation of all the different disaster response teams, including the management team and external partners from the community, vendors, and organizations with interfaces to the institution's systems.

Each test should be planned. Planning elements include objectives for the test and performance measures. Some measures are time-based (i.e., how long it takes to complete a task), and some measures are quality-based (i.e., whether tasks are finished accurately and completely). During testing, monitors can keep observation logs on which they can track the time to accomplish tasks, note comments, and grade the completion of tasks. The test plan should also schedule time for conducting a postmortem, which should incorporate a discussion of what went well and what did not, document the issues and recommendations for fixing them, and catalog any changes that need to be made to the disaster plan. The disaster planning group has the responsibility to follow through on the recommendations.

Maintaining the Plan

Determining what needs to be updated and when to update the disaster plan are primary considerations for maintaining the plan. The disaster planning group should review the plan in terms of a reality check: Does the plan match the way things are? Examples of areas to review include systems inventories, notification lists, and vendor contracts and contacts. The entire plan, including the procedures, testing objectives, and criteria, needs to be maintained regularly. Other questions that the disaster planning group should ask with respect to the plan are whether it is comprehensive enough and whether it is detailed enough.

The disaster plan should be reviewed and updated annually. It should also be tied into the change management and configuration management processes. As configurations of production systems evolve, there is a risk that recovery and restoration could be hampered by out-of-date configurations. Relevant portions of the disaster plan should be updated whenever major changes are made to existing systems or interfaces or whenever new ones are installed.

■ Summary

Nobody wants a disaster to happen, and unfortunately, most do not plan for one. To not have a security and disaster plan can be extremely detrimental not only for the university and its students but also for one's own career.

This chapter started off offering the reason, purpose, and structure of a security and disaster plan. One of the first steps in developing the plan is to do a risk analysis to determine the values of functions and information and the cost of losing these services. In going through the risk analysis, threats, vulnerabilities, and countermeasures must be detailed. As important as a disaster plan is the physical security of devices, information, and controls. Standards, procedures, and controls must be in place to maintain this security.

Next is the selection of backup sites and operations centers. The recovery and restoration of information systems, the declaration of "end of disaster," and the organization of the team must also be considered in the planning process.

For the plan to be effective, it must be managed. This means testing, updating, and constant training. Only with these elements can we be fully prepared for when, not if, the disaster strikes.

CHAPTER 5

Student Services in a University Setting

Walt Magnussen Ph.D.

Walt Magnussen, Ph.D., is the Director of Telecommunications at Texas A&M University. In addition to serving as 2007-08 President of ACUTA, he co-chairs the VoIP SIG for Internet2; directs the Internet2 Technology Evaluation Center (ITEC), a VoIP Research Center at Texas A&M University; and chairs the Operational Subcommittee for the State of Texas Telecommunications Planning and Oversight Council (TPOC). He has his bachelors and masters degrees from the University of Minnesota and his Ph.D. from Texas A&M University.

Student services on a university campus can vary widely, depending on the type of campus (residence versus commuter) and the funding strategy (cost minimization/avoidance versus profit center). The funding of these services also varies from pay-as-you-go services (where students buy what they want) to fee-based services (where options are added to the tuition) to being centrally funded by the administration. Regardless of the strategy, the fact is that students are coming to campus today with a very high set of expectations and no fear of technological changes. In fact, students are often the agents of that change.

Typically, student services are classified as either residence services or support services. Residence services usually include telephone services, such as dialtone and voicemail; network connections, both wired and wireless; and cable television services. Student support services cover a wide range, beginning with admissions services and extending beyond graduation into alumni services.

All of these services have changed significantly over the past decade. Dialtone that was once required in every residence hall room has, for the most part, been replaced with cellular telephones; touchtone and wait-in-line course registration have been replaced with online registration; and talking has been replaced with chatting. The one thing that we do not expect to change is the level of change.

This chapter will discuss the delivery of the two categories of services: residential and student support services.

■ Residential Services

Residential services include the sort of services that you would normally expect at home: telephone, broadband Internet, entertainment, and security.

Telephone Services

Of the several methods of delivering residential telephone services, the most traditional is through the campus PBX or Centrex service. While in the past, this often included the dialtone and the instrument, most campuses stopped providing the instrument, because most students were coming to campus with their own cordless answering machine. If the service includes switch-based voicemail, a feature that provides separate voicemail for students who share a room will often minimize arguments over messages not being delivered.

Long-distance service for students—once a significant source of revenue for many universities—is no longer provided by many campuses. With the low cost and popularity of prepaid calling cards and cellular telephones, long-distance service for students often does not justify the administrative overhead.

Among today's students, cellular telephone service has become one of the most popular modes of communication. Some campuses have awarded contracts to wireless telephone companies to provide cost-effective service for their students. These agreements often provide some revenue to the university or college. In exchange for the revenue, some contracts have the university assist in the distribution of the instruments and provide space on campus for a phone mart or cooperate in comarketing efforts. Two potential drawbacks to campus cellular service are (1) it is difficult to get adequate cellular penetration in dormitories, and (2) the increase in cellular traffic on campus forces cellular service providers to add cell sites on campus.

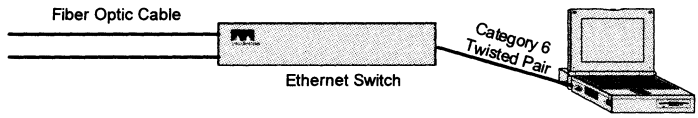
A telephony service with potential for residence halls is voice over IP (VoIP). Current VoIP services usually require either an expensive digital instrument or an equally expensive analog terminal adapter. This greatly reduces the attractiveness of VoIP as a residence hall option. The future of VoIP, however, is the session initiated protocol (SIP), an industry standard that will allow the manufacture of cost-effective instruments in a competitive market. One day a student will be able to buy a SIP phone for $40 at the store of his or her choice. Today, all major VoIP-switch manufacturers either support SIP or have it on their road map for the near future. In the meantime, making VoIP work in dorms requires either broadband network or Ethernet access.

Internet or Broadband Network Services

Access to the Internet or to broadband network service is essential to today's students. To compete with off-campus housing, the college must provide this access. Although there are many methods of provisioning the service, the one that is selected will make little difference to students, because all work equally well. Instead, the decision is primarily a function of cost of installation and maintenance, which are both typically driven by the type of building construction and existing facilities. The various services include copper Ethernet, cable television modem, DSL, and wireless Ethernet.

- *Copper Ethernet:* This service usually involves installing fiber-optic cable to the residence hall and connecting it to an Ethernet switch (usually at a billion bits per second) installed in the communications closet. The switch is then connected to a connector in the room in the residence hall via Category 6 twisted-pair wire (capable of supporting gigabit speed). The switch is typically configured to connect the student at either 10 or 100 Mbps and will autosense to adjust the switch to the appropriate speed. (See Figure 1.) Most universities place one connection per bed.

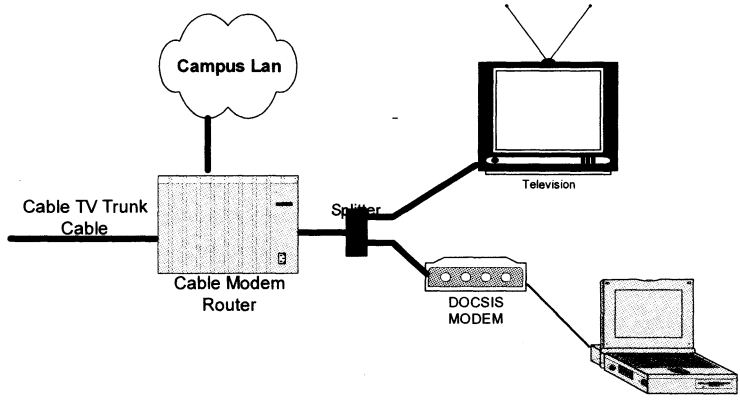
Figure 1. Fiber-optic cable to the residence hall



One drawback to making a 100 Mbps connection available to each student is that students' insatiable hunger for bandwidth can easily overload the campus network if some sort of traffic limiting is not set into place. This will be discussed in more detail later in this chapter.

- *Cable television modem:* If an existing cable television plant engineered with two-way capabilities and high bandwidth (typically > 1 GHz) is already in place, it is possible to provide broadband service through cable television modems. This service can be provided through a cable television service provider for a monthly cost per connection, or the university can buy the cable modem router and provide the service itself. All cable modems are now standards based (DOCSIS), so the campus can either provide the modems or direct the students to the electronics equipment store of their choice. Cable modems communicate with

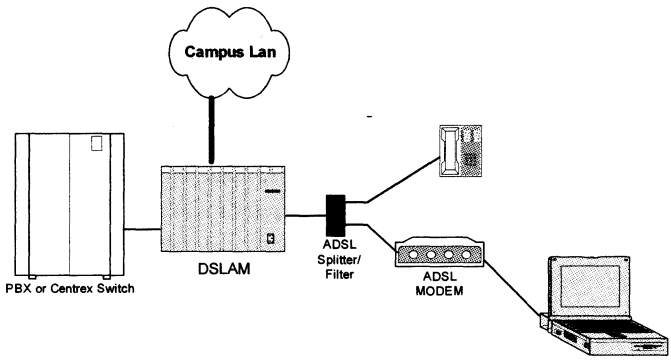
Figure 2. It is possible to provide broadband service through cable television modems



the cable modem router on one or more television channels that are not used for entertainment programming. To the student, the connection is via Ethernet, so the equipment that comes standard with all computers today is sufficient.

- *Asymmetric digital subscriber line (ADSL):* Like the cable modem, ADSL is a viable solution if installation of Ethernet wire is either impossible or not cost effective. Also like cable modem service, ADSL can either be provisioned by the telephone company for a monthly cost per connection or by the college or university. ADSL is the most common in-house network solution for apartment complexes, since it requires no additional wire. Instead, it runs on twisted-pair telephone wire, which is sensitive to the distance between the concentration device and the ADSL modem. Safe cable lengths are 12,000–15,000 feet. Because the concentrator is usually installed in the residence hall, this is typically not an issue. The ADSL concentrator, called a digital subscriber line access multiplexor

Figure 3. The DSLAM connects to the telephone switch and to the campus LAN and combines the two services onto one twisted-pair wire.



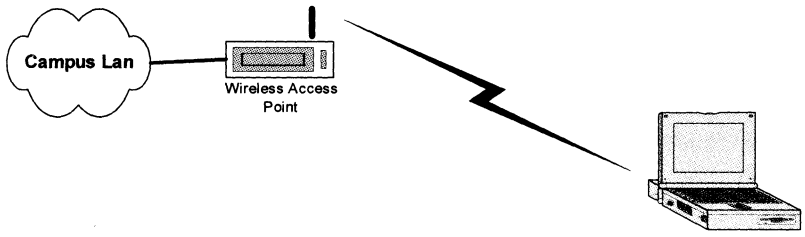
(DSLAM), connects to the telephone switch and to the campus LAN and combines the two services onto one twisted-pair wire. (See Figure 3.) The current version of ADSL supports student connections up to 2 Mbps. Newer versions of ADSL will operate at speeds of up to 6 Mbps. Like the cable service, the modem interface is standardized, so students could get their own modems. There are about six current standards for DSL, however, so a little care in selection is wise, and providing students with guidelines or suggestions helps everyone.

- *Wireless Ethernet:* Many campuses are bypassing any wire-based service and are going straight to wireless Ethernet. With this method of provisioning, wireless connection devices, called access points (APs), connect student computers to the campus network. (See Figure 4.) The IEEE defines three versions of wireless Ethernet: 802.11a, 802.11b, and 802.11g.

There are various members of the wireless family. The oldest is called 802.11b, or "b" for short. The 802.11 surname comes from the IEEE standards committee that created "b" many years ago. B operates on the 2.4 MHz frequency band and is relatively slow. B's successor, "a" (same surname), operates at a higher frequency (5 MHz) and thus has very different user characteristics and is much faster (54 MBps). The latest member of the family is "g," which operates at 2 MHz but at the same blazing speed of "a"—54 MBps. Most PCs today come with cards that operate at the "g" and "a" standards.

Most APs now support all three standards. The 802.11X systems operate in either the 2.4 GHz or the 5.8 GHz spectrum. Since these two frequency bands have different characteristics in terms of how far they will carry and how well they work through walls, the proper design of a network that will ensure 100 percent coverage can be tricky. The design is also affected by the construction of the dorm—sheetrock vs. brick walls. For the most part, an access point will cover

Figure 4. Wireless connection devices, called access points (APs), connect student computers to the campus network.



a 100-foot radius. Institutions can use design tools to create a network appropriate for its campus layout.

Security is a concern with any technology and is especially acute with wireless technologies. There are many methods of securing a wireless network. One popular method is WPA (WiFi Protected Access), which requires a passphrase to ensure that users are who they say they are. WEP (Wired Equivalent Privacy), the oldest of the wireless security mechanisms, attempts to use encryption to give wireless access the same security as wired access. Encryption implies that the actual data transmitted is changed through a code, so only the intended receiver can interpret the message. Another mechanism is a VPN (virtual private networks), which can be used for both wired and wireless networks. VPNs use an encryption and authentication scheme to secure the message while it is in transit. There are many other wireless security tools (i.e., SSID and 802.11i), all of which are beyond the scope of this book. We suggest you reference Chapter 3 and do further research before choosing a schema for your campus network.

- *Other dorm Internet access issues:* Campuses considering providing a dorm network service should take into account four other issues, which are the same regardless of the method of provisioning selected.

1. Limiting access from the dorm network to the campus network: Dormitory networks seem to have taken on the generic name of "resnet." These are typically separate networks that are interconnected to the campus network. As discussed earlier, students have the propensity to utilize every bit that campuses make available to them. If left unrestricted, most resnets could bring the entire campus network to its knees. In addition, some applications are considered by the institution to be more appropriate, such as accessing library systems or courseware, while others are considered less appropriate, such as peer-to-peer music sharing. In an effort to mitigate this problem, many campuses have injected a device referred to as a *packet shaper* between the resnet network and the campus network. Packet shapers have the ability to limit either the amount of traffic flowing between the two networks on a time-of-day basis (i.e., 15 Mbps between 8:00 a.m. and 5:00 p.m., then unrestricted after hours) or the type of traffic (i.e., 70 percent of available bandwidth for http or Web traffic, 20 percent for SMTP or e-mail, and 5 percent for peer-to-peer and other traffic). A combination of both methods may also be put in place.

2. Legal requirements to limit peer-to-peer traffic: As a result of applications such as Napster and Mozilla, which make sharing of data easy to do and difficult to find and block, the Recording Industry Association of America (RIAA) has taken a strong stance on the legality of sharing copyright-protected data such as music. When the student violating the law could not be located, the RIAA has held the college and university responsible. The RIAA has issued several "John

Doe" lawsuits, in which they provide the Internet address of the offender and make it the responsibility of the institution to identify the student associated with that address at the time given. Most networks use dynamic addresses, which often change on a daily basis. As a result, universities are now expected to log the Internet address issued against the person so they can go back to the log records to see who was sharing the information on a given day should such a lawsuit be issued.

3. Virus and worm protection: The first day on campus can be an exciting time for students but a nightmare for network administrators. In many cases, new students' computers have no virus protection, or the virus protection may be out of date or turned off. In addition, many of the operating system security patches have not been applied. This large influx of viruses can wreak havoc with any network. Many universities have installed systems that probe each new computer that connects. If a computer is found to be infected, the connection is limited to a site that allows the computer to download security patches. Once the computer is found to be "clean and protected," it is allowed to reconnect to the whole network.

4. Support for student computers in the dorms: Supporting student-owned computers in the dorm raises several issues. Problems can occur in connecting the computer to the network, recovering from a disk crash, installing new applications, or cleaning up an infected computer. Some students can handle complex problems, while others can't do anything beyond using the basic applications. Because the computers are personal property, there may be limits as to how far the campus wants to or can provide this support. Solutions that campuses have used include contracts with outside vendors who provide this support, informal student self-help groups, and campus-supported hardware and software help facilities.

Cable Television and Entertainment Services

Another service students expect is a robust entertainment service or cable television. This service can be provisioned by (1) contracting with the local cable television provider for all services, both to campus and distribution on campus; (2) purchasing a bulk plan from the local cable television service provider and self-maintaining the distribution plant; or (3) building a head-end to bundle the channels and self-maintain the cable plant on campus.

To further explain the process, there are three components to a cable television service:

1. *Payment for the programming:* This involves paying the royalties on a per-channel, per-month basis for the right to redistribute the programming. The cost

per channel can vary widely from free (for informational channels) to a few dollars (for sports channels, such as ESPN). The programmers also offer very significant discounts for purchases of large numbers of connections. As a result, it is very unusual for a college or university to go directly to the program owner. Cable television companies buy access in terms of millions of subscribers. In addition, competitive aggregators will commit to large numbers of subscribers at very low rates and resell these services.

2. *A head-end that combines all the channels into a single broadband service:* This typically involves satellite receivers and off-the-air antennas (for local channels) that pick up individual programming. These programs are then modulated onto a specific frequency (i.e., channel 2 or channel 3). The channels are then combined to create the broadband service. This can be done by either the local cable television service provider or the campus. If done by the cable television provider, it will be delivered via either coaxial cable or single-mode fiber-optic cable.

3. *Campus distribution:* Once the broadband service is created, it must be delivered to the dorms. This is usually done over cable television trunk cable. The cable plant can be built to support anywhere from 200 MHz (about 30 channels) to 1.2 GHz (more than 100 channels). It can also be built as a one-way plant (basic cable television only) or a two-way plant (supports not only basic cable television but pay-per-view and cable modem services as well). Because the coaxial cable requires frequent reamplification of the signal, the plant can be built as a hybrid, using coaxial trunk cable and single-mode fiber-optic cable for longer runs. The fiber requires modulators that convert the coaxial signal to fiber and demodulators that bring it back to coax again. This is an optional process and is only required if the span of the network covers several miles.

Other cable television issues include the following:

- *Digital cable:* Many cable television companies are in the process of converting some or all of their networks to digital. The FCC has set guidelines as to when all new television sets need to be able to support digital programming. Until all sets have been converted, it will be possible to install set-top converter boxes. The conversion from analog to digital will allow for up to four channels to occupy the bandwidth of one of today's conventional channels. As the industry makes the conversion, campuses that own their own cable plant will need to decide if and how to make the conversion. The advantages of digital cable are the ability to add more programming channels and the ability to support pay-per-view.

It is important to understand that digital television and high-definition television are not synonymous. Digital television implies that the signals are transmitted to the user (via satellite, cable, or fiber-optic cable) in digital form (as opposed to analog). Digital signal transmission allows for decreased noise, ease of transmission, and (with encoding) more signals transmitted within the same space. Digital transmission does not imply increased quality of transmission. CDs

and DVDs are digital, but they carry the same quality of information that their predecessors did.

High-definition television (HDTV) is digital in nature, but it also provides increased information and, therefore, quality. The new HDTV will be different in its aspect ratio (shape of the image) and its clarity of image (20 times more content information). Final standards for HDTV are still undetermined.

- *Pay-per-view television:* Many service providers either have added or are in the process of adding pay-per-view programming. This typically involves offering current-run movies on a pay-as-you-go basis. Some providers make this available to campus networks by providing the movies, billing and collecting from the students, and then providing a commission back to the college or university. Most pay-per-view services work on two-way cable plants way so that the ordering request can be sent from the viewer to the network. However, it is also possible to order the movie out of band, such as over the Internet or over telephone lines.
- *IP television (IPTX):* While IPTV is not widely used today, some firms are converting the programming to IP traffic and delivering it over the campus network. Although this is likely to be the direction that all cable television will take in the future, as things like fiber to the premise become more common, the cost of digitally encoding many channels and packing them into TCP/IP packets is currently cost prohibitive.

