Chapter 1

Making the Business Case for the Network

1.1 Management Overview of Network Design

The basic goal of network design is to interconnect various software and hardware devices so that resources can be shared and distributed. Despite the apparent simplicity of this goal, network design is a very complex task that involves balancing a multitude of managerial and technical considerations. This chapter focuses on the managerial decisions involved in planning and designing a network.

Business concerns and philosophy have a profound impact on the network planning process. In some organizations, expenses associated with the network are viewed as "overhead." Taken to an extreme, this view can lead to the perspective that anything but the most basic expenditures on the network are superfluous to the primary business. In this type of environment, it is not uncommon to observe a lack of formal commitment and managerial sponsorship of the network. End users, acting on their own initiative, may buy and install network components and software without working with any central budgeting and planning authority. Although formal budget allocations for the network may not exist, this does not mean that the network is "free." An informal, reactive network planning process is often associated with frequent downtime because the network can be dismantled or changed on a whim, without regard to how the changes might impact the people using it. Thus, there is an opportunity cost associated with the lost staff productivity resulting from the network downtime. There is also an opportunity cost associated with lost productivity resulting from the diversion of staff from their primary job functions to support the network. Furthermore, when changes to the network are not carefully planned and implemented, it compounds the difficulty of maintaining the network in a cost-effective way. For organizations of any substantial size lacking a formal network planning process, it is not uncommon for audits to reveal millions invested in technology that is not effectively utilized and that does not support ongoing organizational needs. Although this is network design at its worst, it is not that uncommon. The moral of this is that ignoring or avoiding direct consideration of the true network costs does not make them go away. A see-no-evil/hear-no-evil/speak-no-evil strategy only “works” when decision makers are not accountable for their actions. In a cost-conscious, competitive business climate that focuses increasing scrutiny on inefficient processes ripe for reengineering, this is a risky approach.

In contrast, there are organizations that view the network as the corporate lifeblood. In this environment there is considerable management accountability for and scrutiny of the network planning and implementation. Increased recognition of the network’s importance to the bottom line improves the chances that the network(s) will be well planned and executed. For example, it is vital to the New York Stock Exchange that its networks perform reliably even under conditions of extreme stress.[1] High-profile, high-performance networks require thorough planning to ensure that they can meet the demands placed upon them. A systems approach is essential to ensuring a comprehensive assessment of critical network requirements.

A *systems approach* means that the requirements are considered from a global perspective that encompasses both top-down and bottom-up views. The discussion that follows outlines a general methodology for performing a systems analysis of the network requirements, from a business perspective. The business perspective is a top-down, big-picture view of how the design will impact the organization. This discussion continues, from a technical perspective, in the chapters that follow. The technical perspective is a bottom-up, narrowly focused view concentrating on essential design details.

1.1.1 Define the Business Objectives

Defining the business objectives is a vital first step in the network planning process. A logical start to the top-down analysis is to define the business objectives served by the network. The business objectives should relate to the strategic focus of the organization. There may be many motivations for building and implementing a network. After the business objectives have been made explicit, they can be prioritized, and objective criteria can be developed for measuring the success of the network implementation. The objectives will also help determine the type of network needed, and the level of expenditure and support that is appropriate. The business objectives have many impacts on technical decisions regarding the selection of technology, the performance requirements, and required resource commitments. When the objectives are poorly defined, there are often many complications down the road.

Many business objectives relate to gaining and maintaining competitive advantage. According to [CARR03], four basic strategies to sustain competitive advantage are:

1. Low-cost leadership
2. Focus on market niche
3. Product and service differentiation
4. Strategic alliances and linkages with partners

Telecommunications technology has transformed business models by supporting all of the above strategies. For example, many small businesses demonstrate low-cost leadership using Internet-based storefronts to offer products and services with less overhead than their larger competitors. If a business has an effective Web site and well-organized internal processes, it is not obvious whether that business has one or a thousand service representatives to support its customers' needs. Thus, even a small business can have a strong presence and international reach.

Interland,[2] a full-service Web hosting provider for small businesses, believes there is vast market potential for software tools to create an online presence for the 20 million businesses in the United States with fewer than ten employees. Interland provides a basic service — for as little as $23 a month — that includes a Web site, a dot.com domain name, and 30 e-mail-message accounts. It also offers hundreds of design templates and "the ability to add and edit pictures and publish and update text without having to program in HTML, or Hypertext Markup Language" so that small companies can easily develop, customize, and maintain their own Web sites with very little cost or training. [LOHR03]

Amazon.com, established in 1994, is another example of how telecommunications technology can be used to capitalize on these strategies for competitive advantage. Amazon.com minimizes its capital outlay by being an exclusively online retailer that holds very little inventory. It outsources almost all of its operations, except for information technology (IT). Integral to Amazon.com's success is its use of sophisticated Customer Relationship Management (CRM) technology to collect and analyze customer buying habits and preferences. Amazon.com leverages customer preference information it collects to effectively target market niches and to make tailored product recommendations to customers when they return to the site. This is called *personalization*. Amazon.com is continuously expanding the breadth and depth of its product offerings through strategic alliances and partnerships with book publishers, retailers (of clothing, toys, electronics, etc.), and technology service providers.

Other business objectives that telecommunications can support include:

- *Compliance with legislation and regulatory requirements that may mandate fundamental business process changes.* An example of this is the Health Portability and Accountability Act of 1996 (HIPAA), which is discussed in more detail in Section 1.5.1. HIPAA has profound and far-reaching impacts on the processing and handling of information and patient records in the healthcare industry.
- *Improved outreach and accessibility.* Many nonprofit and government agencies provide information and services through the World Wide Web because it is a cost-effective means to reach their intended audience.
- *Enhanced marketing efforts to reach new customers and to reduce attrition and churn of existing customers.* This might include customer satisfaction, loyalty, and targeted marketing programs.

New business objectives can have a significant impact on processes, procedures, and systems. Once the business objectives are fully understood, tactical and operational strategies can be developed for the network implementation. To fully understand these impacts, the organization should evaluate:

- Current processes and business practices
- Changes required in current processes and business practices to achieve the desired business objective(s)
- Process, resource, technology, staffing, and organizational requirements for successful implementation

Meetings and idea-generating sessions with decision makers, planners, and other key players can generate a lot of potential business objectives. If the list is long, the "80/20" or Pareto rule can be used to whittle it down to a manageable size.[3] This rule is used to focus on important concerns and to avoid distraction by trivial or overly difficult ones.

To apply the 80/20 rule in the context of management planning, first start by identifying business objectives that are redundant or similar, so they can be aggregated. Objectives that, upon further reflection, appear unimportant should be dropped. Each business objective should be evaluated with

Table 1.1 Identifying High Importance Business Objectives

Pareto Analysis Matrix	*High Importance Business Objectives*	*Low Importance Business Objectives*
High difficulty	Business objective A Business objective B Business objective C ... (Note: these objectives need careful selection and further evaluation)	Business objective X Business objective Y Business objective Z ... (Note: these objectives are definitely not worth pursuing)
Low difficulty	Business objective P Business objective D Business objective Q ... (Note: these objectives should be pursued)	Business objective Ψ Business objective Ω Business objective Φ ... (Note: these objectives are not worth pursuing)

respect to its potential value and difficulty. Table 1.1 suggests a format for collecting and presenting the results of this evaluation. Business objectives with "High Importance/Low Difficulty" ratings (i.e., the "80 percent" solution group) are the most desirable, followed by those having "High Importance/High Difficulty" (i.e., the "20 percent" solution group). High importance objectives are selected for further review and scrutiny. Other objectives on the evaluation list are rejected from further consideration because the effort they require is not warranted by their potential return and risk to the organization.