■ Student Support Services

While it can be argued that all services on campus are in some fashion student services, the rest of this chapter is going to focus on two specific IT-centric student services: student information management systems (SIMS) and course management systems (CMS). These services are a part of the daily academic life of college students, beginning with the application process and lasting all the way through degree application.

Student Information Management Systems

SIMS applications serve many student-support systems. They are typically large, complex databases residing on Unix servers. Modules that students typically interact with include the following:

- *Application:* This is typically a Web-based system that allows students to complete college entrance applications, submit transcript transfer requests and entrance essays, and track the application process.

- *Course enrollment:* Allows students to enroll for individual classes each semester or quarter. Student access to this system is also usually either Web-based or through an interactive voice response (IVR) system (i.e., phone registration).
- *Financial aid:* Allows students to apply for and track financial-aid requests.
- *Student activities:* Allows students to keep up with current activities on campus.
- *Student housing:* Allows students to apply for on-campus student housing, track the application process, select a roommate(s), track meal plans, and check fee balances.
- *Library:* Allows student to read on-line subscriptions, check periodicals, reserve books, and request interlibrary loans.
- *Degree audits:* Helps students select the appropriate courses and apply for a degree when that time finally comes.
- *Alumni:* Allows former students to keep in touch with each other, keep up with the university's current events, and provide financial support.

These are just a few examples of the many types of student-support systems that enhance the daily lives of students. Countless others could be included in a comprehensive list. While these are often stand-alone systems, it is important to think of them in terms of a comprehensive system. A single-portal front-end system with a single sign-on often makes the difference between a positive and a negative image in the eyes of the students.

Course Management System

One type of system that deserves separate attention is the course management system (CMS). There are many CMS vendors, but WebCT/Blackboard and Angel have emerged as the two leaders in higher education. These systems allow faculty members to communicate more easily with students. CMS components often include the following:

- *Course syllabus:* Allows students to clearly understand course objectives and student expectations.
- *Notes posting:* Allows faculty to post notes online.
- *Class e-mail:* Allows faculty to easily send e-mail notices to the entire class. Often will allow students to e-mail the class as well.
- *Student collaboration:* Allows students to instant message (IM) each other or faculty. Also allows class chat rooms and bulletin boards.
- *Homework:* Allows faculty to post course assignments online and students to submit homework online.

- *Test module:* Allows the faculty to give online examinations to students.
- *Grading module:* Allows the faculty member to post grades online.

Other Student Services Considerations

There are three other concerns that need to be mentioned in concluding the student services chapter.

Know Your Students' Habits

When designing support systems for students, remember that students do not keep the same hours that faculty and staff do. On most campuses that offer long-distance service, the busy call hour is either 11:00 p.m. or 12:00 midnight. Support structures need to facilitate student needs.

Know What's Coming

Always keep an eye out for what is trendy. Students are often driven by peer pressure, which places a significant amount of importance on what is in vogue. Case in point: Many of our campus networks were forced to change overnight by the sudden popularity of peer-to-peer music sharing. Another example is the financial impact that student migration from on-campus long-distance to cellular services had on many telecommunications departments.

Know Who You Can Count On

While there are often many partners that can and should be involved in the delivery of new student services, *never* underestimate the importance of student involvement. Most campuses have student leadership organizations that are composed of some of the smartest, hardest-working people you will ever meet. Coupled with this intelligence and drive is an energy level that, if harnessed, can lead to great things. Often the easiest way to sell a new project to administration is to let the students sell it for you.

Summary

The residential services that are usually offered in a campus environment include telephone, broadband Internet, entertainment, and security. There are various alternatives for delivering these services, including installing DSL or stringing

new cable. The delivery service you choose is less important than deciding on the services that your campus should offer to students.

Student support services are usually included in a logical student information management system, which provides the basics to students—financial aid, course enrollment, student housing, and library systems, to name a few. Another student support service typically offered is a course management system to aid in the delivery of instruction to students

Whatever services your campus offers, attention needs to be paid to knowing student habits, knowing the technologies that students want, and knowing who you can count on when implementing student services.

CHAPTER 6

Administrative Services

David E. O'Neill

Dave O'Neill is currently the Executive Director for the Office of Information Technology at Boise State University with responsibility for the university's mission critical applications of voice, video, data, and print technologies. He holds graduate degrees from the University of Montana and Washington State University and has served as ACUTA President. O'Neill has also published numerous articles regarding infrastructure design and implementation, technology planning, and IT organizational development, and has regularly spoken to a wide variety of audiences regarding these topics.

Both the role of technology managers and the technology they provide are becoming ever-more complex. Today's IT managers are expected to share the vision and understand the mission and goals of the enterprise they serve so as to propose, position, and manage technology services that advance the enterprise.

The trend toward more self-service and Web-based services coincides with a greater demand for IT managers to understand the basic functional requirements of the business: its work flows; access, security, and regulatory requirements; appropriate and available software applications; network architectural requirements; and political constraints that create parameters for the environment in which services are provided. The technology manager must also possess the skills to effectively manage complex, often high-cost, and highly visible projects that result from the need to acquire or develop IT applications and services.

The intent of this chapter is not to describe technology's role in the process of strategic planning, although that is significant. Nor is the intent to advance technology's role as a project management resource, even though such capabilities are increasingly being provided throughout the enterprise by the IT- based organizations within the enterprise. Instead, the intent of this chapter is to provide a brief description of those most common services provided and supported by an IT organization and the relationship between those services and the communications requirements they demand.

In addition, this chapter will focus specifically on what has, for convenience purposes, been defined as "administrative" services as opposed to "student" services. This rather arbitrary distinction creates the illusion that data in some way can be defined as one or the other, that data can be managed as one or the

other, and that systems are therefore architected as one or the other. In reality, a clear distinction between the two at the data level does not exist for most enterprise-level systems. Data are administrative- or student-centric contextually and, therefore, dependent on the functions and services they support. Data repositories supporting enterprise systems are carefully indexed and cross-referenced storehouses. These storehouses may also defy a simple labeling. Such repositories have traditionally been a single large database managed centrally. However, as more services become increasingly complex and dependent on a broader spectrum of data, repositories are becoming increasingly more scattered throughout the network and are less likely to represent a single centralized database. Data repositories are managed within a clear set of rules by which specific applications capture, record, store, and update data. These data are then available to all other applications for the provision of services associated with that particular application. Thus, databases are becoming more of a logical concept rather than a physical location.

The provision of services is dependent on access, which is no longer temporal or space bound. Access to services once available only during normal business hours and only at an arm's length has now become independent of time and location. A vast and growing array of technologies now creates self-service applications and environments that provide services on demand. These technologies and their resulting applications represent a significant investment in financial and human capital. They are often the result of enterprisewide visioning and planning efforts, are often highly visible, will consume significant resources with regard to their implementation and ongoing support, and are regularly touted as capable of solving all enterprise ills. Even if their ability to solve all ills were a reality, the successful provisioning of services would remain dependent on access. Communications networks provide the pathway to self-service applications and the services they provide; they must provide not just access but *controlled* access as well. Access security parameters are an intricate and defining element of service provisioning. Even as applications become more capable of providing better services, communications networks that provide secure access will continue to be defined as the critical path to an application's success. Without a clear understanding of the relationships among the demand for services provided, the architecture within which applications have been constructed, and the characteristics of the communications networks anticipated to provide access, failure will be more than an option. It will be inevitable.

Enterprise Mission-Critical Applications

It is important to define, early in this chapter, the relationship between applications and services. For the remainder of this chapter, it is assumed that, in general, an application or association of applications provides the services that meet the needs of the enterprise as defined in its strategic planning documents. It is also assumed that although there are a good many demands for technology services throughout the enterprise, the applications and resulting services described in this chapter are identified as "enterprise mission critical" rather than subordinate "organizational unit mission critical." This assumption may lead some to recognize the vulnerability of subordinate organizational units within the enterprise—a cruel but often exercised reality in today's world.

As noted, many applications herein are depicted as isolated or stand-alone. Trends over the past decade have been to associate applications as modules into increasingly larger systems, which can then rely on a single data occurrence within data repositories. This reliance on a system architecture that draws multiple functions together around a singularly maintained data set is a significant strength of an enterprise system. For purposes of simplicity, however, applications and the basic services they provide will be described here as if they were individuals. Recognize that many vendors continue to amalgamate and associate these modules in increasingly more complex enterprise systems.

For some, the concept of enterprise mission critical may also carry with it an assumption of IT centralization. Although this need not be the case, and there are sound examples from both ends of the organizational spectrum, some business applications and their resulting services are more likely to be centralized. Many of the basic enterprise financial functions—payroll, general accounting, accounts payable, and accounts receivable—are such examples. It is not, however, within the scope of this chapter to assess organizational structures and their characteristics or their ability to support applications and services.

Enterprise Resource Planning (ERP)

One of the most widely recognized associations of technology-based applications today is that of an enterprise resource planning system (ERP). Characterized by the use of a single centralized data repository to support its applications, this highly integrated association of software applications provides the foundational building blocks for conducting the enterprise's business. Most often, the services

---

1 Within higher education, these applications usually include student services. However, student services are excluded for the purposes of this chapter. They are addressed in Chapter 5.

supported are the basic financial accounting, human resource, and student services[1] necessary to meet the day-to-day operating requirements of the enterprise.

Basic financial accounting services often include general ledger, accounts payable and receivable, grants and contracts or sponsored projects accounting, purchasing, inventory control, budgeting, and cash management. Human resource services may include affirmative action functions, position control and budgeting, applicant tracking, time and labor management, payroll, benefits, and training. More sophisticated capabilities now becoming standard ERP functions include modules for strategic planning and progress monitoring via scorecards and preestablished key performance indicators.

An ERP system is regularly architected as an amalgamated set of software modules, each focused on a single business function and each relying on its access to the single set of shared data within the enterprise data repository to complete its tasks. This amalgamated set of software modules works in concert. Each module is responsible for a unique business function, collecting, processing, and maintaining data elements uniquely associated with the business function supported but relying on other data elements collected, processed, and maintained by modules uniquely associated with other business functions. Transactions within the ERP system occur once, data elements are captured once, and all are maintained by a single application, resulting in information and reports generated from a single source and available enterprisewide. This creates two very strong characteristics. First, identical requests from any sources within the enterprise for any data, information, or report should yield identical results. Second, and significant, is that access to business transactions, data, information, and reports can be clearly defined and controlled in accordance with established enterprisewide policies. The final result is consistency and security.

Customer Relationship Management (CRM)

One of the fastest-growing associations of technology-based applications being deployed in higher education is the customer relationship management (CRM) system. Relying on the use of the enterprise's single database repository, this association of software services first became popular in the corporate sales environment for identifying prospective clients; managing and communicating with prospective, current, and past clients; and ensuring a consistent, timely connection between the enterprise and its customers. These applications have now found their way to the higher-education marketplace. Recognized for their ability to manage relationships by accessing common but consistent data and the application of consistent policy-based processes for recruitment, retention, and

fund-raising strategies, CRM systems have been deployed as an enterprise strategy for creating environments of connectiveness, collaboration, mentoring, and lifelong relationship development.

The entire cast of characters outside and within the enterprise—including students, alumni, contributors, supporters, parents, faculty, staff, administrators, and friends of the university—can now be connected with a single communications strategy, tool set, and data set. A CRM system coordinates a personalized series of cross-media contacts, follow-ups, and communications from diverse origins across the enterprise in a seamless and coordinated fashion. Often, a single individual is associated in multiple ways to the enterprise (e.g., alumni, sports booster, and current employee). No longer does the enterprise have to wonder which subunit contacted the individual last and for what purpose, thus eliminating possible unwanted surprises. No longer will the individual receive multiple and disparate contacts from units within the enterprise that may suggest that the right and left hands don't know what the other is doing.

Users can also expect to be directed by this set of applications to additional resources, systems, or individuals. CRM systems often act as transitional agents to direct or move users to other, more specific modules within an ERP or student system.

Again, as with the ERP systems, specific goals, tasks, and objectives established by strategic planning initiatives may formulate performance objectives that can be monitored and measured against preestablished performance indicators.

Contributor Relations Management (CRM)

Traditional contributor relations software applications are often stand-alone systems dealing with single or multiple database modules independent of those characterized by integrated enterprise systems. This isolation has many times been attributed to the need or desire to put an arm's length between the fund-raising entity and the enterprise. Associations, foundations, and other such entities commonly partnered with the enterprise for the purpose of cultivating support and raising funds are often separate from the enterprise, whether by law, common auditing practices, or the perception of unit uniqueness. They may not directly share data, systems, or support. The stand-alone systems may or may not be supported and run by the enterprise IT organization. Their isolation creates issues of data management, access, and security.

Integrated contributor relationship management (CRM or CR) systems can provide an enterprise approach to managing contributor-enterprise relationships. Again, as with the enterprise systems previously described, these integrated systems are characterized by the use of the enterprise's single data repository. The

repository captures business function–unique data elements and relies upon data elements captured and maintained centrally by other enterprise business functions. The capture and use of data by these systems begins as soon as a strategy for identifying prospects is defined. Prospect data may be the result of identifying recent graduates, supporters, or friends of alternative programs within the enterprise or may simply result from identifying those that have inquired of units within or associated with the enterprise. This may lead to the conclusion that a CRM system integrated with other enterprise systems in which data is captured and managed has significant merit. Indeed it does. The use of traditional stand-alone systems often results in the IT unit providing regular data downloads and updates to the stand-alone system. This creates the opportunity for informational time lags, duplication of data, and/or simply a greater workload for the IT staff.

Contributor relations systems—whether found as an integrated enterprise system or as a stand-alone system—all exhibit many of the same attributes. They all have the ability to create and document fund-raising strategies; plan, implement, and analyze events and campaigns; establish goals and action steps; monitor resource assignments and progress; and maintain a contributor's personal information, giving history, gifts, and contributions, whether in-kind, cash, or other assets, from initial commitment to payment.

A stand-alone system must manage correspondence, track communications, and process authorized on-line credit card donations. It must also be capable of recording and reporting financial information from the perspective of both the individual contributor and the fund-raising entity. Such data and information may then need to be "uploaded" to the enterprise financial systems on a regular basis.

Stand-alone systems are becoming less the norm, and the higher-education marketplace is seeing a gradual evolution or migration of stand-alone contributor relations applications into fully capable CRM systems.

Enterprise Performance Management (EPM)

Enterprise performance management (EPM) systems are relatively new to the higher-education enterprise, but they are becoming increasingly more popular as enterprises begin to track performance related to established strategic goals and objectives and to examine their ROI. Although the concepts of performance tracking or assessing ROI for expenditures of capital within a higher-educational enterprise are not new, the use of integrated enterprise systems to document strategies and performance measures, capture performance-related data, project trends, and communicate results is.

The use and acceptance of performance indicators, or "scorecards," for specific functions within the enterprise is also not new. Educational enterprises have historically employed metrics such as the number of new students admitted, the number of freshmen retained, the number of students graduating, the number of research dollars obtained, and a host of other tangible metrics. What is new is the availability of a comprehensive, centrally accessible, technology-based tool or system with a single database in which all who have appropriate rights are granted access to monitor progress.

These systems assist in the development and documentation of enterprise goals and objectives with associated tasks through each level of the enterprise. These objectives, associated tasks, and specific measures of success, or key performance indicators (KPIs), may be assigned to something as general as organizational units or as granular as individual employees or positions. Once established, these performance metrics can be used with trend analysis to manage and project individual or unit accomplishments; determine effectiveness and progress toward objectives and ultimately to enterprise-level strategic goals; or identify organizational units, departments, and individuals needing improvement. The desire for more careful and better-documented workforce and financial capital management will continue to drive the development and increased deployment of these systems.

Document Management

The term *document management* may seem like an overgeneralization and oversimplification for the purposes of this chapter. The concepts, functions, and tasks associated with managing information or materials collected, routed, stored, retrieved, and disposed of during the process of conducting business within an enterprise are not trivial. The term *document management* does not accurately account for the complexities of defining, categorizing, or describing the true tasks at hand. To most, the word *document* infers a written or numerical accounting, often on paper. Some have suggested using *records,* which could encompass a vast array of media and formats that often frustrate those responsible for the management of such assets. Adding the word *electronic* to *document* or *records management systems* (creating EDMS or ERMS) further confuses the issue. Of course, there is always the integrated *electronic documents and records management system* (EDRMS). For those who accept that nearly all data, information, documents, computer programs, pictures, video and audio recordings, records, and other similar such assets can and should be digitized, the term *digital asset management system* (DAMS) may come to mind. An attempt here will be to characterize a few key differentiators and establish a reasonable hierarchy in order to frame an understanding of the attributes associated with systems that touch the enormous

volume of information resources moving into, around, and back out of the enterprise.

Document imaging, or scanning a source document into a computerized data repository, is usually the initial step in a document management regime. Imaging requires digitally capturing each document, indexing it for future retrieval, identifying workflows though which it must move or be made available, and identifying the necessary security or "need to know" so it is accessed by only those authorized. Once digitized, the now-electronic documents have attached to them a set of accompanying attributes, which include (but are not necessarily limited to) initial receipt, all movements and viewings, any annotations made by those with access or processing responsibilities, and all actions taken as a result of the enterprise having received the original document. For many, the most significant action is disposal of the source document. Once digitized and stored in a data repository supported by proper archive and back-up procedures, there is no need to retain the original document. It is securely disposed of, thus freeing floor space, desk space, mailboxes, and mailrooms that were once cluttered with file cabinets, in-baskets, oversized documents, and sorting bins. Most document-imaging systems include limited search capabilities, which are effective only if documents are adequately indexed. Some document-imaging systems provide limited content search capabilities as well.

Records management casts a bit wider loop. Records can be defined as documents, information, physical objects, databases, or other digitized materials that provide evidence of business activities and transactions. In general, the processes for capturing, indexing, storing, securing, retrieving, and managing these assets are similar to those described earlier. Dependency on sound data and systems architecture and IT management practices remains.

Electronic Content Management (ECM)

The concept of content management covers a range of services, from the management of content within documents and records to Web pages and applications to most anything stored electronically. Some systems are focused on a particular segment of content management, such as text, video, webpages, e-mail, graphics, or other specific document/records content, while others offer integrated enterprisewide content management. Whether embedded within a document/records management system, deployed as an individual application, or focused on a particular niche or across the entire enterprise, the basic premise is the same. Information used to manage and make decisions is scattered throughout the enterprise in multiple formats and multiple data repositories. To ensure its value, it must be created, stored, and accessed via a central set of rules, parameters, processes, and workflows.

Most enterprises now recognize the growing necessity to manage via centrally imposed policies all materials generated from within and received from outside the enterprise. ECM systems provide an ability to create and enforce templates, parameters, and rules for creating documents, records, images, webpages, and other items authored within the enterprise. They provide a process by which an enterprise can establish policies, workflows, and access controls.

The strength of content management is the ability to manage all enterprise electronic materials from inception through final demise, establishing rules for creation, capture, access, use, and destruction.

Integrated Library Systems (ILS)

Most can recall the library's traditional data management tool: the card catalog. The application of computer systems to the card catalog and now to managing the wide variety of library resources and tasks has exposed libraries and their services. These computerized systems, not unlike ERPs and CRMs, rely on computerized data repositories and discrete software modules. Such modules include *acquisition management,* for ordering, receiving, and invoicing materials; *catalog management,* for identifying, segmenting, indexing, and storing or shelving materials; *circulation management,* for the distribution and return of materials loaned; and *serials management,* for tracking regularly published materials, such as magazines, journals, and newspapers.

The greatest advent to libraries and other repositories of stored information is the searching capability provided by digitized collection records. Computerized search engines now make fast work of what was once a tedious and insurmountable task of identifying and locating a resource. Digitized holding, interconnectivity, interlibrary agreements, the Internet, and sophisticated search capabilities have now made it possible to access facilities and resources once unavailable.

Digital Asset Management System (DAMS)

Moving toward the extremities of document and records management, digital content management, and integrated library systems are the concepts of digital asset management. Annotating, cataloging, storing, retrieving, and distributing enterprise digital assets represent the ultimate in archiving and retrieval philosophies. This system potentially represents an ability to collect, store, and retrieve all digitally recorded activities or holdings. The ability to search for and reference voice, video, data, pictures, music, art, film, and other by theme, topic, reference, or any other search criteria is ultimately powerful. The DAMS concept—albeit

ever powerful for business, education, scholarly pursuit, or entertainment—also solicits issues and dialogue regarding the need, cost-benefit ratios, rights of privacy, and copyright. Akin to electronic content management systems by function, these titles may disappear, their functionality being melded into what is today the more vogue title of *content management.*

Physical Assets Management

Some service-oriented computer applications record and maintain data regarding an enterprise's physical assets. These systems support the ability to request services; manage the provision of services; schedule and conduct planned or requested maintenance; provide maintenance staff with manufacturers' diagrams, instructions, service bulletins, warrantee information, and parts lists or necessary materials; manage and maintain the inventory of associated stores, including parts and tools; document equipment and facilities use and conditions; produce status reports and records of maintenance activities, asset statistics, and characteristics; and provide billing and invoicing. Physical assets systems often support the facilities management, physical plant, motor pool, IT help desk, and other auxiliary or self-sustaining units within the enterprise. Labeled as computerized maintenance management systems (CMMS), enterprise asset management systems (EAMS), work order management systems (WOMS), or other similar such names, all rely on a set of common data accessible to those with identified need.

Automated computerized dispatch for daily tasks or emergency requests and remote access to these asset management systems by support personnel are becoming the norm. Laptop computers and wireless handheld devices, such as PDAs and cell phones, connect management directly to the technician in the field, as well as provide that technician immediate access to maintenance records, inventories, and other informational resources necessary for problem diagnosis and resolution.

Related to and often offered as an integrated module of a physical asset management system are space management capabilities. Space management systems record building and room characteristics, including total number of square feet, use, assigned user, room conditions, and other attributes, such as size, shape, configuration, construction materials, windows and coverings, type of lights, utilities, communications and audiovisual capabilities, and equipment. Many such systems or modules also provide computer-aided design (CAD) capabilities, making it possible for engineers and architects supporting the enterprise to create and maintain these data as part of the regular changes brought about due to facilities remodeling, demolition, or new construction. The

strengths of these systems are the result of single business transactions creating single data entries and of reliance upon data repositories providing nonunique data generated from other transactions and data entry.

Telecommunication Information Management Systems (TIMS)

All telecommunications organizations within the higher-education enterprise were born or grew as a result of federal legislation enacted in the 1980s. The almost-independent businesses within the enterprise that resulted became entrepreneurial testing grounds for purchasing, provisioning, and reselling telecommunications products and services. Many such organizations quickly became the financial saviors for other businesses within the enterprise, emerging as the cash cows capable of providing services and products often more quickly and cost efficiently than outside telecommunications companies.

These newly created businesses, however, created a need for specialty applications to take and process orders; bill customers; pay providers; manage equipment, plant, and material inventories; and provide directory data. Until this time, all such functions were managed by the outside telecommunications companies. A market niche was thus created, and telecommunications information management systems were born. The capabilities of these service applications grew as the telecom business grew and matured within the educational enterprise.

Today, such application capabilities are much the same, but the modules and applications providing the basic functionality are migrating toward enterprisewide, physical asset management systems. The similarities between IT work-order processing and those of others such as IT help desks, physical plant maintenance shops, and facilities management organizations is accelerating this merger. Again, data unique to the specific business functions (e.g., phone number, equipment type, pair count, rack and patch cable, etc.) performed by the application are stored away in the data repository as the responsibility of that particular application, but nonunique data captured and maintained by other applications is available to complete the record (e.g., building name and location, room number, occupant, etc.).

Desktop Tool Sets

There exists a group of applications that most within the enterprise recognize and use regularly. The services provided by this group of software applications represent the general productivity tools for individuals. Although they are usually bundled, efficiently integrated, and widely understood, they also represent one of the greatest demands for support. The enterprise IT support desk or help desk was born out of this demand. In addition to creating computer accounts for

access to enterprise systems previously described, configuring and maintaining the services of enterprise e-mail, calendaring, and Web access—along with providing other desktop productivity tools, such as word processing, spreadsheet development, presentation capabilities, printing, copying, and Web posting—are of the greatest impact and with the greatest visibility for services provided and supported enterprise wide.

Monitoring, Signaling, and Alarms

A number of provided services often fall within the responsibility of facilities or plant management. The most sophisticated of these—and the one that is gaining significant visibility due to the rising cost of energy—is building controls. Smart building systems, or green building systems, provide an automated process by which utilities can be monitored, scheduled, and controlled within all rooms, buildings, and sites of the enterprise. Lights, HVAC, clocks, and doors can be scheduled, monitored, and alarmed with these systems. In addition to utility and facilities management system services, security and life/safety video surveillance capabilities are services regularly provided by IT organizations.

Webpage and Applications Development

IT organizations that provide support for enterprise applications may also provide design and programming for development and support of the enterprise's presence on the Web. Design and programming services vary significantly, depending on the enterprise's commitment to in-house support, its tolerance for decentralized development and support, and its willingness for fully contracted and outsourced web services.

Server and Web Hosting

Many IT organizations now provide server or Web hosting services. This is often done as an auxiliary service provided for a fee hat is based on processing demands or server shelf space. If the enterprise has sufficient space in an existing computer room with all the environmentals (HVAC and power) already in place, renting out space is an effective way to offset the fixed cost. Services often include archiving and backup, as well as operating systems and data repository management. Applications that include licensing fees, however, remain the responsibility of the "renter." Care must be taken to differentiate between services provided as part of IT organization's central mission those provided as part of a separate service-level agreement negotiated for services not identified as central mission critical.

Point-of-Sale (POS) Systems

Most enterprises maintain and manage some cash-handling operations. These may be for collecting fees and fines or for cashiering in support of the sale of products or services. Today's cash register devices are rarely stand-alone, and typically cash-handling equipment interfaces with computerized data repositories via secure network connections. POS devices are now more likely to have system interfaces capable of (1) scanning products; (2) accessing and updating data repositories for sales data, customer-specific transaction history, and account information; (3) inquiring about product inventory information; (4) conducting financial transaction authentication; and (5) acting as the drawer for collecting cash and giving change. The common thread among all POS systems is secure network access to data repositories in which transaction-unique data is collected and other necessary data are available.

ID Card Systems

The use of enterprise ID cards and the expanding number of services associated with them has grown exponentially in the past decade. Faculty, staff, students, alumni, contractors, and a host of others with legitimate associations to the university enterprise are being issued ID cards. These cards may document affiliation, provide access to buildings and events, and facilitate financial transactions. Smart cards, proximity cards, secure cards, and a growing number of additional card monikers can be attached to the processes of identity management. Although many enterprises have assigned creation and management of organizational ID cards to units such as human resources or the enterprise card office, issuing a card is just one of the final steps in identity management. An ID card is just a transitory trinket of current technology. The use of biometrics is becoming more widely accepted, and a fingerprint may soon be the trinket of the day. Many laptop computers, facilities and events, and food service applications currently use fingerprint comparisons to authenticate access and expenditures.

The organization within an enterprise tasked with identity management has a clearly defined responsibility: to collect personal identification, ensure its authenticity, and document its ability to uniquely define the individual. The parameters of such an activity are dependent upon enterprise policy, the individual's business needs, and an assignment of perceived risk. Government-issued picture identification, its verification, supporting documentation, waiting periods, and, increasingly often, background checks are all becoming acceptable practices that are often the responsibility of human resources. IT organizations are then tasked with the responsibility of recording and securing this information.

Identity management has far-reaching impacts. Within today's enterprises, the greatest technology risk is unauthorized access and the compromising of personal data. IT organizations are increasingly aware of their role in storing and maintaining personal identity data. As a result, many IT organizations, in association with the enterprise's internal auditor, provide review and auditing services enterprisewide to ensure compliance with local, state, federal, and association regulations for secure data management.

■ College/Departmental Mission Critical

Systems acquired, developed, and supported for business needs below the enterprise level are a fact. They provide needed services and may represent unit mission-critical capabilities. They may also have significant effects on the enterprise mission-critical systems, on the resources identified as responsible for those systems, and on the enterprise directly. To provide descriptions of all possible unit mission-critical systems is not possible. Rather, what follows is a summary of the reasons these systems exist, the issues associated with their existence, and the effects they all too often have on other services provided by the IT organization.

Large enterprise systems are often viewed as being inflexible, difficult to navigate, unable to accommodate a business unit's unique business processes, unnecessarily complex, incapable of being easily modified, or too expensive. These may well be true from the perspective of units that are buried inside the enterprise with few resources of their own or lacking a significant enough voice to be heard during implementation or ensuing modifications. Such units may acquire—or more often develop—shadow books, subsystems, and desktop databases perceived as being more capable of meeting their business needs within their organizational boundaries. In addition to drawing unnecessary staff, network, and security resources, however, they often demand the recapture or reentry of data already being captured by the enterprise systems. In addition, these "shadow" systems may reside on equipment that is not architected, supported, and secured to meet regulatory requirements.

These characteristics alone cause many IT managers sleepless nights. The potential replication of data—which often leads to nonsynchronized data and questions such as, "Where'd this come from?" or "Whose data should we believe and use this time?"—is second only to discovering that personal or enterprise data has been compromised from a machine that was, until now, unknown to the IT organization. Compromising personal data destroys public confidence, engages regulators, and may cost an enterprise its public image as well as hundreds of thousands of dollars in fines, not to mention incalculable future business.

A smart and well-focused IT organization provides the enterprise with a general project management and development service. This service creates the ability to hear and see what units within the enterprise are struggling with regard to enterprise-level systems. The IT organization can step in with guidance and resources to help move what could have been isolated sets of shadow books, duplicate subsystems, and desktop data repositories into the mainstream. Modifying the enterprise system, creating acceptable peripheral software or middleware, or defining requirements for the acquisition of departmental subsystems as a partnership between the department and enterprise IT organization can ensure greater efficiencies and regulatory compliance.

■ Legacy Systems

No enumeration of administrative services would be complete without some reference to legacy systems. Legacy systems may be defined as systems or applications whose functions are too essential to be disrupted by redesigning and replacing them, often despite their poor performance or lack of compatibility with other enterprise systems. These systems or applications are often also characterized as having been in operation for a long time, although this is not necessarily a definitive characteristic. The rapid change of technology, coding languages, or even business needs may render a relatively young system or application as legacy. Proprietary equipment and languages used in the past have been the greatest contributors to legacy systems.

The ongoing costs to support legacy systems that are dependent on outdated equipment or software coding, as well as retaining a qualified staff, mount quickly—as do the risks. The inability to recover from systems or software failures grows as the disparity between legacy systems and other newer enterprise systems grows. A single catastrophic failure can quickly mitigate any ROI controversy. As enterprises and IT vendors begin to realize the benefits associated with open standards, a greater number of systems and applications will be more easily updated rather than replaced in wholesale fashion.

■ Access, a.k.a. Communications

No matter how capable a set of enterprise systems or applications are at providing "just right" services, if they are not available to the individuals and organizational units demanding them at "just the right time," all is for naught. Likewise, if enterprise proprietary data or personal data is compromised as a result of providing great services, then all is for naught.

The need to incorporate communications requirements as part of systems and applications development is paramount. Enterprise IT organizations are increasingly dependent on teams staffed not only with qualified technical programmers and telecommunications engineers and competent and experienced project management officers, but also with a systems architect. This role has an enterprise view of how systems and applications fit together, how they can best be structured to coexist and complement the existing technologies of the enterprise, and how best to provide scaleable and secure access to services while still meeting the needs of those being served.

Adoption of Web-based system architectures creates parameters for communications media and protocols. The growing—if not absolute—proliferation of Internet protocols for services and applications testifies to the demand for ubiquitous access. Physical infrastructures within an enterprise are, in part, dependent on these architectural decisions. High bandwidth-rated, twisted-pair copper and fiber-optic cable have all but completely replaced the coaxial cable of proprietary systems and applications. Services are expected to be available via mobile laptop and handheld devices, which are forcing enterprises to incorporate wireless architectural requirements as part of all system updates and implementations. Growing wireless access demands have resulted in a demand for more and stricter rules for access authentication, greater expectations for improved systems and application performance rates, and a need for application formats compatible with the growing number of handheld display devices.

Services supported by legacy communications systems will not be available as demanded by those dependent upon readily accessible, timely, and secure information.

■ Summary

The needs of those being served by an enterprise as well as of those managing the enterprise can be met by an enterprise IT group if those services are preceded by effective enterprise strategic planning and competent IT project design and management. The construct of labels to identify services or groups of services is tenuous and dependent upon the tasks performed, the needs met, and the audience. No matter how well a system or application addresses the services in demand, if those demanding the service have poor or no access to the services, it's the same as having no system or application. Effective communications architectures and strategies must accompany the design, development, and implementation of systems and applications for the successful provision of services.

CHAPTER 7

The Business Side of Information Technology

George Denbow

George Denbow is assistant director for ITS Business Services at the University of Texas at Austin. He prepares financial reports, costs analysis, and chargeback models for all ITS services. He holds a Bachelor's Degree in Accounting from UT Austin.

Accurately planning and budgeting for sustainable funding of information technology is difficult under any circumstances. Current pressures of budget cuts and increased demand for advanced technology on campuses exacerbate the issue. Yet some institutions have found ways to integrate long-term funding with strategic goals and effective planning processes and now have comprehensive, sustainable funding plans in place. Reaching this goal requires understanding new and emerging technologies, institutional goals, the current state of technology on campus, and effective strategic planning.

Business and finance officials and IT managers at both public and private institutions should know what options they have when the time comes to finance a new telecommunications system. This chapter will summarize the financing options available to higher-education administrators, whose goal is to ensure that the system is financed at the lowest possible cost to the institution. Topics for this chapter include assessment, institutional and departmental strategic planning, budgeting for capital and ongoing expenses, maintenance, personnel, and emerging thinking and new trends on long-term IT funding.

Public Institutions

In most institutions, the telecommunications director or a vice president is responsible for the quality of communications on campus and is usually the most informed campus official with regard to the effects of structural changes in the telecommunications industry. As voice, data, and video technologies have converged, so have the responsibilities of those who manage them. Increasingly,

one person is responsible for all forms of communications on campus, and his or her title may be CIO or director of communications. From the beginning, this person should work closely with financial staff so that the limits of what the institution can afford are clear. Such teamwork should be established before the system is bid. (If there is no agreement on how to pay for the acquisition, hiring a consultant or working with a vendor to create a request for proposal [RFP] will be a waste of time.)

The institution's finance officer should be the author, or at least coauthor, of the financing section of the RFP. If a telecommunications consultant is hired, he or she usually incorporates vendor financing proposals in the RFPs. Once responses are received from vendors, the director and the finance officer should catalog the options and determining which option will enable the institution to obtain the lowest price for the equipment. It must be pointed out, however, that overriding political considerations sometimes prevent choosing the option that offers the lowest price.

The structure in place at the University of Texas at Austin (UT), for example, is one in which a vice president for information technology heads a group of approximately 360 employees whose mission is to provide voice, video, data, and technology services to the faculty, staff, and students. The entire financial structure is managed by the director of administration and her staff. Major capital expenditures are budgeted in advance and are carefully tracked. Examples used throughout this chapter will be based on procedures at UT.

Cataloging the Financial Options

Depending on the project, the institution, or a particular situation, any one of several options may be appropriate for public institutions planning to finance IT expenditures.

- *Appropriations:* A lump-sum, line-item appropriation by the state legislature for the amount needed to fund an institution's telecommunications system might be the least complex option. For two reasons, however, most legislative bodies are unlikely to do this. First, because of the decline in federal support and increasing demands for local assistance, most states are not in good enough financial condition to be able to commit to a major new capital expenditure. Second, and more important, there is already a budgeted stream of revenues for existing equipment, usually for an operating (nonownership) lease. For most legislatures, the existence of a previously budgeted line item in an operating budget is sufficient justification to deny requests for the same item in the capital budget.

Funding from the Texas state legislature continues to decrease, as is probably the case with most state legislatures. There are many public institutions within

Texas, and making a request for a capital expenditure that is not directly related to providing improved educational opportunities for students would be futile. For example, a request two years ago for an infrastructure fee to help maintain and repair old buildings was not passed by the legislature.

- *Excess cash:* There are a few institutions that have sufficient excess cash to finance a new system, but this, of course, is not the case with most. UT Austin has always funded switch maintenance and upgrades with excess cash. Dialtone rates are set with an eye toward earning enough revenue to fund annual operations and planned capital expenditures. In 2005, a $2.8 million upgrade to VoIP - switch architecture was funded in this manner. Using dialtone as a funding mechanism for upgrades and new purchases can be an excellent way to provide for the future of communications technology on campus.
- *Debt financing:* Debt can be issued directly by the university and secured by the pledge of student fees and tuition, or it can be issued by a state building authority and secured by annual appropriations of the state legislature. As mentioned previously, securing debt by annual appropriations of the state legislature is probably not available to most public institutions.

Student fees are numerous and growing. With the influx of cell phones and VoIP, students may not use or need a switched telephone system. Tuition in Texas is controlled by the legislature, and thus it would not be an alternative for IT expansion or upgrade. Historically, the legislature in Texas does not look favorably on requests from state university systems for fee, tuition, or budget increases. Institutions in some states, particularly in the East, may still find this to be a viable alternative, while others may find that they do not have statutory authority to issue bonds for other than "auxiliary" enterprises. Dormitories, student centers, and recreation facilities at such institutions are most often financed through a student fee assessed solely for the purpose of retiring the bonds. As an example, students at UT Austin voted to institute a fee that would pay for an outdoor swimming pool. It is currently under construction. A side note: doing so required the demolition of a building that housed the IT help desk. These days, making a case for "academic" equipment, such as a telecommunications system, is usually not received favorably.

In still other states, state law allows institutions to issue bonds for academic purposes without prior legislative approval, and tuition is pledged for repayment of the bonds. While this might seem a less-complex option, universities in states permitting these transactions may find that students do not accept the use of tuition-backed bonds to finance the equipment or that administrators are unwilling to utilize the debt capacity for needs other than brick-and-mortar projects.

It is important for the communications director to understand the institution's debt options as well as the political environment. The mechanics of the transaction are more likely to be the responsibility of the finance officer or the top-level management official. At UT Austin, decisions of this magnitude involve the vice president for IT, the CFO, the provost, and the budget director.

- *Vendor financing:* In the most popular form of vendor financing, the vendor introduces the university to a commercial bank, leasing company, or investment bank that actually provides the financing. Usually, the financing is not limited to the equipment being offered by the vendor. In general, it is in the best interests of the university to separate the equipment-selection decision from the financing decision. A rather lengthy RFP process will probably be required. Considering the political consequences discussed previously, vendor financing should be looked at very closely with the assistance of a consultant.

- *Leasing and lease-purchase financing:* An increasingly popular option is leasing, especially as technological advances continue at such a rapid rate. Leasing provides more flexibility in expanding or even changing the system without sacrificing an investment, and it offers short-term benefits, such as improved cash flow. A good discussion of leasing must include an explanation of how it works, an examination of the benefits, and an explanation of lease revenue bonds and certificates of participation.