The surviving business objectives should be carefully evaluated with respect to risk factors, required effort, and the availability of time and resources. Other metrics may be appropriate, depending on the organization and the nature of the project. Each organization should develop its own evaluation metrics based on the input of planners and decision makers and the resulting organizational consensus. Table 1.2 presents a method for scoring each business goal. To use this table, each decision factor should be entered in a separate row under the column labeled "Decision Factor." The example shows risks the organization wants to avoid, with each decision factor measured on a scale from 0- to 100. Decision factors with high scores (i.e., 100) reflect low-risk, desirable outcomes; and those with low scores (i.e., 0) reflect high-risk, undesirable outcomes. Each decision factor, in turn, should be weighted by its relative importance. *The total of all the weights for all the decision factors must sum to one (1).* Note that the final score obtained for the example shown in Table 1.2 should be interpreted as a rank order score. Thus, this score

Table 1.2 Scoring Business Objectives: An Example

Business Objective:	**Decision Factor**	**Decision Factor Score (Max. Score = 100; Min. Score = 0)** **(a)**	**Decision Factor Weighting (%)** **(b)**	**Decision Factor Total Score** **(c) = (a) * (b)**
Provide online shopping capability to DoD for radioactive materials	(Substitute appropriate metrics as required)	(Note: This score is typically determined by organizational consensus)	(Note: The relative weights of the factors with respect to each other are determined by Saaty or other method)	
[redacted]	Legal liability if executed poorly	$(a_1) = 0$	$(b_1) = .50$	$(c_1) = 0.0$
	Required man-hours	$(a_2) = 10$	$(b_2) = .10$	$(c_2) = 1.0$
	Time required	$(a_3) = 50$	$(b_3) = .05$	$(c_3) = 2.5$
	Capital costs	$(a_4) = 2$	$(b_4) = .30$	$(c_4) = .60$
	Other factors	$(a_5) = 90$	$(b_5) = .05$	$(c_5) = 4.5$
Total		**(Note: "100" = Low Risk, "0" = High Risk)**	**100.00%** **(Note: the total of *all* decision weights must exactly equal 100%)**	$\boldsymbol{\Sigma (c_i) =}$ $(0 + 1 + 2.5 + .6 + 4.5) = \mathbf{8.6}$

has meaning only in relationship to the scores assigned to other alternatives under consideration. The scoring is not like high-school grading where a score of "90 to 100" is an A, a score of "80 to 79" is a B, etc. If an alternative $\mathcal{A}_1$ receives a score of "8.6" and this is the highest computed score for all alternatives, then this means that $\mathcal{A}_1$ is the best alternative, based on the decision factors and the weighting used. The score does not mean that that $\mathcal{A}_1$ meets a minimum threshold of acceptance; this must be determined independently. If the next highest ranked alternative,

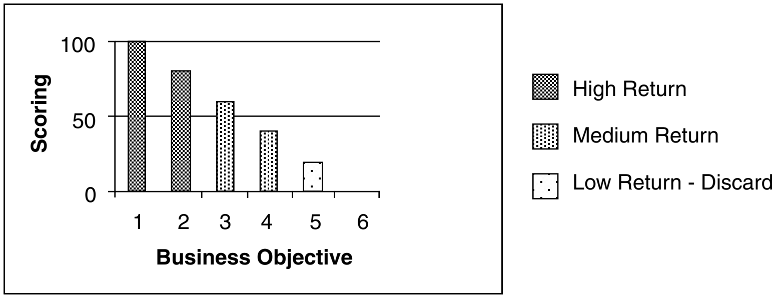

Figure 1.1 Scoring business objectives using Pareto analysis.

$\mathcal{B}_1$, receives a score of "4," this cannot be interpreted that $\mathcal{A}_1$ is twice as good as $\mathcal{B}_1$. It only means that $\mathcal{A}_1$ is to be preferred over $\mathcal{B}_1$. Human judgment is needed to determine the number of final alternatives that will be accepted for consideration, after all the alternatives have been ranked. In some cases, after all the alternatives have been scored and ranked, the decision makers may decide that none of them adequately addresses the requirements at hand. In this case, all the alternatives may be rejected and new alternatives may need to be devised.

A number of methodologies are recommended in the literature to develop relative weights for decision factors.[4] One of the more well known is Saaty's Hierarchical Pairwise comparison method. [SAAT80] Other methods based on fuzzy logic, which incorporate the notion of subjective evaluation factors, are presented in [RUBI92] and [RUBI99]. Once the decision factors and their corresponding weights have been agreed upon within the organization, they should be applied consistently to each and every business objective under consideration. After a total score is calculated for each business objective, Pareto analysis can be repeated to further refine the list of business objectives upon which the organization will concentrate. As presented in this example, high scoring business objectives are preferred over lower scoring ones. This scoring process is illustrated in Figure 1.1.

Scoring each business goal provides a basis for selecting which projects should be undertaken based on the underlying value to the organization. Mathematical scoring helps ensure consistent evaluation across a set of choices. Scoring is a useful tool, but the process should not be applied too stringently because the scoring process may obscure some of the subtleties in the selection process. Scoring should be used as a gross filter, not a fine one. The human element and common sense should prevail during the decision-making process. The intent is to engage the appropriate stakeholders in discussion and to achieve consensus on the organizational focus. This process helps ensure that technology is not being adopted for the sake of technology, but for what it can do for the organization. This is the foundation for an effective technology selection process.

In summary, the business objectives and related findings should be formalized in a written document. We recommend that this report include the following sections:

- Executive Summary
- Business Objectives of the Network
  - *Strategic Objectives and Goals:* this is driven by upper management and their vision and direction for the company or institution.
  - *Tactical Objectives and Goals:* this concerns meeting budget objectives and planning directives.
  - *Operational Objectives and Goals:* this focuses on short-term, day-to-day operational concerns.
  - Desired Competitive Advantage(s)
  - Evaluation Metrics and Their Relative Importance
- Major Functional Units and Staff Affecting and Affected by Proposed Network
- Project Infrastructure
  - Senior Executive Sponsor(s)
  - Project Sponsor
  - Project Manager
  - Team Members
  - Key End Users
  - Support Services and Facilities

1.1.2 Determine Potential Risks, Dependencies, Costs, and Benefits

After the business objectives are well understood, their feasibility should be evaluated in light of the proposed network project. This involves a thorough and systematic evaluation of the resources, people, procedures, and environmental aspects of the network project to determine potential vulnerabilities and interdependencies.

The feasibility of the project should be considered relative to a number of risk factors, including:

- *Technology-related risk factors,* which may include:
  - The use of new and emerging technologies, which are inherently more risky than the use of proven, well-established technologies, and may cause unforeseen delays or expense.

  - Limitations in the technology relative to its intended use. For example, the use of public network infrastructures, such as the Internet, poses different risks and trade-offs than the use of private network infrastructures.
- *Personnel or labor risk factors,* which may include:
  - The organization's experience with similar projects. Often, the network implementation will run into difficulty because the organization is not well positioned to support network maintenance. The ability to manage and maintain the network once it is in place is an important determinant of whether or not the project will succeed.
  - The degree of organizational support and commitment to the network project. Lack of executive follow-through is a major reason large IT projects fail. In part, this is due to the fact that "major IT projects require radical change in an organization… including changes in both job functions and time-honored ways of doing business. Radical change can't occur if people are thinking, 'Does the boss really care about this?'" [WAHL01]
- *Security risk factors,* which may include:
  - Vulnerability to unauthorized outside intrusion via computer viruses, Trojan horses, denial-of-service attacks, and hacker invasions.
  - Vulnerability to inappropriate use of corporate resources by "authorized" system users. An example of this risk is an employee with access to sensitive corporate documents who might illegally copy and make them available to competitors.
- *Financial risk factors,* which may include:
  - Tangible financial impacts resulting from lost profits, budget changes, etc., due to project or network failure. Research has shown that companies with an average market capitalization of $27 billion per year lose "$670 million in market value over a two-day period after announcing an IT related problem, [such] as a hardware or software glitch." [WAHL01]
  - Intangible impacts resulting from loss of customer goodwill, industry perceptions, etc., due to project or network failure. Although these can be very difficult to estimate, they can be very significant. When Citibank publicly admitted in 1994 that hackers had broken into its network, making $10 million in illegal transfers, its banking rivals were quick to court top customers with claims that its computer systems were more secure. [BEHA97] Now, having learned from Citibank's experience, the financial industry keeps security breaches unpublicized. "…companies are increasingly adept at covering up

breaches because disclosing vulnerabilities can leave them open to more attacks and more bad publicity. The dozen FTC investigators working on Internet security cases rely mainly on reports from the news media and individual users." [TEDE03]

- *Disaster risk factors,* resulting from occurrences such as:
  - Natural catastrophes, such as floods, earthquakes, hurricanes, etc.
  - Acts of war
  - Fire
  - Power outages
- *Legislation, regulatory, and liability risk factors,* which may include:
  - Legislation that may either create or eliminate markets and avenues for competition. For example, the United States House and Senate are considering Internet gaming laws that would have far-reaching implications for various local, state, and federal agencies. These laws, if passed, would also "have the potential to impact multiple markets (banking, ISPs, and the U.S.$26 billion gaming industry, for example)." [DAVI03]
  - New regulatory requirements that may force major business process and infrastructure changes to ensure the compliance required for continued operation. For example, The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, has provisions to protect the personal financial information of consumers held by various types of institutions, including banks, securities firms, insurance companies, and institutions offering the following services: lending, brokering, consumer loans, transferring or safeguarding money, individual tax return preparation, financial advice or credit counseling, residential real estate settlement services, and consumer debt collection. [FTC03] It has a major impact on the networking infrastructure, and processes and procedures of these institutions.