1. *How leasing works:* A lease is an easy way to take advantage of the benefits of the latest technology without assuming the up-front costs and risks of ownership. A lease can include equipment, software, voice and data cabling, extended maintenance agreement, installation, programming, and other services.

A lease in the technology arena is not different from any other property lease: it is a usage agreement between an equipment owner (lessor) and a user of that equipment (lessee). The lessee pays a periodic fee, usually monthly, to the lessor for the use of the property.

Leases usually take the form of written contracts with specific terms and conditions spelled out: length of lease term (usually 24, 36, 48, or 60 months), amount and timing of lease payments, and any end-of-lease conditions or stipulations. Depending on one's point of view, contracts can either be beneficial or not. All of UT Austin's contracts must be signed by legal, contract, and purchasing officials.

The lessor is usually viewed as the owner of the equipment during the lease term, but depending on the type of lease, either the lessee or the lessor may be able to claim the tax benefits of equipment ownership. Regardless of which type of lease is selected, the future expected value of the equipment (the residual

value) is considered when pricing most types of leases. The residual value is the lessor's estimate today of the value of the equipment when the lease term ends.

At the end of the lease term, one of the following alternatives will be available to the lessee, depending on which type of lease was chosen:

• Return the equipment and sign a new lease for the most current, updated equipment.

• Exercise a purchase option and buy the equipment at a predetermined residual value.

• Keep the equipment and stop making payments if the lease-to-own option is available.

According to the Equipment Leasing Association (ELA), eight out of ten companies lease some or all of their equipment today—that's more than $120 billion of equipment leases a year. Leasing is gaining in popularity around the world. The advantages of leasing have made it attractive to businesses across the spectrum—from one-person operations to Fortune 500 companies.

According to ELA, the types of equipment being leased are just as diverse, including telecommunications systems, medical equipment (such as CAT scanners and MRI), computers, and commercial airliners. Transactions can range from a couple of thousand to millions of dollars.

2. *Advantages of leasing:* A number of factors make leasing an attractive option for an institution.

• Changing technology: A university telecommunications system, just like a private business, is subject to changes almost daily. New technology (e.g., VoIP), new market forces, new financial strains, and new organizational structures all add up to a need for flexibility. When selecting new technology, the consumer cannot know whether it will be replaced by a faster, more powerful alternative next year or even next month. Leasing equipment avoids the risks of ownership, because payments are only for the use of the equipment. When the lease expires, the equipment can be bought or traded in for the latest technology or simply abandoned (depending on the type of lease chosen).

Leasing provides access to the latest equipment and technology. Leasing protects against owning equipment that may not meet future needs, and it provides the flexibility to move up to the newest releases, features, and functionality as they become available. Leasing is often the financing solution of choice when concerns are raised about equipment becoming obsolete before it can be fully depreciated.

• Conserving capital: Leasing leaves capital free for other expenses, instead of tying it up in fixed assets.

• Generating profits: Invest the cash saved in inventory or other equipment needs.

• 100% financing: Unlike bank loans, leasing usually requires no down payment and, in most cases, no compensating balances on approved credit. Leasing provides for the whole package: equipment, cabling, installation, programming, maintenance agreement, and even software.

• Tax advantages: Leasing offers important tax benefits that reduce the cost of obtaining equipment. Depending on the type of lease chosen, the entire monthly payment may be written off as an operating expense or capitalized outlay.

• Budgeting advantages: Leasing guarantees a fixed monthly lease payment for the length of the lease term, simplifying budgets and forecasting of equipment expenses. It also provides the flexibility to obtain unbudgeted equipment. Annual operating budgets may accommodate a monthly lease payment, but capital budgets often cannot be stretched to allow for an outright purchase.

• Redeploy funds already budgeted for telecom: Leasing of updated phone equipment may provide the ability to redeploy funds already budgeted for monthly telecom expenses. For example, many of today's phone systems have both digital and analog capacities, allowing for devices that in the past may have required their own phone line (credit card terminals, modems, fax machines) to be connected to the phone system, using existing phone lines. This feature can reduce overall monthly telephone bills, and those funds can then be used to lease new phone equipment.

3. *Lease revenue bonds and certificates of participation:* For many years, lease financing has been among the most popular methods for financing capital improvements while complying with or avoiding constitutional debt limitations applicable to states, cities, counties, and school districts, as well as to other public entities. Its popularity increased further following the successful development of the certificates of participation (COP) structure in the early 1980s. California surpasses all other states combined in using lease and COP financing, and these techniques are becoming increasingly prevalent in other states.

Lease revenue bonds or COPs have been used to finance such projects and programs as:

• Office buildings, public administration buildings, courthouses, police and fire stations, civic center complexes, museums, and convention centers

• Elementary and high school buildings, relocate-able school buildings, and "land bank" programs for growing school districts

• Telephone, telecommunications, and data processing systems

- College and university buildings and equipment, including laboratories, high-tech educational facilities, libraries, and instructional facilities
- Prisons, jails, and other correctional facilities
- Healthcare facilities
- Cogeneration projects and other electric power facilities
- Water system facilities
- Wastewater treatment facilities
- Aviation hangars and other airport facilities
- Parking structures
- Public golf course and recreational projects
- Open space
- Asbestos-removal projects at schools
- Unfunded pension liabilities
- Land acquisition
- Light rail transit
- Equipment, buses, computers, and other personal property

The leases or other agreements on which these financings were based have involved such features as:

- Master lease arrangements
- Leveraged leases
- Transfer of tax benefits
- Rent payable from a general fund but limited to the amount of a particular tax or other revenue received by the lessee

Investment bankers have applied their experience in small-equipment lease financing to the design of lease-purchase finance programs for multimillion dollar telecommunications systems. The program provides cost-effective, nondebt financing with flexible repayment terms and conditions. In addition, the leases can be sold at interest rates lower than small-equipment leases because of the marketing advantages of securing investment-grade ratings and because of the emphasis placed by investment bankers on developing a much broader marketing approach.

Traditional small-equipment lease financing involved one lease for the total amount of equipment to be financed. Usually, the lease was sold as a whole to one investor, because there was no legal mechanism for breaking the lease into smaller investment pieces. This structure, however, would not be appropriate for the

multimillion dollar leases necessary to finance telecommunications systems at many institutions.

The use of COPs, representing a proportional interest in lease payments made by a lessee, has become an accepted security in the market and allows a governmental unit to raise funds outside of the legal definition of debt. The state institution selects an issuing company to issue the COPs, and the issuer uses the proceeds to finance projects. COPs are paid off through annual payments appropriated by the state government.

COPs are fractional shares of an obligation (i.e., a lease-purchase transaction), represented by a certificate that signifies that the investor owns an interest in the lease payments made by a governmental entity. While COPs have many of the same characteristics as municipal bonds, they do not normally constitute legal debt for the lessee.

COPs split the ownership of a lease into small denominations. These certificates are structured in a manner similar to bond issues, maturing serially over the financing term, and they pay interest semiannually. The interest portion of the payment is exempt from federal income taxes and may, depending on state law, be exempt from state and local taxes.

The COP structure allows the institution (i.e., the government unit) to make lease payments based on its cash-flow capabilities and on the estimated life of the equipment. Most lease-purchase agreements in the telecommunications area can be structured so that the lease payments coincide with the lease payment that the university has made for decades under operating (nonownership) agreements. Ownership of the equipment passes directly to the institution upon remittance of the final payment. The university's obligation to make lease payments is designed to ensure that the lease will not be considered a debt under applicable state statutes and that it will not require legislative approval or diminish coverage ratios for student tuition or fee-secured bond issues.

Legal documents pertaining to the transaction are a hybrid of traditional bond and equipment lease financing documents. The terms and conditions of the lease are contained in the lease and agreement between the university (lessee) and the nominal owner (lessor). The lessor can be the telecommunications equipment vendor, a commercial bank, or a university foundation. The responsibility for monitoring the transaction, collecting the lease payments from the lessee, disbursing principal and interest payments to the certificate holders, and liquidating the equipment in the event of default or nonappropriation rests with the trustee and is detailed in the trust indenture. The trustee is a third party, typically a large commercial bank or trust company. COPs are sold by the investment banker pursuant to an official statement that summarizes the lease agreement and the trust indenture and provides other pertinent information regarding the

transaction and the university. These basic documents are drafted by nationally recognized bond attorneys and disclosure counsel.

Determining the Financing Option

It is important for the finance officer and the communications director to be familiar with the key variables that are unique to the institution's situation. Several factors influence selection of a financing method for a telecommunications system.

- *Legal constraints:* The most important legal issue to be resolved is the institution's authority to (1) issue bonds and (2) enter into lease-purchase agreements. It is important to distinguish between traditional lease-purchase agreements and those that are publicly offered certificates of participation. Most universities have long used standard lease-purchase documentation for lower-priced equipment items. This documentation may or may not stand the legal scrutiny that publicly offered COPs will undergo. In most cases, nationally recognized attorneys in the field of tax-exempt bonds need to be consulted.

- *Political constraints:* The nature of the relationship between the university and the executive and legislative branches of state government can significantly affect the choice of a financing method. If the legislature exerts strong control over the issuance of debt, then the use of a lease-purchase agreement without the consent or knowledge of the legislature might have severe repercussions. Similar problems could arise between a university system and the executive branch of state government if a financing mechanism that has not been approved or used previously is chosen.

State funding in Texas is usually intended for salaries of faculty and staff, with little left over for purchases of the magnitude discussed here. UT Austin finances upgrades with dialtone, and thus debt has not been an issue. The university's executive leadership would need to advise the legislature should the issuance of debt or use of lease contracts become necessary.

- *Capital cost of the system:* A third factor in determining the financing mechanism is the acquisition cost of the system. Many institutions under 5,000 full-time enrollment (FTE)without a dormitory system can purchase an adequate system for less than $2 million. It might be easier for such an institution to obtain a lump-sum appropriation from the legislature for this amount rather than issue bonds to finance the acquisition. On the other hand, a large institution of 40,000 FTE with a significant dormitory population would be more inclined to issue bonds or COPs, assuming that student use of the telephone system warranted the acquisition. UT Austin discontinued long distance for residents of dormitories in 2004 and may be asked by Housing and Food to discontinue dialtone altogether.

With an enrollment of 50,000-plus—6,800 of which live in residence halls—usage of dialtone is at less than 50 percent. E-mail and cell phones have made dialtone virtually obsolete.

- *Technological obsolescence:* Telecommunications equipment is subject to rapid change and potentially rapid obsolescence. This affects the length of the financing more so than the type of financing. The time standard that is becoming accepted as the preferable lease term is 7 years, with some leases being extended to 11 years. With the rapidly developing VoIP technology, a shorter term or an upgradeable system would be preferable. UT Austin is upgrading a Nortel SL-100 switch to a CS2100 with VoIP capabilities and vastly improved expandability for $2.5 million.

The lease term is important in the lease transaction because the ultimate security is the system itself. In a debt transaction, the ultimate security is the pledged revenue stream, so the life of the equipment need not be an important consideration. Underwriters and rating agencies view the "essentialness" of the telecommunications system as greater than that of most other equipment on the campus (e.g., administrative data-processing equipment). They are, therefore, more comfortable with a somewhat longer lease term for an integrated telecommunications system.

- *Budgeted cash-flow analysis:* The acquisition of a new telecommunications system can be accomplished within the framework of already budgeted appropriations, or what is commonly called the base. Legislative or executive branch budget analysts will recognize the existence in an institution's budget of the current expenditure for telecommunications equipment. This will make it difficult for the institution to pursue "new" sources of revenue to finance a replacement system, whether by lump-sum appropriation or by legislatively authorized bond payments. Such a situation could make lease-purchase financing attractive, because the maturity schedule of the lease can be adapted to match the currently budgeted expenditure for the nonownership lease.

■ Independent Institutions

In general, independent institutions have the same type of financing alternatives as do public institutions; however, the financial instrument used may be very different. Alternatives for the independent institution include *internal financing* (endowment, reserves, operating funds) and *external financing* (public or private bonds; public/legislative funds; secured lease; and other, usually secured, debt).

Internal Financing

- *Endowment funds:* One area that may offer an attractive financing mechanism for an independent institution is the use of endowment funds. This can be done in one of two ways: First, in the event that the institution has sufficient available funds to directly support the acquisition of a switch, direct purchase can be considered. It is obviously very important to determine that this is the "highest and best" use of the funds, since expenditure of endowment funds for a project of the magnitude of a switch significantly reduces the liquidity of the institution's portfolio, and affects future income streams. Further, the legality of such an expenditure of funds must be determined, particularly if restricted endowment funds are involved.

  The second alternative is to use endowment funds as an internal source of funds for borrowing. In this case, the institution should determine the appropriate rate of return to be credited to the endowment earnings (and charged to operations), along with an appropriate amortization schedule to restore the endowment principal at the end of the communications system's life. An accurate determination of this rate should include such factors as the return received from the alternate investment of these funds and a reasonable estimate of the interest rate that would be charged in the financial markets for financing the switch. (Obviously, if the income rate exceeds the cost of financing, borrowing from endowment should not be used as a source of funds.) The legality of borrowing from endowment funds should also be determined.

  An ideal situation would be an endowment that is specifically earmarked for IT purchases, maintenance, and upgrades. Although not usually the case today, as technology changes in the future, this may be a reachable goal.

- *Reserves:* Depending on the institution's accounting methods and fiscal policies, reserves may be available for equipment purchases. Because it is unlikely that large amounts of funds have been set aside for purchase of a switch, the accumulation of reserve funds toward a second purchase should be considered. To the extent that reserves are available, they can also be very useful as a source of funds for tactical projects (e.g., purchase of telephone sets or long-distance controllers) to enhance the present system or for short-term borrowing to structure a complete project. Using reserves, however, always requires proper accounting/auditing procedures and validation of the need for the funds.

- *Operating funds:* It is possible to use operating funds to finance major acquisitions, at least in part. Although UT Austin is not an independent institution, the model of using dialtone rates to fund all aspects of switch operation, maintenance, repair, and upgrade is certainly valid. However, the displacement of expenses is often miscalculated and overstated, as communications switches are

dynamic and must always be expanded. Sufficient operating funds (or reserves for ongoing enhancements) must be available for the purchase of additional items needed as the switch expands. Thus, use of operating funds for direct financing should not be relied on unless the assumptions about growth and ongoing expense reductions can be shown to be reliable. Most of the unreliable assumptions in the analysis of financing plans result from overestimating the availability of funds.

Operating funds should, of course, be used for acquisition of expendable items or for temporary payment of items until a long-term instrument can be prepared. It is advisable to avoid external financing of expendable items or carrying short-term items into long-term debt.

External Financing

The forms of external financing for independent institutions are quite similar to those that can be considered by public institutions. However, the market and legal requirements may be quite different, reflecting the difference in control and the diversity of state legal requirements.

- *Bonds:* Bond issues have become increasingly important in the past few years and now account for a substantial portion of communication equipments placement. Bonds may be issued either on the basis of public authority—which will often yield lower interest rates—or privately through bond counsel and underwriters. (It should be remembered that legal and financial requirements for bond issuance vary from state to state.)

Placement and marketability depend on the guarantees provided and securities pledged against repayment. (The ability to place is very much dependent on the financial rating of the issue guarantees by a state authority or agency. Bonds issued by an independent institution without guarantee have limited marketability.) In any case, bonds are an extremely important form of financing. There are strong arguments in favor of using bonds to acquire a communications system at an attractive interest rate, provided that the institution can secure a favorable rating in the financial markets and is willing to provide appropriate security for bond repayments in the form of pledged future income.

- *Public funds:* In many states, provision has been made for the use of public funds by independent institutions. This may be in the form of housing bonds or equipment allocations from the state legislature to the board of regents for distribution to independent institutions. Public funding may consist of grants for specific purposes (such as equipment) or of a portion of a state educational bond issue. The amount of these funds may be limited, with allocations based on institutional size, or they may be available on a first-come, first-served basis.

There may also be specific conditions regarding the use of such funds (e.g. term, purpose, expected lifetime of the equipment to be purchased, etc.). While such "strings" may pose problems, substantial interest rate advantages can be gained, and it is even possible that outright grants could be obtained.

- *Leasing:* Independent institutions often use leases or lease-purchase agreements to acquire a communications system. These agreements must be arranged by the vendor or placed privately through institutional contacts. Leasing is most complex in relation to operational activities, as it requires accurate identification of parts, inventory, and other information as to source, replacement, and ownership. Leases or lease-purchase agreements may be entered into directly with the manufacturer of the equipment or, as is more frequently the case, with a third party as lessor. Only the very largest manufacturers are willing to enter into direct agreements, and even in those cases, the agreements can usually be assigned to a third party at the option of the vendor.

A variety of concerns must be addressed when purchasing a communications system under a lease agreement. These range from possession of title to the equipment during the lease to specification of remedies that may include liquidated damages. For example, if items are stolen or destroyed or outgrown, are sums due and payable immediately, or are payments to be made over the remaining term of the lease? Do the institutional auditors take the same position as the lessor? Is the institution obligated to continue making payments on the lease to the third party or assignee while it attempts to recover from the manufacturer/distributor?

- *Other debt:* Other debt can be used when the institution is willing to offer other assets as security against borrowing to keep communications equipment unencumbered. Unsecured debt will probably not be very attractive to lenders. Certainly, the use of other assets, such as stock or other investments, as security is an alternative that can be used to raise "equity money." The institution must determine, as a matter of policy, whether it is prepared to make such a commitment and whether this action is appropriate.

- *Fund raising:* Administrators should not overlook the possibility that the financing of a telecommunications system may be an attractive fund-raising opportunity for development personnel.

- *Student resale:* For many years, another opportunity for earning institutional revenues to retire leases or debts was resale of long-distance and other telecommunications services (e.g., CATV, data network access/Internet) to students. However, this does not seem to be the case anymore. In the past, students benefited because the institution provided them with attractive long-distance rates, purchased at "wholesale." The institution benefited by charging rates that

included a margin above actual cost. The 1992–1993 ACUTA Membership Facilities/Services Index showed more than 300 colleges and universities with student long-distance resale programs in place, and another 70 in the planning stage.

What a difference the years have made. Most ACUTA institutions now report little or no student long-distance revenue. UT Austin discontinued providing long-distance service to its 6,800 resident students at the end of the Spring 2004 term. Revenue had dropped from a high in 1990 of $1 million annually to $12,000 in fiscal year 2003–2004. Cell phones, e-mail, and the Internet have virtually eliminated the need for long distance in residence halls. Some ACUTA institutions, such as the University of Toledo, now have very active and profitable cellular programs.

Other student resale programs are aimed primarily at selling data access. UT Austin sells bandwidth by the gigabit, and students are monitored to ensure that they comply with all rules of usage. Students who are discovered abusing the system are removed from the network.

Factors involved in a student resale program include available resources (staff and equipment capacity), developing a call accounting system (for preparation of usage reports and billings), negotiations with carriers, enrolling students in the program, determining a deposit fee (if any), setting rates, and collecting fees. At UT Austin, all student-related charges are billed through Student Accounts Receivable, and students are barred from registration and possibly graduation if they fall behind in payments.

Whereas student long-distance resale was a promising source of funding for equipment upgrades, the new and next generation of technology has yet to be as lucrative.

■ Universal Considerations

Certain considerations apply to both public and private institutions.

Determining Costs

Knowledge of costs is necessary in order to make intelligent managerial and financial decisions and to help examine the appropriateness of each cost. This knowledge helps define whether costs are excessive, how operations and activities are going, how to formulate pricing, how to analyze cost data for short-term and long-term decisions, how to manage and control costs, and how to set realistic pricing models.