After identifying potential risks, it is important to calculate their probability of occurrence and quantify their impacts so the organization can develop mitigating strategies. These strategies — which should be developed as early in the planning process as appropriate — involve risk reduction, control, and transfer. Risk reduction and control might involve, for example, the adoption of a disaster recovery and data continuance strategy. Risk transfer involves shifting the burden of exposure to a third party, often through insurance or outsourcing.

Risks can be evaluated using the techniques outlined in Section 1.1.1. A decision matrix, listing each risk, associated decision factors, and the relative weight of each decision factor, can be summarized in a table similar to Table

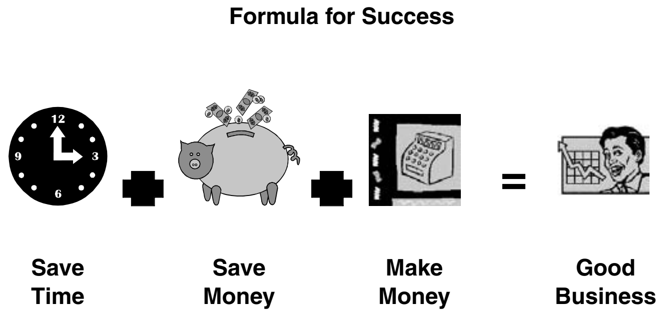

Figure 1.2 Making the Business Case for the Network

1.2. The results can be used to determine which risks require special attention and further action (i.e., reduction, control, or transfer).

A cost-benefit analysis should also be performed to determine expenditure levels and payback time periods required for a viable project. Companies are under considerable pressure to do more with less, and IT budgets have suffered significant cutbacks. Many companies are maintaining profitability, not by growth but through attrition and savings. The business model has become: if last year you spent a dollar, this year spend 80 cents to do the same or more.

According to the Gartner Group [BABA02], the IT services industry is over $520 billion and steadily increasing. Technology spending is too large a percentage of most corporate budgets for CEOs and upper management to ignore. Increasingly, this is reflected by the fact that more CIOs (Chief Information Officers) have reporting relationships directly under CFOs (Chief Financial Officers). This, in turn, changes the dynamics of how IT projects are approved and increases the emphasis on more tangible and shorter ROI[5] than ever before. Required payback periods of 12 to 14 months are not uncommon.

The perceived value of an IT project's success largely depends on the financial returns realized by the organization. Careful financial analysis of proposed costs and benefits is essential to obtaining senior management buy-in throughout the network implementation life cycle. Return on investment (ROI) is a powerful, nearly universal, and well-understood metric to help justify new initiatives to demonstrate how they will make money, save money, or save time. Figure 1.2 summarizes the goal of ROI analysis. Appendix A presents a detailed case study and ROI analysis for a proposed network solution to demonstrate how ROI is used to determine payback periods. The ROI analysis of a major network infrastructure project usually includes a comparison of the available options, such as:

- Do nothing.
- Postpone project initiative.
- Outsource.
- Build a custom solution.
- Buy off-the-shelf products and integrate components.
- Combine some of the above options.

Typically, large corporate clients have an internal, core IT group to consolidate vendor contracts and to get high-volume discounts. To get instant ROI, big companies are doing more project management and are consolidating from perhaps as many as 25 to 30 down to 3 to 5 IT vendors to leverage their ability to get volume discounts. As companies experience reductions in IT staffing, they have even more incentive to consolidate vendors and to sign multi-year contracts because it is easier to manage and minimizes risk.

Although it is generally cheaper to use fewer vendors, this may also mean a loss of flexibility or opportunities to embrace new technology. Oftentimes, company headquarters will tell business units to work internally with centralized corporate buying groups. If a business unit can demonstrate a better business case with a seller or provider outside the approved vendor list, they usually will be allowed to use them. However, when it comes to problem resolution and project management, the business unit must sink or swim on its own because, in general, it will not get the same level of corporate backing as if it had used internally sanctioned vendors. The centralized IT function should retain a firm hand in overseeing vendor arrangements outside approved lists. If too many business units negotiate vendor contracts separately, the company will not be able to achieve the same high-volume discounts they could otherwise.

IT staffs are cautious about giving up the rights of ownership to too much of their organization because they do not want to outsource their own jobs. However, companies — both large and small — are looking for providers to perform services for them that are not a part of their core competencies. Web hosting, data co-location, and disaster recovery services are some of the areas companies are increasingly looking to outsource in an effort to achieve cost reductions in IT.

It can be extremely difficult to properly estimate costs and ROI, particularly when the benefits are intangible, new technologies are being used, or a new system is being implemented. For example, quality is difficult to justify in quantifiable, tangible terms, and yet it is an especially important aspect of computer and network security. For example, many companies currently using ATM[6] and Frame technology[7] are considering using the Internet for their network infrastructure, because IP/VPNs[8] can cut corporate network costs as much as 30 to 40 percent. Older Frame Relay and ATM networks are based on private, dedicated lines over which the company has complete end-to-end control. However, if the public Internet is used to transport confidential and sensitive company data, additional measures are usually needed to provide adequate protection against security breaches and loss or corruption of critical data. If companies are going to *save* 30 percent by using a VPN, they should also bear in mind that they will likely need to *spend* at least another 5 percent for additional security, such as firewalls, to ensure the quality and integrity of the network.

Depending on how company budgets are structured, security might be funded by the CSO,[9] as opposed to the CIO,[10] creating organizational difficulties when trying to get additional security expenditures approved for a new information technology initiative. To deal with these issues, it is important to demonstrate how scrimping on security to save a few thousand dollars might lead to security breaches with sizable, tangible costs. For example, if it can be shown that one security breach might cause a $50 million loss that could be prevented with a $150,000 firewall, and you are saving $2 million by switching from Frame Relay to a VPN, it should be much easier to justify the funds needed for the firewall.

Outside organizations are often used to demonstrate potential risks and vulnerabilities from hackers and insiders. Once the need for security is evident and quantifiable, it is easier to sell incremental increases in the security budget to upper management. Sometimes the perceived risk of using Internet-based networking leads the organization to reject it as an option and to keep its network infrastructure private. This might occur if business units do not want to fund additional costs to secure the network or to risk possible compromise of sensitive, confidential information. This is particularly true in risk-averse companies, such as banks and other financial institutions.

Merrill Lynch is an example of a company that uses ROI as the cornerstone of its technology planning. Merrill Lynch has over 2000 active IT projects at any one time. According to Marvin Balliet, Merrill Lynch's Chief Financial Officer for the Global Technology and Services Group, ROI is used as part of an "overall governance model" to help select and manage technology projects. Any technology initiative over $2 million requires a business case or appropriation request that has been completed according to a standard format. After a budget request is approved, a quarterly report must be prepared on the project status. This report must include information on the project budget, scope, user involvement, and an updated ROI estimate of the project value. [MCEA02]

In summary, the findings of the risk, dependency, and ROI analysis should be formalized in a written document. We recommend that the following sections be considered for inclusion in this report:

- Executive Summary
- Project Scope
- Business Issues Requiring Further Study
- Major Dependencies
  - Other Corporate Initiatives That May Affect Project
  - Skill Requirements
  - Technology Issues
  - Timeframe Requirements
- Assessment of Project Risks
  - Potential Impacts on the Business as a Whole
  - Types of Potential Risks
  - Recommended Strategies for Risk Reduction, Control, and Transfer
- Cost-Benefit Analysis
  - Quantified Tangible and Intangible Benefits
  - Impacts on Profitability
  - Impacts of Hidden Costs
  - Impacts of Tangible and Intangible Risks
  - Analysis of Procurement Options (e.g., lease or purchase)
  - ROI Analysis of Networking Alternatives
- Comparison of Alternative Solutions
  - Key Rating Factors and Relative Importance Evaluation
  - Ranked Alternatives by Weighted Factor Analysis
  - Recommended Solution(s)

1.1.3 Identify Project Requirements

At this stage in the network planning process, information is collected on what the proposed network is supposed to do. Because many technical decisions will be based on this information, it is important that the requirements analysis be as accurate as possible. This step will likely involve interviewing decision makers and staff who have a significant role in planning or using the network. It will also involve collecting information from various sources on the following:

- Estimated traffic patterns and flow
- Application programs and services to be supported by the network
- Destination and number of proposed system users
- Estimated equipment and line costs
- Network reliability requirements
- Network security requirements
- Network delay requirements

In general, it is not easy to collect the information needed to perform a complete requirements analysis. Chapter 8 discusses at length why this is so, and how the requirements affect the network design. However, the main reason the data collection is time consuming and complex relates to the fact that the data needed is often not available or is not in the form needed for analysis. Considerable effort is usually required to estimate and derive the real parameters needed to design the network.

The extent to which a company relies on outside vendors to document the project requirements largely depends on the available internal resources, staffing, and skills sets. Small and medium-sized companies usually do not have the resources to plan extensive network projects and rely more heavily upon vendors for assistance in preparing this documentation. Larger companies are better staffed and wish to maintain more control over the requirements definition process. They typically take a more proactive role in defining the project requirements before vendors are asked to present proposals. In large companies, project requirements are assessed on an ongoing basis and as part of budgetary planning.

Engaging end users in the discussion of project requirements can provide important insight into the types of applications that must be supported, as well as problems that need to be addressed. End-user discussions can also be helpful in clarifying requirement priorities. However, end-user involvement must be managed carefully so as not to encourage unrealistic expectations about the network implementation.

Requirements specification usually evolves over time with a Request for Information (RFI), Request for Quote (RFQ), and finally a Request for Proposal (RFP), from qualifying vendors.[11] Chapter 6 discusses this process in more detail.

Ultimately, the project requirements should be documented in a written report that consolidates the findings. We recommend the following sections for inclusion in this report:

- Management Summary
- Project Requirements
  - Functional Requirements
- Performance Requirements
  - Low, Normal, and Peak Usage and Capacity Requirements
  - Response Time, Delay, and Queuing Constraints
  - Availability and Uptime Requirements
  - Reliability and Transmission Accuracy Requirements
- Specialized Application and Software Requirements
- Potential Growth, Expansion, and Scalability Requirements

- Distance and Geographic Requirements
- Backup and Redundancy Requirements
  - Budgetary Constraints and Restrictions
  - Quality Assurance and Control Requirements
  - Security and Control Requirements
  - Test Plan Requirements
  - Resource Requirements
- Partial List of Supporting Documentation
  - Estimated Traffic Patterns and Flow
  - Current and Future Application Programs, and Services Supported
  - Current and Future Network Destinations and Sites
  - Current and Future Network Node Types (i.e., external, internal, suppliers, etc.)
  - Protocols Required to Support Applications and Network Services
  - Current and Future Number of Proposed System Users
  - Existing Legacy Equipment (servers, routers, etc.)
  - Switching and Gateway Requirements
  - Estimated Equipment and Line Costs
  - Number of Existing and Planned Lines and Capacity
  - Mix and Types of Data Transmitted (i.e., percent data traffic, percent voice traffic, percent video traffic, etc.)

1.1.4 Develop Project Implementation Approach

Once the business objectives, project feasibility, and major requirements have been determined, a strategy for moving forward on the network design and implementation should be developed. A number of factors must be considered when formulating the project approach. Among the most important factors are the business and technical constraints and risks. Constraints and risks heavily influence decisions on whether or not to proceed with the design using outside consulting help, or with in-house staff, or with some combination of the two.

Tactics to manage the potential project risks should be developed early on in the project, particularly if the risks are great. One method of dealing with risk is to create an implementation plan that is evolutionary, as opposed to revolutionary. This suggests a phased implementation approach that might, for example, specify how existing systems are to coexist or be transformed to operate in the new network environment. Pilot projects may be helpful in evaluating various network options and can be planned at this stage.

Business processes affected by the network implementation should also be examined and those needing refinement should be identified. Strategies for making the workflow adjustments should be addressed in the project plan. To promote awareness and support of the network, it may be necessary to incorporate educational and internal communications programs into the project plan.

Given the pace at which technology is evolving, it is important to accept change as a fact of life and to plan accordingly. This involves planning reviews at critical points throughout the network planning and implementation process to identify unforeseen problems or changes that must be accommodated by mid-course adjustments. The urge to resist "scope creep" must remain strong while making these mid-course adjustments, to prevent the project requirements from changing and burgeoning out of control.

The implementation strategy should be formalized in a written document. We recommend the following sections for this report:

- Management Summary
- Assumptions and Major Constraints
- Workflow and Organizational Impacts
- Project Approach
  - Risk Management Strategies
  - Project Staffing
  - Project Schedule
  - Transition and Deployment Plan
  - Change Control Procedures

After completing a top-down business analysis of the network plan, the organization is well positioned to begin a detailed analysis of the technical network requirements and to develop network alternatives for consideration. The chapters that follow discuss this process in detail.

1.2 Strategic Positioning Using Networks

The planning process described in the preceding sections provides the foundation to understand how relevant technologies are aligned with the business objectives. It also ensures that the organization has acceptable trade-offs between risks, costs, and benefits. This is needed to decide whether and how new technology makes sense in the organizational context.

This section presents a number of case studies to demonstrate how effective use of technology can transform markets, foster demand, and create strategic advantage. It also shows how important it is in today's environment to keep pace with technological developments, even if it does not make sense to be an industry innovator. Finally, this section presents a method for calculating potential rewards to be derived from using or developing a new technology.

1.2.1 Case Studies

Some companies are very successful being innovators and early adopters of technology. Other companies, in the same market niche, are not. Sometimes, the more successful long-term strategy is to wait until a technology matures before adopting it. It is not always easy to decide when to adopt a new technology.

Early adopters derive the benefits of new technology and sometimes the ability to capture new market share. However, they must also be ready to contend with problems of interoperability and less than perfect solutions and performance, because there are usually a lot of bugs and other issues to work out in the early releases of any new technology service or product.

Conservative adopters of technology seek to minimize risk. Conservative adopters wait until the prices and the risks of new technology go down. They watch to see what works and what the dominant trends are in the marketplace before making a commitment to the technology. Large companies have used this strategy very effectively by copying a small innovator and bringing to bear large resources to dominate and capture a market once it has started to germinate.

Late adopters of technology operate in a reactionary mode. Even when faced with massive customer defections due to their lack of innovation, they may be unwilling or unable to change. These organizations do not employ technology as a strategic weapon.

Small companies can be nimble and quick to develop new business models using innovative technology and networking infrastructures. When successful, they reap the benefits of being first to market with the new capabilities. However, if they cannot scale to meet demand, they will be unable to capitalize on the market they helped create. Large, well-capitalized organizations that know how to manage technology effectively are the best positioned to transform markets and establish industry leadership. However, as the case studies below illustrate, both large and small companies have successes and failures.

The United States military has always been a major source of technological invention. The development of the Internet is a direct result of DARPA's efforts to develop a robust computing network to ensure national security. However, the military is increasingly using commercially available network technology when it is easy to deploy and cost effective. "During the [Desert Storm] Gulf War, for example, ground commanders lacked timely satellite photos to prepare for combat because the four computer systems handling the pictures couldn't talk to one another…" [WALL95] When the United States invaded Iraq in 2003, American solders used GPS (Global Positioning System) devices with wireless hands-free radios and notebook computers to analyze digital maps made from satellite photographs. [SCHN03] The government has commissioned MCI to build a $45 million wireless phone network in Iraq based on the European GSM wireless standard. The network will have 19 cell towers servicing up to 10,000 mobile phones and will be used by reconstruction officials in Baghdad. [ASSO03] Loren Thompson, military analyst at Lexington Institute in Virginia, says that "The single most important advance that the U.S. military has made since Desert Storm has been to hugely improve the coordination of its forces… all [has] changed courtesy of the information revolution." [PUZZ03]

Federal Express (FedEx) is an industry example of a technology pioneer. FedEx's information technology infrastructure is based on a long-term strategy fostered by the company founder, Fred Smith. The core of FedEx's service is designed around sophisticated network and tracking systems. FedEx's success in implementing fast, effective tracking has been a major factor in the erosion of the United States Postal Service's (USPS) share of the very profitable overnight mail delivery market. FedEx was the first commercial express shipping and mail service to offer its customers the ability to track letters and packages using the Internet, free of charge. The USPS, UPS (United Parcel Service), and other competitors have had to make considerable investments in technology to remain competitive. FedEx's leadership role in the shipping and mailing industry is a direct reflection of its investment in and use of technology.