Cost analysis looks at the different types of costs incurred and how they may be controlled from a functional perspective. Cost analysis examines the costs associated with a particular decision and what may be done about those costs in the future. By knowing what costs are and how they behave, steps can be taken to improve efficiency and engage in cost-reduction programs.

A few basic goals to manage costs include the following:

- *Cost reporting:* Classifying, summarizing, communicating, and interpreting cost data so as to provide accurate information to various internal or external stakeholders
- *Cost measurement:* Relates to specific products and services
- *Cost management:* Accurate product-costing data are needed to assist managers in making critical decisions, such as pricing, product mix, process technology, and alternative courses of action
- *Cost analysis:* Requires that cost data be reviewed and translated into information useful for managerial planning and control and for making short-term and long-term decisions

Cost information is vital for all phases of management. In general, the work that management performs can be classified as:

- *Strategic planning:* Involves the selection of long-range and short-term objectives and the drawing up of strategic plans to achieve those objectives
- *Coordinating* Management must decide how best to put together resources to carry out established plans
- *Controlling:* Entails the implementation of a decision method and the use of feedback so that goals and specific strategic plans are optimally obtained
- *Decision making:* Selecting the best choice to accomplish the goals that have been set forth

Funding Models and Strategies

Much of academic technology is distributed throughout the colleges and departments rather than centralized. Accordingly, it is hard to get an accurate assessment of both expenditures and needs for academic technology. At UT Austin, weekly meetings of technology deans and key IT (ITS at UT) personnel help close the gap and identify needs.

Funding and Implementation

Getting an IT strategic plan funded and implemented requires the understanding of costing methodologies, annual and multiyear budgeting, and life-cycle

funding. Financial models can be designed that apply to small, medium, and large institutions—private or public. Both traditional funding mechanisms, such as budget allocations, student fees, chargeback, and debt financing, as well as new and innovative mechanisms, such as partnerships with other institutions, partnerships with vendors, external grants, and gifts, should be examined.

Aligning IT Investments with Institutional Priorities

One of the most difficult questions facing any enterprise, including universities, is where to invest limited IT project resources for the maximum benefit to customers, constituents, and institutional missions. Clearly defining institutional priorities and critical success factors, as well as defining and prioritizing IT investments accordingly, is very important. In addition to prioritization, this process fosters a functional partnership and a shared language and perspective on the value and risks associated with IT across the university's senior management team.

Funding Capital Programs

Finding resources for capital projects is always a challenge, whether in the public or the private sector. The task of seeking money for large capital projects within public and private institutions is always difficult. Infrastructure is hard to sell, so creative funding methodologies are needed. Ideas include

- Selling what can't be sold—infrastructure
- Creative financial planning for capital needs in infrastructure
- Potential resources—building reserve funds, selling bonds, corporate investments, donations
- Long-range planning
- Strategic planning for major investments

Forecasting Maintenance Costs

Issues include budgetary options and timing of software, network, and hardware infrastructure upgrades. All possible options should be reviewed in advance, and a plan created and followed.

Managing IT Repair and Replacement Costs

Many in IT management and leadership are able to convince senior management of the value of proposed projects only to find that the ongoing cost of supporting

the equipment and software nibbles away at limited operating budgets. Make sure that the full cost of new projects undertaken is included when projects are approved. Steps should be taken not only to identify and cover costs at the outset but also to potentially reduce costs.

Changing Models: Risk, Organizational Structure, and Value

University IT units are focused mainly on supporting core mission activities. Expanding needs with decreasing budgets are issues faced by all. By embracing risk-based activities that create quantum change in business processes and by creating an environment of flexible, matrix-based organizations that can provide more efficiency while promoting better services to campus, IT units can report planned, value-based decisions rather than reactive ones. Activities should include

- Embracing and managing innovative risk within the academic setting
- Creating and maintaining organizational flexibility
- Reporting value and measuring success

Budget and IT Recruiting/Training and Retention

Training and retention strategies work together to create a high-quality IT staff. These strategies require adjustment to deal with current events, market competition, and diversity, including age and gender. While not specifically discussed previously, recruitment and retention can make or break a budget.

Effectively Communicating the Benefits of IT Expenditures to Campus Constituencies

IT is often taken for granted. If IT works, no one notices, so it is hard to sell the various constituencies on the need to upgrade, expand, or replace. If IT breaks or fails, however, it is as if the world ended. Every part of the campus has a different interpretation of what IT is, what it does, and how it is important to them. Some areas to address are

- Building a campus communications network—instruction, research, administration
- Designing strategic plans that provide mechanisms for input—getting the attention of all constituencies
- Balancing investments—everyone gets something
- Coping with expectations versus available funding—creative thinking, creative design

Alternative technologies should be addressed when structuring the financial arrangement for a new campus telecommunications system. Some colleges and universities may require the assistance of a competent consultant when considering the complex variables involved in moving intelligently into the future.

The financing arrangements must address all the assumptions made earlier in the process of identifying the preferred bid. Based on the complete and detailed analysis of that step, the financing agreement must be structured to ensure that proper amortization is occurring. A less-than-ideal decision regarding switch selection can be tolerated if the assumptions of switch cost and life cycle were accurately determined; if the financing arrangements were based on improper life cycles, however, the institution will face major financial problems in liquidating and salvaging its position.

The analysis of each component is extremely important in order to call into account all assumptions made in switch selection. If the financial analysis shows that an improper overall assumption was used to evaluate alternatives, the institution runs a substantial risk of being left with a "stranded" investment at the end of the switch's life cycle. With proper assurances that the switch financing will not exceed the useful life, the institution can be somewhat ensured that even if the decision turns out to be less than ideal, a reasonable level of service can be maintained within financial constraints.

Analysis may show that switch selection has been driven by a preference for a particular technology or by the availability of a specific amount of funds. It is important that institutions allow neither technology nor financing alone to drive the choice. A balance must be reached so that an institution does not find itself with more equipment than it can pay for or with equipment that becomes outmoded too quickly because sufficient funds were not available to obtain an adequate system. An institution must live with a communications system for a relatively long time—it is a major investment, not to be replaced in 1 or 2 years. Thus, all segments of the community must be reasonably satisfied with the choice.

■ Summary

In this chapter, we looked at the financing for IT initiatives within a campus environment. Several options were brought forward: appropriations, excess cash, debt financing, vendor financing, leasing, and lease-purchase financing. The decision depends on many political, cultural, legal, and budgetary factors within a campus environment. We also explored the advantages and options within leasing.

The chapter closed with a discussion of methods of determining costs for services provided. Whatever financing alternatives, leasing, and costing methods are chosen, it is imperative that financial issues be taken into consideration before technology is applied. We must consider not only the costs of purchasing the technology but also the total cost of ownership of technology and the proper funding for this. We all know what happens if technology is not properly supported and funded and the negative implications that this can hold. For the benefit of our institutions, our students, and our careers, the appropriate funding and long-term support of technology must be secured.

CHAPTER 8

The Role of Consultants

David C. Metz

Dave Metz is currently senior consultant with Vantage Technology Consulting Group. He has more than 40 years in the computing and telecommunications industry, serving as telecommunications director at Rensselaer Polytechnic Institute and the University of Colorado at Boulder. Metz is a former ACUTA Board member who presently serves on the ACUTA Journal Editorial Review Board and is a frequent presenter at ACUTA events.

The introduction of new technologies in the past few years and the resulting convergence of voice, data, and video services on most campuses have dramatically altered the communications landscape in higher education and the corporate would. Perhaps now more than ever, consultants who have experience in both the voice and the data worlds can provide services to help those who manage these worlds on campus succeed.

No longer can the consultant be viewed only as someone who helps you select a new system. With vastly different levels of expertise and experience derived from different backgrounds, consultants specialize in different aspects of telecommunications and are familiar with a variety of industries and applications. What does a consultant do? When should one be hired? Where can one be found? What is a reasonable charge for consultant services? How can you tell if a consultant is ethical, experienced, or right for the job? Given the complexity of communications today and the size of the investments being made, getting solid answers to these questions is essential.

■ Why Engage a Consultant?

There are many reasons to seek the advice and assistance of a consultant. Probably the most common reason is to gain the benefit of specialized expertise. For example, implementing a campuswide VoIP system to replace a conventional PBX is a complex task that carries considerable risk if not done well. It is unusual to find an IT or telecom staff with all the skills and experience needed to effect such a massive change—one that will affect every user on campus, may require major upgrades to the data network, has implications for communications

closets, has wide-reaching implementation and support ramifications, and more. Consultants who have had significant experience with just such projects on other campuses are familiar with the pitfalls and complexities, know what to do and what to avoid, and can provide invaluable guidance.

Consultants can also provide an objective viewpoint on many different topics. Even the best communications technology staff may profit from input from an experienced and unbiased outsider who has the benefit of viewing decisions in a broader context, unhindered by the sometimes distorted lens of departmental or institutional history or politics. The opinions of an outside expert may also be useful in selling change internally, both within the department and to upper management.

Another major reason to hire a consultant is that sometimes there is just too much work in a department for the number of hands and heads available. Projects can be divided into components, and then specific parts can be assigned to a consultant. A fresh perspective, broader expertise, and experience with proven methodologies can help organize and direct the project, resulting in less time wasted working on the wrong issues or pursuing blind alleys. In addition, hiring a consultant for a specific task is often less expensive in the long term than adding permanent staff.

■ What Do Consultants Do?

The list of available consulting services is long. Institutions may want to use only a few services or may need a broader range of help. Typically, the larger and more complex the task at hand, the more specialized the skills and experience required. If the institution has a small staff or if assistance is needed in dealing with a specific political situation, more assistance may be required. The important point is that the institution must determine the appropriate level of consulting involvement. This decision must be absolutely clear and must be conveyed to the consultant.

Some of the more common consulting services include assistance with the following issues:

- *Long-range strategic planning:* Where is telecommunications going in the institution? How is this function going to further the institution's goals?
- *Shorter-range tactical planning:* Given the money we have (or might have), what projects should we do and in what order, and what do we need for additional staffing and tools?
- *Organizational design and structure:* How many in-house managers and analysts will be needed once the system is installed? How many maintenance

technicians, billing clerks, and other types of employees? To whom should the telecommunications management function report? Should voice, data, and video be combined into one organization?

- *Business analysis:* What kind of cost allocation and chargeback algorithms will provide an equitable and predictable funding stream to supply and support present and new technologies?
- *Cable plant:* What is the status of the cable plant? Is it capable of supporting proposed higher-capacity service? Where are potential bottlenecks? What construction will be needed to accommodate new cable plant?
- *Current system evaluation:* How cost effective is the system? Is the service level adequate? Can growth be accommodated? Should we change? Can we wait?
- *New technologies:* What are the implications of VoIP (or any other new technology) for our campus? Is the network ready? What will it cost to make the network ready? What are the alternatives? Assuming VoIP is inevitable, what is the best timetable for our institution?
- *Equipment inventory:* How many stations of each type does the institution have? Where are they located? What is the nature of the cable plant?
- *Needs assessment:* What new functions are needed? How can the institution take advantage of newer technologies, such as unified messaging, text to speech, and speech-enabled systems?
- *RFI and/or RFP preparation:* Conversion of operational and management needs into technical terms that vendors can understand and deal with is a special skill.
- *Vendor proposal evaluation:* A thorough knowledge of system architecture, features, and vendor reputations from past installations is crucial in any evaluation, as is a detailed financial analysis of the proposals.
- *Contract negotiations:* What is the vendor likely to give away? Where can the vendor be expected to draw the line?
- *Installation project management:* Even turnkey contracts do not always run smoothly; an experienced watchdog is invaluable and often mandatory.
- *System acceptance testing:* Designing performance criteria for system acceptance and then making certain that the system performs according to those standards will prevent many problems later on.
- *Network design:* What is the campus's relationship to the rest of the organization and the rest of the world? How should the institution communicate best?
- *Education and training:* With a new system, every user will need some training. Who is best qualified to design a practical training program that will ensure success?

- *Software selection:* What type of management software will be needed? Where will it come from?

Consultants get involved in all of these issues at various levels. Each institution must determine the level of support it wants and needs. For example, one approach to compiling an equipment inventory is for the consultant to design an inventory system and for the in-house staff to conduct the inventory itself. Some consultants, however, have enough staff to perform the whole job. Typically, vendors supply a certain amount of user training for new systems, but the consultant can assist in specifying the nature and extent of training when writing the RFP and can supervise the vendor's performance. In general, consultants will be of the most value doing those things for which the institution does not have qualified, available in-house staff.

■ Which Consultant Is Right for My Institution?

Great care must be taken in selecting the right consultant. Consulting firms range in size from one-person shops to divisions of large management consulting and accounting firms with offices around the globe. Many hardware and software vendors offer "consulting" services. Some corporations, having developed a sophisticated staff to deal with their own internal problems, have later turned that staff into a new division that sells consulting services to outside users.

Size is not a good determinant of quality. The personal attention and commitment that is frequently offered by small firms is harder to find with the larger organizations. On the other hand, some one-person shops lack the technical depth needed for very large, complex tasks. Consulting provided by hardware and software vendors must be examined carefully for the presence of a conflict of interest or ulterior motives.

The name and reputation of traditional management consulting and accounting firms give them credibility. They have large staffs that usually represent a broad spectrum of technical understanding and experience. Partly because of their size, they tend to operate in a more highly structured and formal manner than smaller firms, and they tend to be relatively less flexible, whereas many of the small firms are more specialized. The approach of small firms can be more easily tailored to the needs of an individual institution. These firms are also frequently less expensive than their larger competitors. Finally, many large firms have rightly gained the reputation of selling a project using high-level, experienced consultants but then perform the work with less-skilled, entry-level staff.

Cost is an equally poor means of choosing a consultant. The least-expensive consultant may, in retrospect, turn out to be so inept as to be very costly. On the

other hand, the most expensive is not necessarily the best either. Rates run from $800 to $2,500 or more per day, plus travel and lodging expenses.

■ How Do Consultants Charge?

Most consultants will quote either a fixed price or a range with a minimum and maximum for performing a specific task, usually with a stated rate per day for extras outside the agreed-upon scope of work. One important implication of this is that the institution must clearly convey to the consultant the exact scope of work, and the consultant must understand and agree. For projects where the consultant's scope of work is less clear, a contract based on an hourly or per diem rate in which the consultant is paid for actual work performed might be the best approach. In either case, negotiating a detailed contract with the consultant is advisable.

Other means of computing compensation are less common. For example, the use of contingency fees, where payment is a percentage of the annual savings realized as a result of a consultant's recommendations, has declined in recent years. This approach may produce large savings by eliminating important services or functions, only to leave the patient—after the fee has been paid—near death's door because the level of service is no longer adequate. At this point, most of what has been removed in the cost-saving effort must be replaced. Some consultants charge a certain amount per line based on system size. Obviously, this can lead to overbuilding the system. Whenever possible, both the contingency fee and the per-line approaches should be avoided. The consultant should always be compensated by the client, not by the selected vendor. If this were the case, it would be reasonable to wonder whether the recommendation was made in your best interest or the consultant vendor's.

■ Selecting a Consultant

Organizational size and cost should be just two of the factors considered in selecting a consultant. A partial list of questions to ask includes the following:

- Does the consultant have any experience with systems of the institution's size and type? A 10,000-line VoIP system on a 500-acre campus requires many skills not needed with a 400-line TDM switch confined to one building.
- Is the firm experienced with working in the higher-education environment? Most firms that do not have such experience find it difficult to understand that higher-education institutions consist of loose federations of independent contractors, and they fail to realize the highly complex political nature of colleges

and universities. Furthermore, the consensus-based decision-making processes unique to higher education has stymied many a consultant not familiar with it.

- Has the consultant ever worked in a public bidding situation (if this applies)? Public purchasing rules are very different from those that apply to private companies, and a misstep on the consultant's part can invalidate the whole process and cost months of time and effort.
- Does the consulting firm have any outstanding lawsuits? These are not necessarily a negative factor. In our highly litigious society, the consultant may indeed be innocent. Still, a lawsuit is cause for further investigation.
- Does the consultant have any apparent biases? Many have entered the consulting business as a result of corporate downsizing in the technology sector. Some of these carry personal biases for or prejudices against their former employer that may work to the institution's disadvantage.

Answers to some of these questions can be supplied by the consultant. Other information can be obtained only through third parties. The consultant's references should be checked through administrators at other institutions and managers in business and industry who have dealt with the firm. Ask the consultant for a list of recent recommendations and look for patterns that indicate lack of breadth or product biases. Request sample reports and presentations to check for style, clarity, and "packaging." Contacts available through membership in local and regional telecommunications organizations and industry-specific organizations, such as ACUTA, are absolutely invaluable and can provide a wealth of information.

Questions concerning how a particular consultant "fits" the institution can be answered satisfactorily only through actual interviews with prospective consultants. Many consulting contracts run for a year or two, especially for major projects, and it is important for the "chemistry" to be right. One of the major advantages of a small- to medium-sized firm is that the individuals with whom the institution is dealing before the contract is signed are likely to be the same persons who will be doing the actual consulting.

■ Working with a Consultant

Consultants have very different styles of operation. One extreme is the expert who is reluctant to reveal the reasons for making specific recommendations. This consultant spends time at the institution analyzing and coming to understand its needs and problems and then disappears. Later, he or she appears on the doorstep with a complete set of recommendations and solutions. Those at the institution have no idea what occurs between meetings, and they are unlikely to find out.

The other extreme is a consultant who merely repeats the solutions that he or she thinks the institution wants to hear, whether or not they are correct.

A more desirable approach to consulting is for the consultant to be not only an expert and a leader, but also an educator and trainer. One goal of both the consultant and the client should be to educate the institution and its personnel. Eventually, the consulting contract will terminate, and the task will be completed. From then on, the permanent staff will be expected to continue to run the system and justify and implement decisions and plans made with the consultant's assistance. A good understanding of the reasons for those decisions and of the operational basics of the system is crucial for the long-term success of any project.

It is also essential to develop a good working relationship with a consultant. This is much more easily achieved if the duties and responsibilities of the consultant and the institution are clearly established in the contract. During any project in which another vendor is involved, such as the installation of a new PBX, the relationship must also include the vendor. Some consultants attempt to act simply as intermediaries between the vendor and management, dominating the project. A more beneficial structure is one in which the consultant helps the institution and the vendor understand each other's problems and positions so that mutually acceptable solutions may be reached.

■ Summary

There is no easy formula for selecting the right consultant, but some steps will help:

- Be clear about what you want the consultant to do—in your own mind and in the solicitation for consulting services.
- Get a detailed scope of work and methodology from the consultant. Understand what the consultant plans to do, when, and why. Be sure you know what the consultant expects from you in terms of support, responsiveness, and information.
- Contracts are important but will probably need to be customized. Your standard language for a contract programmer or product procurement will not fit the bill.
- Do your homework. Check references. Make sure the consulting firm is what it claims to be.
- Be flexible. Situations change, and approaches that seemed to make sense on the surface may need to be modified as the project proceeds.

The decision depends on the unique situation of the institution—on its needs, funds available, existing personnel, politics, and personal preferences. Consultants should be seen as simply one potential resource among many. Exercising care in selecting and dealing with a consultant can provide many benefits to the institution.

Compiled by Michele Narcavage, University of Pennsylvania.

Special thanks to Harry Newton for permission to use Newton's Telecom Dictionary (22nd Edition, 2006) as a primary source for this glossary.

Glossary

ACCESS POINT (AP) Basically a device that connects a computer to a network.

ACUTA Association for Telecommunications Professionals in Higher Education. Prior to 1998, it was the Association of College and University Telecommunications Administrators. The new name is more meaningful, but the acronym stuck. ACUTA is an international, nonprofit educational association serving approximately 800 institutions of higher learning, represented by 2,100+ individuals. Members are typically director level or higher, and are responsible for data and video communications, and all variety of networks, in addition to traditional telephony. Corporate affiliate members are welcome as well. www.acuta.org.