Wal-Mart is another renowned case study. Wal-Mart is the nation's largest private employer, with more than one million employees. [KERS03] The company started as a small discount store in the 1930s. From the beginning, the company founder, Sam Walton, realized the importance of tracking inventory, sales, and trends and required management reporting on a weekly and monthly basis. Although he was "notoriously cheap, Walton could be convinced to spend money on things that would save the company money in the long run and to allow it to grow." [BASE00] In 1977, Wal-Mart implemented its first computer network, which it used to automate the collection of sales data and to link stores to distribution centers and to headquarters. By the 1980s, it had implemented EDI[12] and the largest privately owned satellite network in the country. The satellite network was used for internal communications and for credit card authorizations, which drastically reduced customer transaction times. By the 1990s, Wal-Mart had sophisticated systems to track customer shopping habits and preferences. [ORTE00] In contrast, Kmart's first store opened in 1962, the same year as Wal-Mart. In 1963, Kmart had 53 stores, while Wal-Mart had one. However, Kmart did not gather data as quickly or as efficiently as Wal-Mart, nor did it invest as heavily in an information infrastructure. Even in the 1990s, Kmart analysts could not automatically generate reports providing a corporatewide view of supply and demand. Instead, they would feed data from multiple reports into a spreadsheet to aggregate figures. Although Kmart has made significant investments in technology over the past decade, it has not been enough to keep the company from Chapter 11 bankruptcy, which was filed in 2002 and from which it only recently emerged.

Yahoo! and Google are examples of companies that started as small, informal ventures. Today, they are both recognized as industry leaders for their technological capabilities and networking infrastructure. In 1994, two Stanford Ph.D. candidates, David Filo and Jerry Yang, devised a tool to keep track of their favorite Internet links. The popularity of their idea eventually led to Yahoo!'s incorporation and an initial public offering in 1996. Yahoo! is now the largest portal on the Web. Yahoo! also offers a variety of online enterprise services, including Corporate Yahoo!, a customized enterprise portal toolkit for "audio and video streaming, store hosting and management, and Web site services." [YAHO03] Google was incorporated in 1998 by Sergey Brin and Larry Page, also students at Stanford University. Google is now the world's largest search engine, with an index of more than three billion Web pages, and handles over 200 million search queries a day. Yahoo! directs search requests from its site to Google. Google has based its business model on two revenue streams: search services and advertising programs. [GOOG03] Various analysts estimate that Google had revenues in excess of $1 billion in 2003 and in 2004, it became a publicly held company.

Microsoft is a premier example of a company that is very strategic in choosing when to be first to market and when to be second. Microsoft created its monopoly position by a strategic legal and business alliance with IBM to sell personal computers with its operating system. This allowed the Windows operating system to become a *de facto* industry standard, even if IBM personal computers did not. When UUNet approached Bill Gates in 1995 for funding, he was quick to recognize the huge potential of the Internet as a vehicle to promote worldwide demand for personal computers. Microsoft acquired a 15 percent equity position in the then-private UUNet, and paid "for the deployment of 40,000 modems on the network, the largest such project on the Internet at the time. The software giant also became a banker for UUNet, lending the company almost $40 million at favorable interest rates." [CHAN97] Microsoft also funded UUNet's expansion into Europe. Today, UUNet is the largest Internet provider in the world, and the global market for personal computers running Windows operating systems is legendary.

Microsoft has solidified its market position by steadily augmenting the functionality of its operating system. In 1995, during the early days of the World Wide Web, Netscape was the leading Internet browser, with over an 80 percent market share. The same year, Microsoft introduced Internet Explorer as part of Windows 95. Microsoft made slow gains by steadily surpassing Netscape's functionality and eroding its market share. Things reached a head in 2002 when Netscape announced major layoffs and restructuring and its parent company, America Online (AOL), initiated an antitrust lawsuit against Microsoft. Finally, in May 2003, Microsoft and AOL announced a $750 million settlement, in which AOL will continue distributing Microsoft's Internet Explorer with its online service but will not have to pay royalties to Microsoft for a period of seven years. There is widespread industry speculation that this agreement will seal Netscape's fate and reflects a lack of commitment to Netscape on the part of its parent company. At the time of this writing, Netscape has about 5 percent market share, while Internet Explorer has almost 95 percent.

Microsoft and AOL announced as part of their settlement that they will work together to improve the interoperability of their instant messaging (IM) products. It will be interesting to watch this scenario unfold. AOL has about 100 million registered home users. [SAUN03] AOL's Instant Messenger™ provides a real-time, text-based chat capability that only AOL subscribers can use. It is in AOL's best interests to keep its instant messaging system proprietary as long as possible, because it is a leading reason why customers prefer AOL's paid service. According to Genelle Hung, analyst with Radicati Group, "IM is the killer application. There is no other feature that keeps people coming back [for AOL]." [NEWY03]

Because AOL's legacy offering is based on a dial-up Internet connection, it is not suited to bandwidth-intensive applications such as video. In contrast, Microsoft's MSN Windows Messenger is based on the IETF standard, Session Initiation Protocol (SIP),[13] and comes bundled as part of Windows XP. This protocol provides the capability of supporting APIs and real-time multimedia applications. It, too, is a free service to consumers and is supported by Microsoft's MSN network. Microsoft claims to have over 100 million users of its IM service. [MICR03a]

AOL is faced with a serious threat to its market as consumers migrate to other, lower cost narrowband options and to broadband DSL and cable modems, which are up to 100 times faster than dial-up modem connections. DSL dominates the global broadband market and represents about 62 percent of the broadband modems sold in 2002. Currently, about 27 percent of all U.S. home Internet connections are broadband; and by 2008, this figure is projected to grow to about 60 percent. In Europe, about 7.5 percent of all household Internet connections are broadband. [GREEN03] AOL is offering the RoadRunner service — based on an all-optical broadband IP data network — to allow it to compete in the broadband market. [AOL03]

In the corporate arena, there are over 30 players in the instant messaging (IM) market. [GREY02] Enterprise IM (EIM) products provide security and network management capabilities (with message logging, archiving, and monitoring, etc.) not found in consumer IM products. However, they are not free[14] and provide a significant revenue opportunity for vendors. Key players to watch include:

- AOL's Enterprise AIM services
- IBM's Sametime
- Yahoo's Messenger Enterprise Edition
- Microsoft's MSN Windows Messenger

Currently, IBM's Sametime is the dominant player in the enterprise IM market, controlling over 70 percent of the market. [KEIZ03] AOL's AIM can be accessed by Lotus Notes' Sametime through a contact list that is kept and accessed separately. AOL and IBM have announced plans to improve the interoperability of their respective proprietary products. According to Gartner Group, IBM has a limited window of opportunity to grow this market before Microsoft captures market share with its enterprise IM product — Microsoft Real-Time Communications Server 2003 Standard Edition (a.k.a. "Greenwich"). [KEIZ03]

As a condition of approving AOL's merger with Time Warner, the FCC requires AOL to open its IM network to competitors if it launches advanced high-speed IM services. [HU03] This was a condition for which Microsoft lobbied vigorously. AOL is currently petitioning the FCC to try to remove this restriction and to allow it to pursue its proprietary, closed approach to high bandwidth IM.

Microsoft views both consumer and enterprise instant messaging as an extension of its overall product architecture. Like EIM and Sametime, Microsoft's RTC IM strategy is based on IETF (SIP) standards and offers such state-of-the-art capabilities as photographic file sharing, audio conversations, Voice-over-IP telephone calls, e-mail, application sharing, and co-browsing. *Co-browsing* allows customer service personnel, for example, to interact directly with a customer's Web browser. Using this capability, a customer service representative might demonstrate order entry functions or answer questions directly on the customer's screen. *Collaborative browsing* integrates IM chats, e-mail, fax, telephone, and Internet phone contact in a single interaction. This capability is fully integrated and plug-and-play with the Windows XP operating system and Microsoft applications (e.g., Outlook, Word, PowerPoint, Excel, Project, etc.). Summing up, Microsoft has devised a multi-pronged strategy to make its Windows platform ever more compelling, fully integrated, and functional in supporting end-user voice, video, chat, e-mail, and software applications, thereby ensuring that it will remain a dominant player in the market. In the view expressed by Microsoft's Chief Executive, Steven Ballmer, hardware is becoming a commodity but software is not. Microsoft's strategy is to deliver powerful "Integrated Innovation" to simplify the automation of business tasks. [LOHR03B]

Lands' End (landsend.com) is another company that has made strategic use of technology and, in so doing, has transformed the business model for the clothing industry. From the beginning, Lands' End has been a direct marketing catalog company and, until its recent acquisition by Sears, did not sell clothing in stores. Lands' End works directly with mills, manufacturers, and customers. Customers now have the option of shopping by phone, mail, fax, the Web, or in Sears stores. Since Lands' End launched its Web site in 1995, it has introduced a number of industry innovations, including: [LANDS03b]

- *My Virtual Model*™. This is a tool that allows customers to create a three-dimensional model of their bodies. This model can be used to "try on" clothes that are offered on the Web site.
- *My Personal Shopper*. Customers are asked to enter data about their clothing preferences. This data is used, in turn, to allow a "personal shopper" to suggest items and outfits.
- *Lands' End Custom*™. After customers supply their measurements and information on their body type, computer-operated cutting machines are used to make custom tailored and fitted clothes.