ADSL Asymmetric digital subscriber line. One of a number of DSL technologies, and the most common one. ADSL is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream.

ANALOG TERMINAL ADAPTER (ATA) A device for a Northern Telecom Norstar phone system that lets it use analog devices, for example fax, answering machines, modems and single line phones, behind the Norstar's central telephone unit (its KSU). IPBX/VoIP systems also use ATA's to convert packets to/from analog.

ANTIVIRUS / VIRAL Programs which scan disks looking for the telltale signatures of computer viruses.

ASYNCHRONOUS asynchronous transmission. Literally, not synchronous. A method of data transmission which allows characters to be sent at irregular intervals by preceding each character with a start bit and following it with a stop bit.

AT&T AT&T Corporation, formerly American Telephone and Telegraph Company, was incorporated on March 3, 1885, to manage and expand the burgeoning long-distance business of American Bell Telephone Company and its licensees. It continued as the "long-distance company" until December 30, 1899, when it assumed the business and property of American Bell and became the parent company of the Bell System. It remained the Bell System parent, providing the bulk of telecommunications equipment and services (local, long distance and international) in the United States, until January 1, 1984, when it divested itself of the Bell operating companies that provided local exchange service. On September 20, 1995, AT&T announced that it would be splitting into three companies: a "new" AT&T, to provide long distance and international transmission and switching; Lucent Technologies, to design, make and sell telecommuni-

cations systems and technologies; and NCR Corp., to concentrate on transaction-intensive computing. The strategic restructuring was completed on Dec 31, 1996. Sadly, things didn't work out for the company which retained the name AT&T. Its long distance business contracted as competition expanded and prices plummeted. And in early 2005, it agreed to be purchased by SBC, one of its former local phone companies, for $16 billon. At one stage, AT&T and the Bell System had over one million employees. By the time of the SBC acquisition announcement it had fewer than 50,000. In the fall of 2005 SBC changed its name to AT&T.

On December 29, 2006, the Federal Communications Commission approved the acquisition of BellSouth valued at approximately $86 billion. The new combined company retained the name AT&T. The deal consolidated ownership of both Cingular Wireless and YELLOWPAGES.COM, once joint ventures between BellSouth and AT&T. Wireless services were to be offered under the AT&T name.

ATM Asynchronous transfer mode. Very high speed transmission technology. ATM is a high-bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique. Usable capacity is segmented into 53byte fixed-size cells, consisting of header and information fields, allocated to services on demand. The term "asynchronous" applies, as each cell is presented to the network on a "start stop" basis—in other words, asynchronously. The access devices, switches, and interlinking transmission facilities, of course, are all highly synchronized

AUTHENTICATION The process whereby a user or information source proves they are who they claim to be. In other words, the process of determining the identity of a user attempting to access a system.

AUTHORIZATION Think of charging things on your MasterCard, Visa, or American Express card. If the store cannot authorize the amount of your purchase, your Visa card will not allow you to make the purchase. Authorization is needed for many long-distance calls, especially those made using credit cards, telephone company calling cards, etc. Authorization is done by the operator's computer checking with the remote validation database service.

AUTOMATED ATTENDANT A device which answers callers with a digital recording and allows callers to route themselves to an extension through touch-tone input in response to a voice prompt. An automated attendant avoids the intervention of a human being in the form of a console attendant, thereby avoiding related personnel costs. Commonly implemented in voice processor systems and software, front-ending PBXs, and ACDs.

BANDWIDTH In telecommunications, bandwidth is the width of a communications channel. In analog communications, bandwidth is typically measured in Hertz cycles per second. In digital communications, bandwidth is typically measured in bits per second (bps).

BELL SYSTEM The entire AT&T organization prior to when it was broken up at the end of 1984. The Bell System included Bell Labs, Long Lines, Western Electric, and the 23 Bell operating companies.

BIOMETRICS is the study of unique and measurable physical (or biological) characteristics such as fingerprints, retinal pattern, or handwriting. Biometric authentication devices capture, encrypt, and use these unique and measurable characteris-

tics as the basis for confirming identity and determining whether to grant or deny access to physical or logical assets.

BLADE A blade is any card placed into a backplane in a telephone system. Usually a blade is an additional module. The "blade" term shows the aspect of insertion of the flat plane.

BLOG / BLOGGING Also called weblog. The word blog is a combination of web and log. A blog is a fancy name for a free website containing news, information and opinion about all manner of things.

BLUETOOTH A short-haul wireless protocol that is used to communicate from one device to another in a small area usually less than 30 feet. The commonest use is a wireless headphone communicating with the user's cell phone or desk phone.

BROADBAND Today's common definition of broadband is any circuit significantly faster than a dial-up phone line. That tends to be a cable modem circuit from your friendly local cable TV provider, a DSL circuit, or a T1 or an E1 circuit from your friendly local phone company. In short, the term "broadband" can mean anything you want it to be so long as it's "fast." In short, broadband is now more a marketing than a technical term.

CABLE PLANT A term which refers to the physical connection media (optical fiber, copper wiring, connectors, splices, etc.) in a local area network. It is a term also used less frequently by the telephone company to mean all its outside cables, those going from the central office to the subscribers' offices.

CAD Computer aided design. A computer and its related software and terminals used to design things.

CALL CENTER A place where calls are answered and calls are made. A call center will typically have lots of people (also called agents), an automatic number call distributor, and a computer for order entry and lookup on customers' orders. A Call Center could also have a predictive dialer for making lots of calls quickly. The term "call center" is broadening. It now includes help desks and service lines.

CATEGORY 5 CABLE (CAT 5). A category of performance for inside wire and cable systems. CAT 5 cables can be of various gauges and are useful in support of applications requiring a carrier frequency of up to 100 MHz; the transmission rate achievable depends on the compression scheme employed. ...Category 5 technical specifications are defined by FCC Part 68, EIA/TIA568, TIA TSB36, TIA TSB40, and ANSI/ICEA S91661.

CATEGORY 6 CABLE (CAT 6). Proposed Category 6 standards from the TIA (Telecommunications Industry Association), known as Class E standards at the ISO (International Organization for Standardization), describe a new performance range for unshielded and screened twisted-pair cabling. Category 6/Class E is intended to specify the best performance that UTP and ScTP cabling solutions can be designed to deliver based on current technology.

CATEGORY 7 (CAT 7 or CLASS F). A developing cabling standard from the TIA (Telecommunications Industry Association) for STP (shielded twisted pair), intended to support signaling rates up to 600 MHz in support of ATM and Gigabit Ethernet. A corresponding standard under development by the ISO (International Organization for Standardization) is known as Class F.

CATV Cable television. The term originally stood for "community antenna television" reflecting the fact that the original cable systems carried only broadcast stations received off the air; however, as cable systems began to originate their own programming, the term evolved to mean cable television.

CDMA Code division multiple access is a digital, spread-spectrum, packet-based access technique generally used in RF (radio-frequency) radio systems. Perfected by Qualcomm, CDMA is used in certain cellular phone systems and in some WLANs (wireless local area networks).

CELLULAR CMTS CMTS stands for the Cellular Mobile Telephone System. The original and still most common CMTS is a low-powered, duplex, radio/telephone which operates between 800 and 900 MHz, using multiple transceiver sites linked to a central computer for coordination. The sites, or "cells," named for their honeycomb shape, cover a range of one to six or more miles in each direction.

CENTREX is a contraction of Central Exchange. Centrex is a business telephone service offered by a local telephone company from a local telephone central office (also called a public exchange). Centrex is basically normal single-line telephone service with additional "bells and whistles" such as intercom, call forwarding, call transfer, toll restrict, least-cost routing, and call hold (on single-line phones).

CEO Chief executive officer

CHAT A common name for a type of messaging done over a network, involving short messages sent from one node to another. Chatting usually happens in realtime, sometimes in just short messages that are replied to quickly. Sometimes, however, chatting software is RAM resident, meaning it can be "popped up" inside an application (program). Users are usually notified of an incoming chat by a beep or a message at the bottom of their screen.

CHATROOM Realtime chat services offered by many Internet information service providers, such as America Online. Supporting a dozen or so participants, they act much like a teleconference, although on a text basis. Private rooms are those that can be entered by invitation. Public rooms allow anyone to participate.

CIO Chief technology/information officer

CIRCUIT SWITCHED/SWITCHING is like having your own railroad track for your conversation to travel on. It's yours for as long as you keep the connection open. No one else can use it. Once you hang up, the next caller gets to use that track. Virtually all voice telephone calls are circuit switched, although that won't be true in the future. All dialup modem calls are circuit switched also.

COAXIAL CABLE A cable composed of an insulated central conducting wire wrapped in another cylindrical conducting wire. The whole thing is usually wrapped in another insulating layer and an outer protective layer. A coaxial cable has capacity to carry great quantities of information. It is typically used to carry high-speed data (as in connections of 327X terminals to computer hosts) and in CATV installations.

COMMUNICATIONS ACT OF 1934 Federal legislation which established national telecommunications goals and created the Federal Communications Commissions to regulate all interstate and international communications.

CONFERENCE BRIDGE A telecommunications facility or service which permits callers from several diverse locations to be connected together for a conference call. The conference bridge contains electronics for amplifying and balancing the conference call so everyone can hear each other and speak to each other.

CONVERGENCE The word to describe a trend—now that most media can be represented digitally—for the traditional distinctions between industries to blur and for companies from consumer electronics, computer and telecommunications industries to form alliances, partnerships and other relationships, as well as to raid each others markets.

CTO Chief Technical Officer

DASHBOARD Traditionally a control panel located under the windshield of an automobile, now it is frequently an electronic means of sharing/monitoring information such as the status of a user (presence).

DEGAUSSED To demagnetize. To degauss a magnetic tape means to erase it.

DEMARC Demarcation point.

DEMARCATION POINT. Pronounced DMarc. The demarcation point is the physical point at which the separation is made between the carrier's responsibilities for the circuit and those of the end-user organization. The carrier is responsible for the local loop, which connects the user organization's premises to the carrier's CO (Central Office) or POP (Point of Presence) at the edge of the network.

DEMODULATOR In general, this term refers to any device which recovers the original signal after it has modulated a high frequency carrier.

DENIAL OF SERVICE You're no longer allowed to use a service. That service might be anything from normal phone service (you didn't pay your bills) to not being allowed into the company's e-mail because you were just fired.

DHCP Dynamic Host Configuration Protocol. DHCP is a TCP/IP protocol that enables PCs and workstations (VoIP phones) to get temporary or permanent IP addresses (out of a pool) from centrally administered servers.

DIRECTORY SERVICES A service that provides information about network objects. DNS (Domain Name System) provides node address information.

DMZ DeMilitarized Zone. A partially-protected zone on a network not exposed to the full fury of the Internet, but not fully behind the firewall. A DMZ is a host computer or computer network which is inserted as a neutral zone between two other computer networks, one or both of which are untrusted.

DNS Domain Naming System is a mechanism used in the Internet and on private Intranets for translating names of host computers into addresses.

DOCSIS Data Over Cable Service Interface Specification. A North American cable modem initiative, DOCSIS is now known as CableLabs Certified Cable Modem, a term trademarked by CableLabs. The specifications themselves remain known as DOCSIS, and are of several versions.

DOT COM A company which operates its business mainly on the Internet, using ".com" URLs.

DSL. Digital subscriber line. See ADSL.

DSLAM Digital Subscriber Line Access Multiplexer. A device used in a variety of DSL technologies, which are lumped under the category of xDSL, with "x" being the generic "what ever." A DSLAM serves as the point of interface between a number of subscriber premises and the carrier network.

At each subscriber premises is a splitter or a standalone modem, depending on the specific form of xDSL involved. The DSLAM generally is positioned in the ILEC's (Incumbent Local Exchange Carrier's) Central Office (CO).

DUAL TONE MULTI FREQUENCY (DTMF) Term describing push button or Touchtone dialing. In DTMF when you touch a button on a push-button pad, it makes a tone, actually a combination of two tones, one high frequency and one low frequency.

DUMB TERMINAL A computer terminal with no processing or programming capabilities. Hence, it derives all its power from the computer it is attached to — typically over a local hard wire or a phone line. A dumb terminal does not employ a data transmission protocol and only sends or receives data one character at a time, sequentially.

E911 Enhanced 911 service. Dial 911 in most major cities and you'll be connected to an emergency service run typically by a combination of the local police and local fire departments. The 911 service becomes enhanced 911 emergency reporting services where there is a minimum of two special features added to it. E911 provides ANI (automatic number identification) and ALI (automatic location information) to the 911 operator.

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. Current membership comprises more than 2,000 colleges, universities, and educational organizations, including 200 corporations, with 15,000 active members. (http://www.educause.edu/)

E-MAIL A colloquial term for electronic mail

ENCRYPTION Term for scrambling a message so that no one can read it except for the person for whom it's intended. Encryption is the transformation of data into a form unreadable by anyone without a secret decrypt key.

ENTERPRISE RESOURCE PLANNING (ERP) A concept developed by the Gartner Group to describe the next generation of manufacturing business systems and MRP (material resource planning) software.

EVOLUTION DATA ONLY (EvDO) is a wireless telecommunications technology that provides wireless data connections that are 300,000 to 600,000 bits per second, as much as 10 times faster than a regular dialup modem.

FAILOVER when one individual computer fails, another automatically takes over its request load. The transition is invisible to the user. Failover involves switching off the failed redundant component and switching on the backup unit. A disk subsystem is running in failover mode when it switches to a hot spare or begins to use the backup disk in a mirrored pair.

FAX Facsimile equipment which allows hard copy (written, typed, or drawn material) to be sent through the switched telephone system and printed out elsewhere.

FCC Federal Communications Commission. The organization based in Washington D.C. set up by the Communications Act of 1934. It has the authority to regulate all interstate (but not intrastate) communications originating in the United States. The FCC is the U.S. federal regulatory agency responsible for the regulation of interstate and international communications by radio, television, wire, satellite, and cable.

FERPA The Family Educational Rights and Privacy Act (FERPA). (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. From http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FIPS Federal Information Processing

FIREWALL Hardware or software, or both, which protects against two threats from outside the firewall: 1. Denial of service. 2. Intrusion. Firewalls do not protect against computer viruses and spam e-mails. For that you need other protection.

FTE (1) Full-time equivalent, a call center term, or full-time employee. (2) In higher ed, full-time enrollment.

GLB Gramm-Leach-Bliley The *Gramm-Leach-Bliley Act*, also known as the *Gramm-Leach-Bliley Financial Services Modernization Act*, was enacted by Congress Nov. 12, 1999. It opened up competition among banks and addressed the issue of disclosure of nonpublic personal information. http://www.ftc.gov/privacy/glbact/glbsub1.htm

GSM Originally stood for Groupe Speciale Mobile. Now it's known as Global system for mobile communications. It is the standard digital cellular (also called mobile) phone service you will find in Europe, Japan, Australia, and elsewhere.

HACKER Originally, a person who "hacks" away at a programmable system until it works. In contemporary lingo, a person who breaks into computer systems, usually over the Internet.

HIPAA Health Insurance Portability and Accountability Act Enacted in 1996, this act presents standards for the maintenance and transmission of personal information regarding individuals.

HONEYPOT A honeypot is a decoy server attached to the Internet designed to attract hackers' attention. The honeypot gives the owner of a targeted server a chance to analyze the attack, develop a strategy to thwart the attack and to block access without causing damage to the main server.

HOST 1. An intelligent device attached to a network. 2. A mainframe computer. 3. A computer with full two-way access to other computers on the Internet.

HOT SPOT A small geographic area of several thousand square feet in which you can get access to a 802.11b wireless local area network (also called WiFi) which is in turn connected to the Internet, and thus the World Wide Web.

HTTP Hypertext transfer protocol. HTTP is the standard way of transferring information across the Internet and the Web.

HTTPS Hyper text Transfer Protocol Secure. A type of server software which provides the ability for "secure" transactions to take place on the World Wide Web. If a

website is running off an HTTPS server, you can type in HTTPS instead of HTTP in the URL section of your browser to enter into the "secured mode."

HUB The point on a network where circuits are connected.

HVAC Heating ventilation and air conditioning systems

IDS 1.Internal Data Service 2. Intrusion Detection Service

IEEE Institute of Electrical and Electronics Engineers Inc. IEEE, founded in 1884, says it's the world's largest technical professional society, consisting of over 360,000 members in 175 countries. www.ieee.org.

IEEE 802.11A is an updated, bigger, better, faster version of 802.11b (also called WiFi), which is now commonly installed in offices, airports, coffee shops, etc. The newer 802.11a, also an IEEE standard for wireless LANs, supports speeds up to 54 Mbps. 802.11a runs in a 300MHz allocation in the 5 GHz range, which was allocated by the FCC in support of UNII (the Unlicensed National Information Infrastructure).

IEEE 802.11B is now the most common wireless local area network. 802.11b is now installed in offices, airports, coffee shops, hotels, boardrooms and homes. 802.11b is also called WiFi or WiFi (Wireless Fidelity). 802.11b is a low power wireless system so the closer you are to a transmitter, the faster it will be.

IEEE 802.11G In November, 2001, Task Group G of the IEEE's 802.11 Committee voted to finish the specs on a new wireless networking standard (802.11g) that would allow wireless data rates up to 54 megabits per second in the 2.4 GHz spectrum.

IM Instant Messaging

INTERNET To say that the Internet is the world's largest and most complex computer and communications network is to trivialize it. But it is. The global network of computer-based information networks, accessed by their computers through established communications protocols and logon procedures.

INTERNET PROTOCOL (IP) Part of the TCP/IP family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages. Used in gateways to connect networks at OSI network Level 3 and above.

INTERNET TELEPHONY In the very beginning, Internet telephony simply meant the technology and techniques to let you make voice phone calls—local, long distance and international—over the Internet using your PC. The definition of Internet telephony is broadening day by day to include all forms of media (voice, video, image), all forms of messaging, and all variations of speed from real time to time delayed.

INTERNET2 is a high-speed network created by a consortium of U.S. universities called the University Corporation for Advanced Internet Development (UCAID). It transmits high quality audio and video with almost no delay. Thirty-four universities announced the formation of Internet2 in October 1996. http://www.internet2.edu/.

INTRUSION DETECTION A technology that gathers and analyzes information across gateways, servers, and desktops to identify possible security breaches that can occur from within or outside an organization.

IVR Interactive Voice Response. Think of IVR as a voice computer. Where a computer has a keyboard for entering information, an IVR uses remote touchtone telephones. Where a computer has a screen for showing the results, an IVR uses snippets of recordings of human voice or a synthesized voice (computerized voice).

JITTER is variability in latency, or delay. If a network provides varying levels of latency (i.e. different waiting times) for different packets or cells, it introduces jitter, which is particularly disruptive to audio communications because it can cause audible pops and clicks.

KEYLOGGER / KEYLOGGING Keylogging software, also called a keylogger, is a piece of software that sits on your PC and records every keystroke you type – including passwords and email messages. Then secretly mails out copies to whomever planted the keylogger.

LAN Local area network. A fancy name for a communications network connecting personal computers, workstations, printers, file servers, and other devices inside a building or a campus.

LDAP Lightweight directory access protocol. LDAP defines a standard manner of organizing directory hierarchies and a standard interface for clients to access directory servers.

LINUX Open-source computer operating system

LOCAL LOOP The physical connection from the subscriber's premise to the carrier's PoP (point of presence). The local loop can be provided over any suitable transmission medium, including twisted pair, fiber optic, coax, or microwave.

LONG DISTANCE Any telephone call to a location outside the local service area. Also called toll call or trunk call.

MAC Moves, adds, and changes.

MAN Metropolitan Area Network. A high-speed data intra-city network that links multiple locations within a campus, city, or LATA.

MODEM Acronym for MOdulator/DEModulator. Conventional modems comprise equipment which converts digital signals to analog signals and vice versa.

MODULATOR See Modem.

MP3 / MPEG Layer3. MP3 is the most popular audio-compression format on the Internet. MP3 provides an efficient audio-coding scheme, which allows compression of audio files by a factor of up to 12, with little loss in quality from the original CD.

MPLS Multi-protocol label switching. A family of IETF standards in which the Internet protocol networks can make forwarding decisions based on a pre-allocated label to setup a label switches path (LPS). MPLS grew out of Cisco's proprietary TAG switching protocol.

MULTIMODE FIBER (MMF) is a type of optical fiber mostly used for communication over shorter distances, e.g. within a building.

NAPSTER is a web-based service that allows its members to download music from the hard disks of the PCs belonging to other members. Napster's brilliance was creating the software that allowed peer-to-peer (P2P) computing.

NETWORK INTERFACE CARD /NIC card. A printed circuit board comprising electronic circuitry for the purpose of connecting a workstation to a LAN (local area network).

NIST National Institute of Standards and Technology, which was formed in 1901 as the National Bureau of Standards, is part of the U.S. Department of Commerce.

OPEN SOURCE Open source software is typically free. It's typically written by programmers all over the world contributing their efforts for the common good of mankind. Open source promotes software reliability and quality by supporting independent peer review and rapid evolution of source code. To be certified as open source, the license of a program must guarantee the right to read, redistribute, modify, and use it freely.

OPTICAL FIBER A thin (approximately 125 micrometers in diameter) silica glass cable with an outer cladding material and around 9 micrometers diameter inner core with a slightly higher index of refraction than the cladding. A typical index of refraction is 1.443 so that light travels in a fiber at roughly 2/3 the speed of light in a vacuum. Optical fiber is made of glass or plastic, and guides light, whether or not it is used to transmit signals. Optical fiber is an almost ideal transmission medium.

PACKET SNIFFER Most data is now transmitted in packets. A packet sniffer is a piece of software that simply examines every packet on whichever circuit(s) it's assigned to monitor. A packet sniffer could be used by a legitimate company to protect itself against unwanted intruders into its network. It could also be used by an intruder to monitor a data stream for a pattern such as a password or credit card numbers

PBX Private branch exchange. A PBX is a small version of the phone company's larger central switching office.

PEER-TO-PEER (P2P) is a fancy way of saying grid computing and communications. Peer-to-peer describes communications between two entities that operate within the same protocol layer of a system.

PHREAK A phone phreak (also known as a phreaker) is to the phone network community what the original hackers were to the computer revolution.

PIGGYBACKING A technique used at the data link or transport layer in a layered network architecture that allows for transmission acknowledgments to be carried in transmission frames received from the destination.

PODCASTING is a way of having Internet audio programs delivered automatically to your MP3 player so that they be recorded there and you can listen to them at anytime.

POE Power over Ethernet

POINT-TO-POINT A private circuit conversation or teleconference in which there is one person at each end, usually connected by some dedicated transmission line. In short, a connection with only two endpoints.

POS POINT OF SALE / POINT OF SERVICE A point-of-sale device such as a credit-card scanner used for authorization when a purchase is made.

QoS QUALITY OF SERVICE is a measure of the telecommunications—voice, data, and/or video—service quality provided to a subscriber. It's not easy to define "quality" of voice telephone service, which is very subjective. QoS is easier to define in digital circuits, since you can assign specific error conditions and compare them

RAS 1. Remote access server or remote access service 2. Registration, admissions, and status signaling function (H323).

RFI Request for information. General notification of an intended purchase of equipment or equipment and lines sent to potential suppliers to determine interest and solicit general descriptive product materials, but not prices or a formal request.

RFID Radio frequency IDentity. RFIDs are tiny chips and wireless radio antennas that can be embedded into products and used for various identification purposes.

RFP Request for proposal. A detailed document prepared by a buyer defining his requirements for service and equipment sent to one or several vendors. A vendor's response to an RFP will typically be binding on the vendor; i.e., he will be obliged to deliver what he says in his RFP at the prices and following the conditions explained in that RFP.

ROI Return on investment.

ROOTKIT A rootkit is a set of software tools intended to conceal running processes, files, or system data from the operating system. Rootkits have their origin in relatively benign applications, but in recent years have been used increasingly by malware to help intruders maintain access to systems while avoiding detection. (http://en.wikipedia.org/wiki/Rootkit)

ROUTER 1. As software, router is a system-level function that directs a call to an application. 2. As hardware, routers are the central switching offices of the Internet and corporate intranets and WANs.

SATELLITE A microwave receiver, repeater, or regenerator in orbit above the earth.

SERVER Hardware definition: A server is a shared computer on the local area network (LAN) that can be as simple as a regular PC set aside to handle print requests to a single printer. Or, more usually, it is the fastest and brawniest PC around. It may be used as a repository and distributor of data. It may also be the gatekeeper controlling access to voice mail, e-mail, and/or facsimile services.

SIP / SESSION INITIATION PROTOCOL is the most important standard for setting up telephone calls, multimedia conferencing, instant messaging, and other types of realtime communications on the Internet (and corporate intranets)

SLA / SERVICE LEVEL AGREEMENT is that part of a service contract in which a certain level of service is agreed upon. An SLA is therefore not a type of service contract, but rather a part of a service contract. (http://en.wikipedia.org/wiki/Service_Level_Agreement)

SMART ANTENNAS A type of cellular base-station antenna. The technology replaces conventional cell-site antennas with a multibeam antenna array that allows network operators to target the transmission and reception of calls more

precisely and, therefore, reduce the amount of spectrum consumed and the amount of interference. The basic benefit of a "smart antenna" is to allow a cell phone provider to serve more cell phone customers without a new investment in basic cell site radio and electronics

SNIFFER is a registered trademark owned by Network General Corporation. The Sniffer Network Analyzer is a member of the family of Network General products that monitors traffic on a network and reports on problems on the network. The company is sensitive about the word Sniffer being used as a generic term for network monitoring. If you do use it as a generic term, their VP and General Counsel, Scott C. Neely, will write you a letter telling you about trademarks, etc. See next definition.

Sadly Scott's worst nightmare came true. Sniffer is now a generic term used to describe a piece of software which runs on a 802.11(b) equipped PC. The software sniffs out (as in smells out) the existence of an 802.11(b) WiFi hotspot—a small geographic area which will receive and transit data according to the 802.11(b).

SOCIAL ENGINEERING Gaining privileged information about a computer system (such as a password) by skillful lying — usually via a phone call. Often done by impersonating an authorized user.

SONET Synchronous Optical NETwork. A family of fiber-optic transmission rates from 51.84 million bits per second to 39.812 gigabits (billion, or thousand million) per second (and going higher, as we speak), created to provide the flexibility needed to transport many digital signals with different capacities, and to provide a design standard for manufacturers.

SPAM Unsolicited commercial e-mail. Unwanted e-mail.

SSL The Internet has opened a new world of commerce through electronic transactions. To keep unsavory characters that prowl the alleys and byways of cyberspace from stealing important, sensitive information that is sent across a network, secure socket layer (SSL) is used to provide authentication, encryption, and message integrity services. Secure socket Layer, a transport level technology for authentication and data encryption between a Web server and a Web browser, i.e. sending documents around the Internet and the Web.

STREAMING VIDEO (media) – streaming video is basically audio and video coming at you in packets over the Internet.

SWITCH A mechanical, electrical, or electronic device which opens or closes circuits, completes or breaks an electrical path, or selects paths or circuits.

SYNCHRONOUS The condition that occurs when two events happen in a specific time relationship with each other and both are under control of a master clock. Synchronous transmission means there is a constant time between successive bits, characters, or events.

T1 / TRUNK LEVEL 1. A digital transmission link with a signal speed of 1.544 Mbps (million bits per second) in both directions.

TCP/IP According to Microsoft: Transmission control protocol/Internet protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems. TCP (transmission control protocol) and IP

(Internet protocol) are only two protocols in the family of Internet protocols. Over time, however, "TCP/IP" has been used in industry to denote the family of common Internet protocols.

TDM / TIME DIVISION MULTIPLEX A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by interleaving a piece of each signal one after another.

TELECOMMUNICATIONS ACT OF 1996 U.S. A federal bill signed into law on February 8, 1996 "to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage rapid deployment of new telecommunications technologies."

TEXT-TO-SPEECH (TTS) Technologies for converting written text into spoken speech output.

TFTP / TRIVIAL FILE TRANSFER PROTOCOL A simplified version of FTP that transfers files but does not provide password protection or user-directory capability.

TOUCHTONE is a generic term for pushbutton telephones and telecommunications services.

UNIFIED MESSAGING SYSTEM Also called integrated messaging, universal messaging, and unified communications (UC). You walk into your office in the morning. You turn on your PC and load up your messaging software, e.g. Microsoft Outlook. That's the software you typically use to receive and send e-mails. Only today, you notice that instead of seeing only e-mails awaiting your reading pleasure, you also see faxes and voice mails received by your telephone system. You can seem them all in one list.

UNIFORM RESOURCE LOCATOR (URL) An Internet term. A standardized way of accessing various resources on the Web. In more technical terms, a URL is a string expression that can represent any resource on the Internet or local TC/IP system. The standard convention for a URL is as follows: method://host_spec {port} {path} {file} {misc}

UNIVERSAL SERVICE FUND (USF) Under the direction of the FCC, the National Exchange Carriers Association (NECA) administers the USF, which is a cost-allocation mechanism designed to keep local exchange rates at reasonable levels, especially in "high cost" (i.e., rural) areas.

UPS / UNINTERRUPTIBLE POWER SUPPLY A device providing a steady source of electric energy to a piece of equipment. Typically used to provide continuous power in the event of a failure of the commercial power system.

VIDEO CONFERENCING Videoconference is to communicate with others using video and audio software and hardware to see and hear each other.

VPN / VIRTUAL PRIVATE NETWORK With VPN, employees can log into a distant corporate local area network, server, or corporate intranet over the Internet.

VLAN / VIRTUAL LOCAL AREA NETWORK. A VLAN in a switched network is a collection of devices grouped together to form a virtual network within a larger network. VLANs allow an administrator to create networks based on parameters beyond the network address, hence the name "virtual."

VOICE OVER INTERNET PROTOCOL (VoIP). A VoIP phone call is transmitted over a data network. The "Internet Protocol" is a catchall for the protocols and technology of encoding a voice call that allow the voice call to be slotted in between data calls on a data network.

VOICEMAIL Allows you to receive, edit, and forward voice messages.

WAN Wide area network

WEP Wired Equivalency Privacy (WEP) is an optional IEEE 802.11b (WiFi, or Wireless Fidelity) feature designed to offer privacy equivalent to that of a wired LAN.

WAN / WIDE AREA NETWORK A public voice or data network that extends beyond the metropolitan area.

WIFI Wireless Fidelity, A WLAN specified by the IEEE as 802.11b

WIKI A wiki, in its simplest form, is a website that can be written upon and edited by multiple users at once.

WiMAX Worldwide Interoperability for Microwave Access is a broadband wireless solution that is based on standards recommendation from both the Institute of Electrical and Electronics Engineers (IEEE) 802.16 working group and the European Telecommunications Standards Institute (ETSI).

WIRE TAP The attaching to a phone line of a piece of equipment whose job is to record all conversations on that phone line. Wire taps are illegal. Law enforcement agencies use them, but must receive authorization from a court to apply the tap. Such authorizations are given if the law enforcement agency argues that applying the tap will prevent crime or help bring a suspected criminal to justice. Wire taps are not authorized lightly.

WIRELESS Without wires. Any system of transmitting and receiving information without wires.

WORM A malicious piece of software that duplicates itself repeatedly.

Index

A
acceptable-use policies, 50
access
  broadband, 12, 14
  from dorm networks, 72
  to Internet, 12
  to mission-critical applications, 93–94
  to services, 80
  wireless Internet in classrooms, 8
access controls, 42
  firewalls, 42–43
  virtual private networks, 43
access points (APs), 46
  IEEE 802.11 support, 71
  rogue, 46
account management
  centralizing administration of, 40
  for network security, 39–41
  for systems and resources, 40
accounting, 39–41
ACUTA, 7
  membership characteristics, 9
administrative services *versus* student services, 79–80
adoption of technology in workplace, 15
adware, 35
AECOM Services Group, outsourced network management tasks, 20–21
alarms, 90
  for security incidents, 56
alternative technologies, considering, 112
alumni student-support system, 76
Amazon.com, 22
Angel, 76
application development, outsourcing, 21
application student-support system, 75
applications
  general productivity tools, 89–90
  and services, 81

applications development, 90
communications requirements, 94
appropriations, state, for funding telecommunications systems, 96–97
architecture
physical network, securing, 55
Web-based, 94
assessment audits, 41–42
assets
criticality and sensitivity of, 51
digital asset management systems, 85, 87–88
enterprise asset management systems, 88
identifying and prioritizing, 51
managing, 88–89
protecting, 54–55
asymmetric digital subscriber line (ADSL) service, 70–71
asymmetric encryption, 47
auditing compliance with security policies, 41–42
authentication, 39–41
authorization, 39–41

B
backup operations centers (command centers)
establishing, 61
securing, 61
biometrics, 27–28, 91
blogging, 25–26
blogs, 25
Bluetooth, 17
bonds, for financing telecommunications systems, 107
broadband access
demand for, 12
international, 14
over long distances, 19
broadband network services, 68
building controls, 90
business analysis, consulting services for, 116
business continuity management, definition of, 57
business initiatives, 9–10
business intelligence, from Web services data, 23
business-to-business (B2B) applications, 9

C
cable television service, 69–70, 73–75
campus distribution, 74
consultant analysis and management of, 116
digital cable, 74
head-end for channel bundling, 74
IP television, 75
pay-per-view service, 75
payment for programming, 73–74
campus constituencies, communicating benefits of IT expenditures to, 111–112
campus networks. *See also* telecommunications systems; university telecommunications
dorm network access, limiting, 72

peer-to-peer traffic, limiting, 72–73
virus and worm protection, 73
campus PBX service, 68
capital programs, funding, 110
cellular telephone service, 68
cellular telephones. *See also* communications devices
on campus, 67
customer expectations of, 15
Center for Advancing Business through Information Technology (CABIT), 29
centralization, 81
centralization of network services, 37
Centrex service, 68
certificates of participation (COP) financing structure, 100, 102
change management process, for security solutions, 39
chatting, online, 67
chief information officer (CIO), 6, 96
skills requirements of, 28–29
circuit-switched networks, security concerns with, 32–33
classrooms
multimedia-enabled, 7–8
wireless Internet access in, 8
Cognos, 23
collaborative tools, 25
combination devices. *See also* communications devices
customer expectations of, 15
communications devices, 15
affordability of, 17
convergence of, 17
customer expectations of, 15–16
interoperability of, 16
miniaturization of, 17
obsolescence of, 15–16
privacy and security of, 16
communications in higher education. *See* telecommunications systems; university telecommunications
competition
promotion of, 11
in telecommunications, 12–13
competitive local exchange carriers (CLECs), 11
compliance with security policies, 41–42
computer support for student-owned computers, 73
computer viruses, 34
computerized maintenance management systems (CMMS), 88
confidentiality of electronic transmissions, 37–38
connectivity, ubiquitous, 15
consultants, 114
compensation of, 118
engaging, 114–115
selecting one, 117–120
services of, 115–117
working with, 119–120
content, digitalization of, 23–24

content management, 85–86
content management systems, 24
contract negotiations, consulting services for, 116
contributor relations management (CRM), 83–84
controls
  costs of, 53–54
  implementing, 53
  standards and procedures as, 55
convergence, 16–17
  of services, 11–12
cookies, 35
coordinating resources, 109
copper Ethernet service, 69
copyright law infringements, 11
cost analysis, 108–109
  of components, 112
cost management, 109
cost measurement, 109
cost-recovery system, establishing, 8–9
cost reporting, 109
costs
  capital costs, 103–104
  of controls, 53–54
  determining, 108–109
  of firewalls, 43
  forecasting, 110
  of maintenance, 110
  partitioning, 8
  of repair and replacement, 110–111
countermeasures, documenting, 51–52
course enrollment student-support system, 76
course management systems (CMSs), 22, 76–77
critical functions and assets, identifying and prioritizing, 51
CrownPeak, 24
Crystal Reports, 23
customer needs, forecasting, 8
customer relationship management (CRM), 82–83

D
data
  collecting from Web services, 23
  encrypting, 47–48
  loss of, 35 (*See also* network security)
  replication of, 92
data access, selling, 108
data networks, 33–34
  video content transmission over, 33–34
data repositories, 80
  POS system access to, 91
debt financing, for funding telecommunications systems, 97–98
decision making, 109
  financing and technology as drivers of, 112

defense-in-depth, 36
degree audits student-support system, 76
delivery of services online, 8
demilitarized zone (DMZ), 42
denial of service (DoS) attacks, 35
desktop tool sets, 89–90
devices. *See* communications devices
dialtone, as IT funding mechanism, 97
digital asset management system (DAMS), 85, 87–88
digital cable, 74
digital signal transmission, 74–75
digital subscriber line access multiplexor (DSLAM), 70–71
digital television, 74
digitalization, 23–24
disaster management, definition of, 56
disaster plan
    contents of, 59–60
    distribution of, 60
    maintaining, 65–66
    testing, 64–65
    training for, 64–65
disaster planning, 56–66
    alternate sites and operations centers, 61
    considerations, 57
    detection, 60
    end of disaster, determining, 62–63
    initial response, 60
    recovery and restoration, 62
    responsibilities, 57–58
disaster planning group
    membership, 58
    responsibilities, 58–59
disaster recovery/business continuity, 9
disaster recovery management, definition of, 56
disaster response team
    logistics and support, 64
    organization of, 63–64
    responsibilities of, 63–64
disasters
    definition of, 57
    impact analysis for, 52–53
distance education, emphasis on, 10
document imaging, 86
document management, 85–86
documentation
    physical security of, 55
    of security processes and techniques, 38
domain name services (DNS), security issues, 33
dorm networks, limiting access to campus network, 72
Druple, 24

E
e-reserves, 23
EditMe, 25
EDUCAUSE, 9
Ektron, 24
El Paso County RFID system, 27
electronic content management (ECM), 86–87
electronic documents and records management systems (EDRMSs), 85
encryption, 47–48
endowment funds, for financing telecommunications systems, 105
enterprise asset management systems (EAMS), 88
enterprise goals and objectives, developing and documenting, 85
enterprise mission-critical applications, 81–92
  contributor relations management, 83–84
  customer relationship management, 82–83
  desktop tool sets, 89–90
  digital asset management system, 87–88
  document management, 85–86
  electronic content management, 86–87
  enterprise performance management, 84–85
  enterprise resource planning, 81–82
  ID card systems, 91–92
  integrated library systems, 87
  monitoring, signaling, and alarms, 90
  physical assets management, 88–89
  point-of-sale (POS) systems, 91
  server and Web hosting, 90
  telecommunication information management system, 89
  Webpage and applications development, 90
enterprise performance management (EPM), 84–85
enterprise resource planning (ERP), 81–82
entertainment services, 73–75
equipment
  inventorying, consulting services for, 116
  lease financing, 101–102
  obsolescence and financing, 99, 104
  physical security of, 54–55
Equipment Leasing Association (ELA), 99
Ethernet service
  copper, 69
  wireless, 71–72
ethical computing policies, 50
excess cash, for funding telecommunications systems, 97
external financing of telecommunications systems, 104
  bonds, 106
  fund raising, 107
  leasing, 107
  public funds, 106–107
  student resale, 107–108