Today, landsend.com sells more clothing than any other Web site in the world. Until Lands' End proved the contrary, the "common" wisdom was that the clothing industry was not likely to achieve success on the Internet because shoppers would want to touch, feel, and try on clothes before making purchases. Lands' End's well-designed Web site makes it easy to display merchandise, receive suggestions, and request fabric samples. Strategic use of technology enabled Lands' End to effectively counter barriers to entry in the E-commerce market.

Looking at Web-based retailing on the whole, the year 2002 was the first time Web-based retailers made a profit, on $76 billion in sales. Among the most profitable were Web merchants, like Lands' End, with preexisting catalog operations, with profits of about 22 percent. As a group, online-only retailers had losses averaging about 16 percent. The key to profitability for many online companies is to control shipping and customer service costs. The former can be addressed by contract negotiations and better shipping strategies, while the latter can be addressed using online tracking and e-mail notification to reduce customer calls. “Whereas the heralded ‘first movers’ of consumer E-commerce captured Wall Street’s fleeting attention, the E-tailers still in business have captured something of more lasting value: the expertise that accompanies experience and the time to take advantage of it.” [TEDE03] According to Shop.org, an online retailers’ association, the biggest online sales growth in 2002 was in health and beauty (93 percent), apparel (54 percent), and flowers, cards, and gifts (>50 percent).

The effects of the Internet have become so pervasive that even if companies or organizations choose not to have a presence on the Web, they can be profoundly impacted by it, for good or bad. For example, in 2002, Intuit released TurboTax with anti-piracy controls, which greatly upset many customers who expressed their displeasure on Internet forums. Intuit responded to the vehement outcries by agreeing to discuss potential product changes online before implementing them in the future. The movie “My Big Fat Greek Wedding” benefited from early favorable reviews posted on Web sites, which helped compensate for its small advertising budget. [THOM03]

New Internet shopping paradigms are also shaping marketing, customer loyalty, and advertising programs. Reflecting the rising influence of informed online shoppers, Amazon.com has eliminated its entire advertising budget for television and print. Instead, it is offering customers free shipping on qualifying orders. To make their Web sites less intrusive and annoying, some “E-tailers” are converting to behavior-based advertising. Instead of asking personal questions, they monitor where site visitors click. Based on inferred visitor preferences, screen content and ads are modified accordingly. The *Wall Street Journal Online* and the *New York Times* are examples of companies currently using behavior-based advertising on their Web sites. [IVES03]

1.2.2 Calculation of Technology’s Strategic Value

Calculating the possible gains from technology in tangible financial terms is an imprecise and challenging task. It involves careful consideration of the following:

- How does your product or service relate to the target markets you wish to serve?
- Among the buyers of your product or service, what is the mix that will embrace innovation and change? What percentage of each are early adopters, conservative adopters, and late adopters?

- What types of innovation are you proposing — product or process innovation?
- What is the time horizon for implementing the new technology — near term, a year, or longer?
- What barriers, if any, exist to keep your rivals from adopting a similar strategy to compete?
  - Pricing
  - Cost to convert from existing to new technology
  - Similarity of features or functions between existing and new technology
  - Regulatory requirements
  - Availability of technology
- What is the size of your company and experience with technology?

The answers to the above questions can be used as input to a discounted cash flow model to determine the potential value of a new technology to the enterprise. Discounted cash flow can be computed in a number of ways. The Adoption-Diffusion Model, developed by the Department of Agriculture, is a well-documented method, with the following steps:

1. Estimate profits to be gained by using the new technology in the initial stages. This may come from incremental revenue, return on capital, or cost reductions.
2. Forecast the time period over which the product or service will be commoditized as competitors and conservative and late adopters enter the market to drive down prices. The Adoption-Diffusion Model is based on the premise that the mix of early, conservative, and late adopters will affect the timing and mix of customer buying. The proportion of each buyer type and the time before they will enter the market as buyers should be estimated.
3. Compute expected decreases in profit flows as the product or service becomes a commodity.
4. Calculate the total discounted cash flow based on the forecasted life cycle of the product, service, or project. This calculation incorporates the projected revenue streams for each buyer type (i.e., early, conservative, and late adopters).

In short, there are many ways a network can enhance an organization's competitiveness. Networks can be used to offer new services and capabilities, streamline operations, enhance image and visibility, increase productivity and reduce costs, and improve customer service. Organizations with creativity and insight have produced networks that offer dramatic advantages over competitors that are not as effective in their use of technology. The race to adopt new network technology continues to quicken as more and more organizations extend their reach and influence through the use of global networks. Organizations, large or small, cannot remain complacent in their use of technology if they are to remain competitive in today's environment.

1.3 Dealing with Major Design Challenges

Increasingly, a company's ability to adapt to changing technological, market, legislative, economic, social, and homeland security conditions rests squarely on its IT and networking infrastructure. Network design, by its very nature, has always been complex and multifaceted, posing many organizational and technical challenges. However, these challenges continue to escalate as companies are forced to do more with less and to react in shorter and shorter timeframes. IT budgets for staffing and capital expenditures have been hit hard in recent years. To keep costs down and maintain corporate profitability, many companies are postponing routine network maintenance and upgrades. It is a fact of life that companies no longer invest in technology for the sake of technology — immediate business returns and tangible results are needed to induce corporate IT investment. The proliferation of new technologies — especially public Internet technologies — and the impetus to change must be carefully weighed against the benefits and risks.

The following sections discuss the major issues facing corporations as they plan their technology infrastructure. Common sense and good management principles should dictate the strategies for meeting these challenges.

1.3.1 Organizational Concerns and Recommendations

1.3.1.1 Senior Management Involvement and Support

A recent survey by CIO Insight of 500 chief executive officers revealed the following: [ZIFF03]

- 73 percent say their companies are highly innovative
- 65 percent agree the economy is slowing technology adoption
- 41 percent of technologies under evaluation are adopted
- 53 percent involve business executives in technology adoption
- 40 percent say the primary goal in adopting technologies is cost cutting

These findings reflect the importance of having senior management that is in tune with the overall business environment and capable of thinking strategically about where the company needs to be in the marketplace. CIOs are faced with significant challenges because there are substantial risks (both personally and to the corporation) in leading technology initiatives to transform old ways of doing business. The ability to successfully lead these initiatives requires an entrepreneurial spirit and a thorough understanding of the market and the company's operation. Senior management must also be able to clearly communicate business objectives so that bottom-line requirements can be factored into the planning and execution of the network strategy. Senior management plays a vital role in ensuring that a process is in place to make this happen.

CIOs and senior management help translate organizational goals into an actionable IT strategy and provide a focal point for responsibility and accountability within the organization. This encompasses a number of dimensions, including:

- Implementing a corporatewide planning process that engages senior management in strategic decision making
- Aligning IT plans with organizational goals
- Instituting capital planning and investment analysis of IT initiatives
- Formulating and implementing a strategic IT architecture
- Ensuring effective IT infrastructure and staffing is in place to meet organizational objectives
- Ongoing measurement and oversight of IT ROI and contribution to overall business performance

In summary, it is increasingly vital to overall corporate success to have senior management with the vision, technical competence, and skill sets to effectively manage and deploy complex network technologies in a dynamic and quickly changing environment. Senior management has a pervasive effect on organizational culture, and serves as an invaluable role model to encourage integrity, ethics, leadership, and innovation.

1.3.1.2 Recruiting, Training, and Maintaining Skilled Staff

The organization should strive to hire, train, and retain skilled managers and staff who understand technology and how it can be used to satisfy organizational objectives. This is not easy, given the highly competitive job market for network specialists and the rapid proliferation of new networking technologies.

Technology for technology's sake is no longer an appropriate organizational goal. However, some employees may push to implement a new technology because it is perceived as a better path for personal growth than other, perhaps more appropriate but older or mundane options. Conversely, there may be a need to adopt new technologies that current staff members are reluctant to embrace because they are resistant to change. Dealing with these matters presents a challenge to technical managers, particularly at a time when companies are cutting training budgets and holding the line on salary increases.