F
Facebook, 25
Family Education Rights and Privacy Act (FERPA), 35
FCC Act of 1932, 11
Federal Information Processing Standards (FIPS) 199, 57
federated identity
  importance of, 27–28
financial accounting services, 82
financial aid student-support system, 76
financing telecommunications systems. *See also* IT funding
  assumptions, addressing, 112
  certificates of participation (COP) financing structure, 100, 102
  debt financing for, 97–98
  decision making and, 112
  external sources, 104, 106–108
  internal sources, 104–106
  leasing and lease-purchase financing, 98–101, 107
  legal constraints on institutions and, 103
  political constraints on institutions and, 103
  vendor financing, 98
firewalls, 42–43
  costs of, 43
five nines reliability, 7
Friendster, 25
fund-raising
  contributor relations management systems for, 83–84
  for financing telecommunications systems, 107
funding. *See also* financing telecommunications systems
  capital programs, 110
  models and strategies for, 109

G
The Gathering Storm, 10
Google, 24
  digitalization of library collections, 24
governance, organization, and leadership, 9
Gramm-Leach-Bliley (GLB) act, 35

H
Hampton RFID system, 27
handwriting recognition improvements, 28
hashing, 47–48
Health Insurance Portability and Accountability Act (HIPAA), 35
help desk services, outsourcing, 21
help desks, 89–90
high-definition television (HDTV), 75
higher education
  changes in, 10
  enrollment increases, 10
honeypots, 45
Hong Kong Airport RFID system, 27
host-based IDSs, 44
human interface design, improvements in, 28
human resource services, 82

human resources, identity management responsibilities, 91–92
human threats, 52
Hutchinson, Peter, 53

I
ID card systems, 91–92
identity management
  with ID card systems, 91
  importance of, 27–28
  systems for, 13
IEEE 802.11 standard, 46
IEEE 802.11a wireless Ethernet, 71
IEEE 802.11b wireless Ethernet, 71
IEEE 802.11g wireless Ethernet, 71
IEEE 802.1X standards, 47
imaging, document, 86
impact analysis, 52–53
incident response, 50
incumbent local exchange carriers (ILECs), 11
independent institutions, IT funding, 104–108
industry directions, forecasting, 8
information assets, criticality and sensitivity of, 51
information security personnel, shortage of, 20
information technology (IT) department
  consulting services for design and structure, 115–116
  services supported by, 6–7
  as strategic resource, 6, 14
  support for communications applications, 6
infrastructure, 9
Inside Contactless, 27
installation, consulting services for, 116
integrated library systems (ILS), 87
internal audits, 42
internal financing of telecommunications systems, 104
  endowment funds, 105
  operating funds, 105–106
  reserves, 105
international issues, 13–14
international research network, 14
International Telecommunication Union (ITU), 14
Internet2, 14
Internet, protecting network from, 42–43
Internet access, demand for, 12
Internet access technology
  capital replacement scheme, 12
  changes in, 12
  infrastructure investments in, 12
Internet services, 69–73
Internet World Stats, 34
Interwoven, 24
intrusion detection systems (IDSs), 44–45
intrusion prevention systems (IPSs), 45
IP television (IPTX), 75
IT centralization, 81

IT funding, 9. *See also* financing telecommunications systems
considerations for, 108–112
independent institutions, 104–108
insourcing, out-tasking, outsourcing and, 9
public institutions, 95–104
IT investments, aligning with institutional priorities, 110
IT personnel
consultants, 114–120
recruiting strategies, 111
retention strategies, 111
shortage of, 20
training, 111, 116
IT support desks, 89–90

J
Jacobi Medical Center RFID patient ID system, 27

K
key performance indicators (KPIs), 85
knowledge management, 24

L
leasing and lease-purchase financing
advantages of, 99–100
how it works, 98–99
lease term, 104
revenue bonds and COPs, 100–101
for telecommunications systems, 107
lectures, viewing options, 8
legacy systems, 93
legal constraints on institutions, and IT system financing, 103
library collections
digitalization of, 24, 26
radio frequency tags for, 26
library student-support system, 76
LiveJournal, 25
long-distance telephone service, 68
revenue from, 107–108

M
maintenance costs, forecasting, 110
managed security services, 20
MasterFormat 2004, 55
May, Thornton, 29
mergers and acquisitions, 13
Mindbridge, 24
mission-critical applications
access to, 93–94
college/departmental, 92–93
enterprise, 81–92
legacy systems, 93
mission-critical functions, identifying and prioritizing, 58

mobility, 17–18
  form factor for, 17
modems, 33
Modified Final Judgment of 1982, 11
Moinmoin, 25
monitoring
  of physical building, 90
  of physical network design, 56
Mozilla, 72
multiband networks, 18
multilayered services, 16
multimedia-enabled classrooms, 7–8
music sharing, 11. *See also* peer-to-peer networking

N
Napster, 72
needs assessment, consulting services for, 116
Net neutrality, 12
network-based IDSs, 44
network hardening, 35
network keys, 46–47
network management, outsourcing, 20
network security
  authentication, authorization, and accounting, 39–41
  breaches, symptoms of, 35
  goals of, prioritizing, 36
  importance of, 13
  network hardening, 35
  nontechnical strategies, 36–42
  risk assessment, 35–36
  technologies for, 42–45
  threat identification, 34–36
  for wireless networking, 46–48
network security technologies, 42–45
  access controls, 42
  firewalls, 42–43
  honeypots, 45
  intrusion detection systems, 44–45
  intrusion prevention systems, 45
  virtual private networks, 43
network services, centralized *versus* decentralized, 37
networks. *See also* network security
  access controls for, 42
  campus networks, 72–73
  circuit-switched networks, 32–33
  connecting by VPN, 43
  data networks, 33–34
  design of, consulting services for, 116
  dorm networks, 72
  international research network, 14
  mesh networks, 18
  multiband networks, 18

multilayered services on, 16
physical design of, 55
segmenting, 43
social networks, 25
video networks, 33
virtual local area networks, 16
virtual private networks, 17–18, 43, 72
voice networks, 32–33
wireless networks, 46–48
neutral zone, 42
1996 Federal Telecommunications Act, 11
Nortel security offerings, 28

O
obsolescence
of communications devices, 15–16
of equipment, 99, 104
online billing systems, 9
online registration, 67
operating funds, for financing telecommunications systems, 105–106
organizational flexibility, 111
Osborne, David, 53
other debt, for financing telecommunications systems, 107
out-tasking, 9
outsourcing, 9
to consultants, 114–120
establishing successful partnerships, 21
increasing use of, 20–21
intrusion detection systems, 44
network security, 36

P
packet shaper, 72
pay-per-view cable television service, 75
peer-to-peer networking, 11
limiting, legal requirements for, 72–73
Percussion, 24
performance indicators, 85
personal digital assistants (PDAs). *See also* communications devices
customer expectations of, 15
personal DVD players. *See also* communications devices
customer expectations of, 15
personal identity data
compromise of, 92
managing, storing, and maintaining, 91–92
personnel policies, 50
physical assets management, 88–89
physical security, 54–56
breaches in, 32
PicoTag labels, 27
plain old telephone service (POTS), 6
point-of-sale (POS) systems, 91

policies
acceptable-use policies, 50
application and management of, 16
auditing compliance with, 41–42
ethical computing policies, 50
personnel policies, 50
security policies, 50–51
standardization of, 37–41
for suppliers, 51
technology policies, 28
user account eligibility and elimination policies, 40–41
political constraints on institutions, and IT system financing, 103
The Price of Government (Osborne and Hutchinson), 53
primary operations centers
equipping, 61
establishing, 61
privacy of electronic transmissions, 37–38
processes, standardization of, 37–41
product obsolescence, 15–16, 99, 104
program management, 49–51
prosumerism, 15–16
public funds, for financing telecommunications systems, 107
public institutions, IT funding, 95–104

Q
quality assurance process for security solutions, 39
quality-of-service (QoS), traffic prioritization for, 16
query-based reporting tools, 23

R
radio frequency, increasing use of, 27
radio frequency identification (RFID), 26–27
Recording Industry Association of America (RIAA)
legal actions, 11
position against peer-to-peer data sharing, 72–73
records management, 86
recovery and restoration from disasters, 62
recruiting strategies, 111
regulation of technology, 28
regulatory and legal environment, 10–12
remote users, connecting to network by VPN, 43
repair and replacement costs, managing, 110–111
request for information/request for proposal preparation, consulting services for, 116
research network, international, 14
reserves, for financing telecommunications systems, 105
residence halls
cellular service penetration in, 68
VoIP in, 68
residential services, 67–75
cable television and entertainment services, 73–75
Internet or broadband network services, 69–73
network access, limiting, 72

peer-to-peer traffic, limiting, 72–73
student-owned computer support, 73
telephone services, 68
virus and worm protection, 73
resnets, 72
retention strategies, 111
risk analysis, 51–54
risk in academic setting, 111
risk metrics, establishing, 54
risk mitigation, 53–54

S
scorecards on performance, 85
secure socket layer (SSL) for VPNs, 18
security
balancing with usability, 32
focus on, 28
importance of, 13
policies for, 50–51
security and identity management, 9
security audits, 41–42
security awareness, promoting, 50
security breaches, 48
disclosure of, 38
security planning
governance of, 49–50
risk analysis, 51–54
security threats, identifying, 34–36
segmentation, network, 43
senior management, sponsorship, commitment, and visible support for security plan, 49–50
Serra, Didier, 27
server services, 90
service components
costs, partitioning of, 8
subsidizing, 8–9
service delivery
online, 8
service providers
constant change in, 12–13
long-term contracts with, 8
services, 6–7
access to, 80
applications and, 81
availability of, 93–94
converged, 11–12
outsourcing, 20–21
reliability of, 7
unbundling, 11
session initiation protocol (SIP)
for integration of services, 17
for VoIP, 68

shadow systems, 92
signaling, 90
single-account realms, 40
small-equipment lease financing, 101–102
smart building systems, 90
social engineering, 25
social networks, 25
software selection, consulting services for, 117
space management systems, 88
spyware, 34–35
staffing. *See also* IT personnel
  for network security, 36–37
standards and procedures
  for network security, 37–41, 55
strategic planning, 9, 109
  consulting services for, 115
student activities student-support system, 76
student desks, electric power supply for, 8
student enrollment, increases in, 10
student fees, as IT funding mechanism, 97
student housing student-support system, 76
student information management systems (SIMS), 75–76
student-owned computer support, 73
student resale, for financing telecommunications systems, 107–108
student services
  versus administrative services, 79–80
  considerations for, 77
  habits of, considering, 77
  residential services, 67–75
  student participation in, 77
  support services, 67
  trends, anticipating, 77
  variations in, 67
student support services, 67, 75–77
  course management systems, 76–77
  student information management systems, 75–76
success, measuring, 111
supplicants, 47
suppliers, personnel security policies for, 51
support for student-owned computers, 73
Symantec security offerings, 28
symmetric encryption, 47
system architectures
  securing, 55
  Web-based, 94
system evaluation, consulting services for, 116
systems development, communications requirements, 94
systems maintenance, technological expertise for, 7

T
tactical planning, consulting services for, 115
teaching styles, 7–8

technical controls for security, 55–56
technological changes, GNP and, 10
technology
  adoption of in workplace, 15
  change in, 6–7
  leasing, 98–103
  new, consulting services for, 116
  prices, trends in, 8
  regulation of, 28
telecommunication information management system (TIMS), 89
telecommunications
  trends in, 15–27
telecommunications director, 95–96
telecommunications equipment. *See* equipment
telecommunications industry
  issues in, 12–13
  mergers and acquisitions, 13
telecommunications spaces, physical security of, 54
telecommunications systems
  budgeted cash-flow analysis for, 104
  capital cost of, 103–104
  consultant services for, 114–120
  costs, determining, 108–109
  external financing of, 104, 106–108
  financial options, cataloging, 96–103
  financing option, determining, 103–104
  funding, 95–112
  funding models and strategies, 109
  implementing, 109–110
  internal financing of, 104–106
  obsolescence of equipment, and financing, 99, 104
telephone services, 68, 107–108
telephones, campus requirements for, 7
television offerings, franchising, 11
testing
  consulting services for, 116
  of network security solutions, 38–39
threats, identifying, 51–52
3G systems, 19
training
  consulting services for, 116
  strategies for, 111
trends in telecommunications
  blogging, 25–26
  convergence, 16–17
  digitalization, 23–24
  mobility, 17–18
  outsourcing, 20–21
  prosumerism, 15–16
  radio frequency identification, 26–27
  social engineering, 25
  Web services, 21–23
  wireless technologies, 18–19

triple play services, 11
TWiki, 25

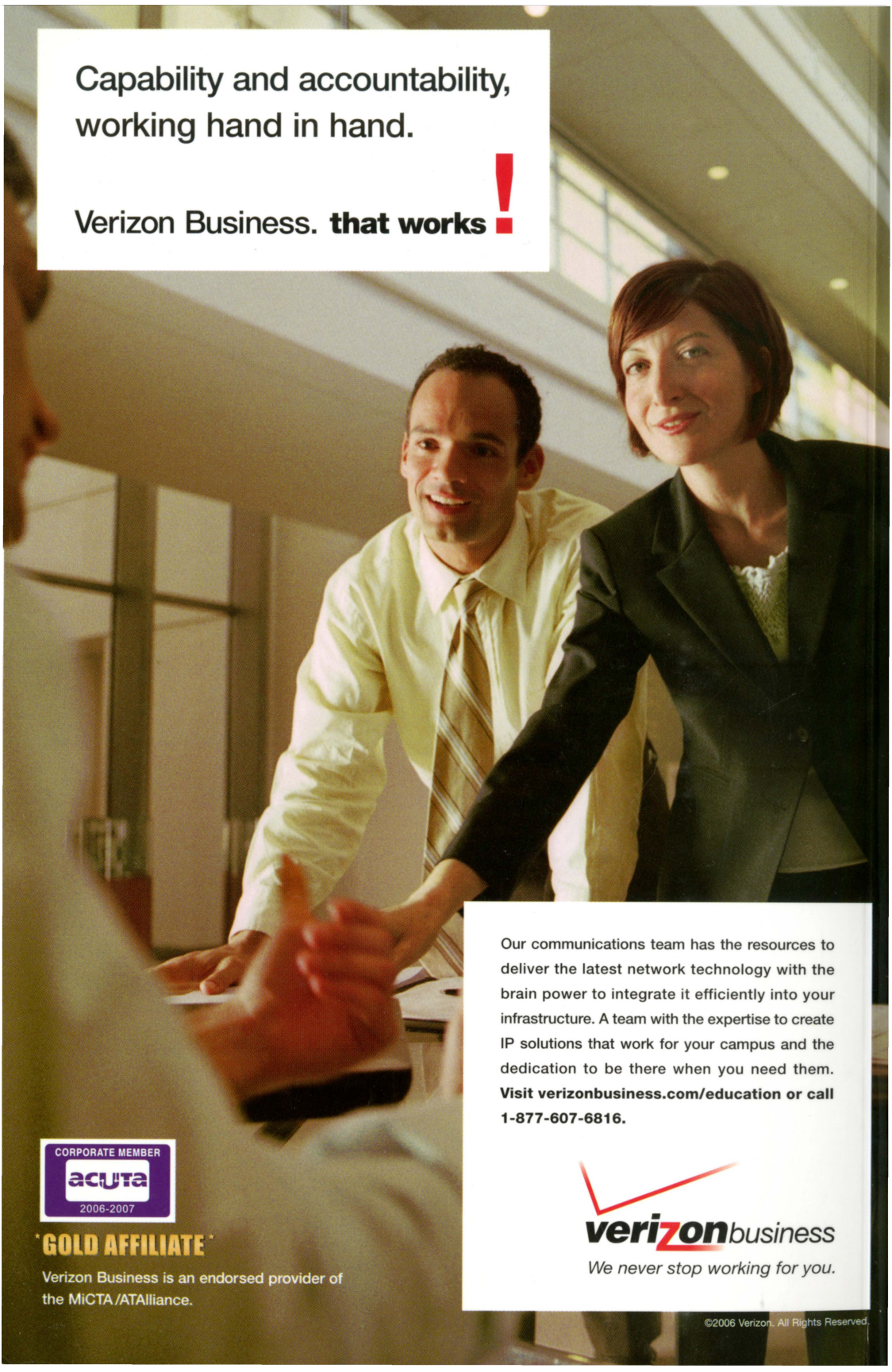
U
United States broadband penetration, 14
universal service, 11
Universal Service Fund, 11
universities, dependence on communications technology, 10
University of Texas at Austin (UT) IT financial structure, 96
university telecommunications. *See also* telecommunications systems
  business aspects of, 8–9
  business initiatives, 9–10
  changes in, 7
  funding the system, 95–112 (*See also* financing telecommunications systems)
  staffing levels, 8 (*See also* IT personnel)
  as strategic resource, 6, 14
  telecommunications to communications technology shift in, 9–10
  themes and trends in, 7–8
U.S. economy, workforce education and, 10
user account eligibility and elimination policies, 40–41
user account management, 39–41
user education, consulting services for, 116, 120
user training, consulting services for, 116
users, security awareness of, 50

V
value, reporting, 111
vendor financing, for funding telecommunications systems, 98
vendor proposals, consulting services for evaluating, 116
vendors
  dependence on, 9
  personnel security policies for, 51
  stability and track records of, 21
video content transmission over data networks, 33–34
video networks, 33
virtual local area networks (VLANs) for policy application and management, 16
virtual private networks (VPNs), 43
  mobility trend and, 17–18
  on wireless networks, 72
viruses, 34
  protection for campus networks, 73
voice networks, 32–33
voice over IP (VoIP), 11, 19
  for residence halls, 68
voice recognition, improvements in, 28
VoIP over WiFi, 19
VPN appliances, 43
vulnerabilities, identifying, 51–52

W
Web-based services delivery, 8
Web hosting services, 90

Web portals, 9, 22
  daily-use service integration in, 22
Web services, 21–23
  business intelligence derived from, 23
  self-service centers, 22
  service availability, 22
  Web portals, 22
WebCT/Blackboard, 76
Webpage development, 90
WiFi, built-in security, 46
WiFi Multimedia (WMM) specification, 18–19
WiFi Protected Access (WPA), 46, 72
wikis, 25
WiMAX technology, 19
Wired Equivalent Privacy (WEP), 72
wireless communications, international use of, 13–14
Wireless Encryption Protocol (WEP), 46
wireless Ethernet service, 71–72
wireless technologies, 18–19
  in classrooms, 8
  deployment rate, 18
  mesh networks, 18
  peer-to-peer technologies, 19
  point-to-point, 18
  quality of service, 18–19
  securing, 46–48
  security concerns, 72
  self-like seeking, routing, healing devices, 19
  thin access points, 18
  3G systems, 19
  VoIP over WiFi, 19
  WiMAX technology, 19
work order management systems (WOMS), 88
worms, 34
  protection for campus networks, 73

Z
zero day reaction times, 45


Capability and accountability,
working hand in hand.
Verizon Business. that works!
Our communications team has the resources to deliver the latest network technology with the brain power to integrate it efficiently into your infrastructure. A team with the expertise to create IP solutions that work for your campus and the dedication to be there when you need them. Visit verizonbusiness.com/education or call 1-877-607-6816.
verizon business
We never stop working for you.
CORPORATE MEMBER
acuta
2006-2007
GOLD AFFILIATE
Verizon Business is an endorsed provider of the MiCTA/ATAlliance.
©2006 Verizon. All Rights Reserved.