This type of dilemma is fairly common. For example, Voice-over-IP (VoIP) is emerging as a new way to consolidate both voice and data traffic over the same network, because the cost of doing so is very competitive. Traditionally, corporate PBX networks have been operated by "voice" staff who are very familiar with trouble tickets and resolution of QoS (Quality of Service) issues. With the migration to VoIP, MIS organizations must train "voice" staff on IP fundamentals. "Data" staff must also be trained to take voice trouble tickets on data networks, which is something they are not accustomed to doing. Packet delivery with Frame Relay, ATM, or TCP/IP protocols is judged on such metrics as packet loss and MTTR. With voice transmission, the ear picks up jitter — much like wow and flutter on a tape deck — if there are problems with packet delay. However, these problems are very difficult to trace in a traditional data network. It is likely that voice MIS staff will start reporting to the data MIS staff once voice traffic starts to go over the Internet. The end result is that initially this will result in a mismatch of skill sets, which will require retraining and organizational realignment. The rapid pace of new technology is likely to have significant, ongoing impacts on the organization and its structure.

Some strategies for dealing with training and staff retention include:

- Work with Human Resources to develop methods for hiring and retaining good staff.
- Where necessary, augment existing staff with consultants and vendor support.
- Encourage cross-disciplinary training and project efforts to foster depth of knowledge and application within the organization. This will avoid islands of staff expertise in specialized areas that are not easily generalized. Cross-fertilization also helps employees see the big picture and how technology relates to the business objectives.
- Use training and internal communication to reduce the fears of those affected by new technology projects.
- Encourage and offer ongoing education to help staff remain current with new trends in technology.
- A voluminous amount of technical information is available from a variety of sources such as vendor/telco/consultant presentations,

conferences, technical books (such as this text!), industry magazines, and the Internet. Turn to these sources on a regular basis to help keep up with new developments in the industry.

1.3.1.3 Effective Program and Project Management

One of the more common reasons technology initiatives fail is poor project management. Therefore, it is imperative that the organization develop internal standards, methods, and procedures to promote effective planning and project management. There should also be a well-publicized organizational commitment to do things the "right" way, which means adhering to standardized processes and procedures even when there are substantial pressures to take risky shortcuts.

A well-defined management review process for allocating staff and capital resources to technology innovation projects is an essential aspect of project management. This will likely involve regular project and capital review meetings with senior management to obtain their buy-in and support of IT initiatives.

Once a project has started, reporting mechanisms should be in place to track progress against milestones, budget allocations, and projected ROI. Projects that achieve targeted outcomes should receive continued funding and management sponsorship. Projects that are failing should be cut short.

During the planning process, potentially serious political and organizational issues should also be identified. For example, some people may feel threatened if they believe a proposed network or technology initiative will compromise their power, influence, or the nature of their job. Consequently, they may attempt to hinder the project's progress. The organization must confront these fears and develop strategies for dealing with them.

1.3.2 Technology Concerns and Recommendations

1.3.2.1 Keeping Abreast of New Developments

The organization does not operate in a vacuum and must be attuned to changes going on around it. For example, there may be legislative, economic, or social pressures that mandate changes in the way the company does business. This, in turn, may have a profound impact on company strategy and technology adoption. Keeping abreast of new developments and relating them to organizational requirements is a formidable task, and it is rare that an organization will have all the expertise in-house it needs to do this well.

Often, consultants and outside vendors are needed to help plan and implement the network. It is much easier to manage the activities of the consultants if the organization has a firm grip on the business objectives and requirements. However, sometimes consultants are needed to help develop and specify the business objectives and requirements. Although outside consultants offer benefits such as expertise and objectivity, they also present their own set of challenges. For example, it is important to develop a "technology transfer" plan when working with outside consultants, to make sure that in-house staff can carry on as needed after the consultant leaves.

Throughout the 1970s and 1980s, if an organization wanted a network, it could call IBM and IBM would design that network. It was a common adage that "the only risk is not buying IBM." However, for the foreseeable future, there will be increasing numbers of network vendors in the marketplace, and a decreasing likelihood that any one vendor will satisfy all the organization's network requirements. Although often unavoidable, using multiple vendors can pose problems, particularly when there are problems with the network implementation and each vendor is pointing a finger at the other. Because it is increasingly likely that a particular network vendor will provide only part of the network solution, it is incumbent upon the network design team to make sure that the *overall* network requirements are addressed.

It is important to maintain ongoing awareness of new product offerings from service providers that provide differentiated, value-added services. This can be accomplished by implementing an ongoing RFI, RFQ, and RFP process. This involves regular interaction with key service providers and vendors. It is also a good way to guarantee that the organization is getting the best deals possible on products and services.

1.3.2.2 Maintaining a Secure Networking Environment

With the growing reliance on public infrastructures and Internet access, and the threat of disasters and terrorist activities, there is a heightened awareness for the need to implement security safeguards to protect sensitive company data. Many companies have responded by creating Chief Security Officer (CSO) positions to ensure corporatewide oversight of all aspects of security. Government has taken a stronger stance with the enactment of the Federal Information Security Management Act (FISMA). FISMA mandates the creation of CSO positions within U.S. federal agencies to oversee all security policies and practices. [USDE03]

Typically, CSO responsibilities include:

- Identifying security goals and objectives consistent with corporate strategy
- Overseeing the protection of tangible assets, intellectual property, computer systems, networking infrastructure, and people

- Managing security policy, standards, guidelines, and procedures to ensure ongoing security maintenance
- Establishing relationships with local, state, government, and federal law enforcement agencies, as appropriate
- Overseeing investigation of security breaches and organizational response to ensure appropriate disciplinary, legal, and corrective actions

Some organizations require or prefer security managers who are CISSP certified. CISSP certification involves passing an examination that covers the following areas: [(ISC)^2]

- Access Control Systems and Methodology
- Applications and Systems Development
- Business Continuity Planning
- Cryptography
- Law, Investigation and Ethics
- Operations Security
- Physical Security
- Security Architecture and Models
- Security Management Practices
- Telecommunications, Network and Internet Security

CISSP recertification is required every three years, along with ongoing continuing professional education (CPE) credits. Certification is limited to individuals who have a minimum of three (with a college degree) or four (without a college degree) years of active experience in one of the ten security domains listed above.

There are always new ways to compromise network security. It is an ongoing process to stay on top of the potential vulnerabilities to which the company is exposed and to maintain proper vigilance. A good security plan is multifaceted and includes both low- and high-tech defenses. Processes and procedures must also be in place to ensure compliance with security requirements. For example, Microsoft NT and XP come with many built-in security features; however, they are not activated when the operating systems are installed. It is incumbent upon the security administrator to enforce the enabling and use of security capabilities provided by the network.

Employees must do their part to safeguard and protect all company resources. For example, some people who use IM and wireless networking technologies are not aware of the potential security risk they pose. Employees have been known to use an AOL IM chat to communicate sensitive data to other employees without realizing that the data is being sent in pure, unencrypted ASCII text — a format that can fairly easily be read by unauthorized hackers. For example, Stifel Nicolaus, a brokerage firm in St. Louis, made headlines when it was discovered that its institutional brokers had been using AOL Instant Messenger clients, which were deployed without permission. The Director of IT encountered stiff opposition to an outright ban on the practice, so he was forced to quickly deploy a gateway from IMLogic to manage, log, and archive IM messages. [FONT02]

Hackers have also been known to eavesdrop on unsecured, unencrypted Internet communications over a wireless network. This is fairly easy to do using hot spot sniffers[15] — such as KISMET, NetStumbler, DStumbler, and Wellenreiter. Employees must take network security threats very seriously and should be provided with the tools to secure their computing environment. Many companies have adopted strict policies and have instituted employee awareness programs to guard against these types of potential security leaks.

Many corporations rely on some form of outside verification and validation of their IT and networking infrastructure. This helps to sidestep political and internal pressures to circumvent security when there is also considerable pressure to implement new systems and networking quickly and cheaply.

The goal of network designers should be to seamlessly integrate security services between different network environments and technologies. To support employee demand for IM chats, for example, might mean implementing enterprise IM software. In the case of wireless networking, employees should be given PKI encryption or products such as Citrix Solutions for Workforce Mobility. If this is not feasible, the organization might need to provide (albeit slow) WAN connections and dial-up links for "road-warrior" employees to ensure the necessary degree of security in their communications. As suggested by these examples, the network environment and types of required access have significant impacts on the security approach the organization should employ.

A number of standards organizations are developing recommendations to help industry and government implement best practices with respect to security. The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS). It "is a partnership between the public and private sectors. This program is being implemented to help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace." [CCEV04] The CCEVS defines open, publicly available standards for "*Protection Profiles*" and *"Security Targets."* Protection Profiles specify consumer security requirements for a wide range of applications (i.e., E-commerce, etc.) and products (i.e., firewalls, etc.). "*Security Targets* are the security objectives of a specific product or system, known as the Target of Evaluation (TOE). The Target can conform to one or more Protection Profiles as part of its evaluation. A TOE is assessed using the Common Evaluation Methodology and assigned an Evaluation Assurance Level (EAL)." [NORT02] Seven EAL levels have been defined:

- *EAL-1:* relates a product's performance and conformance with published documentation and specifications.
- *EAL-2:* relates to an evaluation of a product's design, history, and testing.
- *EAL-3:* relates to an independent evaluation and verification of a product that is still in design phase to assess its potential vulnerabilities, environment controls, and configuration management.
- *EAL-4:* relates to a very in-depth evaluation of the target design and implementation.
- *EALs 5-7:* relate to even stricter levels of evaluation to assess the Target's ability to withstand attacks and misuse. They are used to critique products used in high-risk environments. In the United States, these evaluation levels can only be performed by the National Security Agency (NSA) for the U.S. Government.

The ISSA (Information Systems Security Association) is a nonprofit group of more than 100 volunteers and vertical industry representatives, including EDS, Dell Computer Corporation, Forrester Research Inc., Symantec and Washington Mutual, and others. ISSA's main goals are to "ensure the confidentiality, integrity and availability of information resources." [ISSA03] ISSA organizes international conferences, local chapter meetings, and seminars to promote awareness of security issues and to provide a worldwide forum for discussion. It supports a Web page for information dissemination to ISSA members.

ISSA has also announced that it is working on the completion of Generally Accepted Information Security Principles (GAISP). GAISP focuses on operational recommendations based on three sets of principles:

1. *Pervasive Principles,* which are designed for governance and executive-level management to help them develop an effective information security strategy.
2. *Broad Functional Principles,* which define "recommended tactics from a management perspective" based on the ISO 17799 security architecture.

3. *Detailed Principles,* which are still in progress. They are intended to provide very detailed recommendations on the "way to do everything from securing a firewall to physical security. For the first time, instead of having to meet an abstract goal, professionals will get rationales, examples, cross-references and detailed how-to instructions." [SCHW03]

The ISO 17799 standard has also been developed to help define an information security program. It provides a comprehensive checklist of security requirements and precautions, from which organizations can pick and choose what makes the most sense given their needs and particular situations. The ISO standard addresses the following: [WALS03]

- *Security policy.* This spells out an organization's expectations and commitment to security.
- *Security organization.* This defines the security management structure, responsibilities, and security breach response process.
- *Asset classification and control.* This provides a detailed accounting and inventory of the IT infrastructure and corresponding security requirements.
- *Personnel security.* This includes written security requirements and guidelines, employee background checks, and signed agreements to protect intellectual property and other company assets.
- *Physical and environmental security.* This deals with backup, recovery, and security as it relates to the IT networking infrastructure, physical facilities, and people.
- *Communications and operations management.* This addresses prevention and detection of security breaches.
- *Access control.* This involves establishing processes and procedures to properly restrict user access according to their security clearance.
- *Systems development and maintenance.* This establishes a development process that incorporates security considerations throughout the system life cycle.
- *Business continuity management.* This creates contingency plans to recover from catastrophic failures and disasters.
- *Compliance.* This ensures that all regulatory and legal requirements are met.

CASPR (Commonly Accepted Security Practices and Regulations) is another organization that offers advice and recommendations on security processes and procedures through the free dissemination of white papers and other security-related documents on its Web site. [CASP03]

The IT Governance Institute and the Information Systems Audit and Control Foundation sponsors the Control Objectives for Information and Related Technology (COBIT) project and is another source of advice for implementing security policies, processes, and procedures. The COBIT project is supervised by a Project Steering Committee comprised of "international representatives from industry, academia, government and the security and control profession." [CoBIT03] This organization offers free information downloads or, for a modest fee, one can purchase print and CD-ROM versions of its standards. These standards and recommendations are intended to be broadly applicable worlwide to "management, users, and IS audit, control and security practitioners." [CoBIT03] For example, the COBIT *Management Guidelines* discusses Maturity Models ("to help determine the stages and expectation levels of control and compare them against industry norms"), Critical Success Factors, Key Goal Indicators, and Key Performance Indicators. The complete set of standards also includes: [CoBIT03]

- *Executive Summary.* This summarizes key security concepts for senior management.
- *Framework.* This explains how to control delivery of IT information through 34 high-level control objectives. It also relates key evaluation criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability) to the IT process.
- *Control Objectives.* This provides a basis for policy development by implementing 318 specific, detailed control objectives throughout 34 defined IT processes.
- *Audit Guidelines (ISACA members only).* This suggests activities to support 34 high-level IT control objectives and elucidates risks if the control objectives are not met.
- *Implementation Tool Set.* This provides case studies and presentations to help implement COBIT standards.

1.3.2.3 Managing Complexity

Perhaps the foremost challenge is the sheer multiplicity of options that must be considered when designing a network. Added to this is the fact that networks of today continue to grow in size, scope, and complexity. On top of this, the networking options available are in a constant state of flux. Change is the only constant in the world of high technology.

The key to managing complexity is to simplify wherever possible. Some of the major tactics that companies are using to reduce complexity in their networking infrastructure include:

- *Select protocols and equipment based on ease of use and manageability.* Many network and system products are not designed for easy management and control, and are difficult to install, upgrade, configure, or monitor. The difficulty only increases as equipment, protocol, and software incompatibilities are encountered. Unless there is a compelling reason to do otherwise, industry standard protocols and uniform implementations should be considered. Otherwise, it can be very difficult to manage the inevitable evolution that the network infrastructure will undergo to support new requirements and technologies.
- *Use plug-and-play components wherever possible.* The intent is to minimize the time and money spent customizing hardware and software to support the organizational requirements. Commodity components may reduce risk and improve performance and reliability over a custom solution.
- *Transition from proprietary to open standards.* This provides the organization with more options in future technology migrations. An example of where this is happening on a significant scale is the migration from legacy SNA networks to TCP/IP (this is discussed in more detail later in Chapter 2). It is important to pick the right open standard(s) because there is no guarantee that an open standard will catch on in the market and be supported in the future by a majority of vendors/providers, particularly if a new, improved open standard supplants it. It is also important to make sure that the quality, functionality, and robustness needed by the organization are supported by the standard. Open tools — such as GNU Emacs, a text and code editor — are very widely used. Others — such as IBM's Eclipse Platform for building integrated development environments (IDEs) — are supported by hundreds of tool vendors and provide robust development capabilities.
- *Use client/server and object-oriented application development methodologies to promote code reusability and modularity.* This allows thorough testing and customization, as appropriate, of subcomponents.
- *Integrate voice, data, and video on single IP platform.* An example of this is migration from separate PBX and data networks to a single VoIP data network to handle both voice and data traffic. Companies are using this approach to cut costs and to reduce the number of protocols and equipment that must be supported.
- *Automate data center and network management tasks.* Fortune 200 companies are increasingly looking at data center automation tools to reduce IT staffing costs and to improve efficiencies. An example of this is Opsware, Inc., a leading provider of data automation

software. Opsware is designed to support cross-platform data center environments and a variety of management functions on servers and applications. This includes system provisioning, application provisioning, change and configuration management, asset and license tracking, patch installation, disaster recovery, and security updates. It consists of two major components: (1) Automation Platform, which provides a centralized mechanism to encapsulate business logic for managing a distributed infrastructure and its associated applications; and (2) Intelligent Software Modules (ISMs), which are specific products to manage provisioning, deployment, configuration, and modification of servers and software designed to work with standard equipment, and database and application software. [OPSW03]

- *Utilize middleware to provide network and application control based on predefined business rules.* Middleware supports a broad range of application-specific, information-exchange, and network management functions. Middleware can be used to automate business operations by integrating front-end and back-end applications. For example, middleware can be used to allow the coexistence of new Web-based applications and legacy SNA. It is also used in E-commerce to link payment, accounting, and shipping systems with Internet-based, customer front-end applications. Middleware can also be used for server load balancing, network performance monitoring, and network recovery actions.

1.4 Similarities and Differences between Voice and Data Network Design and Planning

Traditionally, there have been clear distinctions and choices between voice and data networks. Selection of one or the other was determined by the type of traffic carried, cost and performance characteristics, and the types of equipment and services that could be supported by each type of network. However, since the 1990s and beyond, the distinctions between voice and data networks are increasingly clouded, as a variety of integrated voice and data alternatives have become available. New carrier, service, and technology options continue to proliferate. These options support not only voice and data, but also an increasingly diverse array of such applications as color facsimile, video conferencing and surveillance, high-definition television distribution, and LAN-to-LAN and MAN-to-MAN connectivity.

It is easy for an organization to install a "plain vanilla" voice network. To hook up to the public switched telephone network (PSTN), one has