REPORT # 02-09

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

A BEST PRACTICES REVIEW

Managing Local Government Computer Systems

APRIL 2002

Photo Credits:

The cover and summary photographs and those on pages 10, 15, 28, 37, 51, and 56 were taken by Office of the Legislative Auditor staff. The picture on page 48 is a photo image from the © Corel Corporation 1997.

Preface

This report is a best practices review of managing local government computer systems, looking at Minnesota counties, cities, and school districts. It is the eighth in a series of best practices reviews conducted by the Office of the Legislative Auditor. The 1994 Legislature established best practices reviews as a means of identifying effective and efficient practices in delivering local government services. The intent was to help local governments improve the delivery of services by learning about successful practices in use by similar jurisdictions elsewhere.

In May 2001, the Legislative Audit Commission directed our office to study best practices in managing local computer systems and providing local e-government services, based on a recommendation by the Local Government Advisory Council, which was established to recommend topics. Our report on local e-government is being released as a separate document.

We acknowledge and appreciate the help provided by many local government officials involved with planning and maintaining computer systems. Their expertise represented a substantial contribution to this report. The Office of Technology in Minnesota's Department of Administration also provided assistance.

The report was researched and written by Jody Hauer (project manager), Jan Sandberg, Kathryn Olson, Carrie Meyerhoff, and Leah Goldstein Moses. This report and related material are available over the World Wide Web at www.auditor.leg.state.mn.us/ped/2002/pe0209.htm.

St. Paul, Minnesota
April 30, 2002

Table of Contents

		Page
	SUMMARY	**ix**
	INTRODUCTION	**1**
1.	**BACKGROUND ON COMPUTER SYSTEMS**	**3**
	Computer System Overview	3
	Computer System Complexity	10
2.	**ASSESSING OPTIONS FOR MANAGING COMPUTER SYSTEMS**	**13**
	Management Options	14
	Preparing to Evaluate Management Options	33
3.	**BEST PRACTICES FOR MANAGING COMPUTER SYSTEMS**	**43**
	Best Practices and Actions	43
	A Framework Should Be in Place to Guide the Management of a Computer System	44
	Knowledgeable Staff Should Maintain and Use the Computer System	49
	Computer Systems Should Be Secure	53
	APPENDICES	
	A: Study Methodology	61
	B: Glossary	71
	FURTHER READING	**77**
	RECENT PROGRAM EVALUATIONS	**Back Cover**

List of Tables and Figures

Tables — Page

1.1 Computer System Components 4
1.2 Typical Hardware Components of Personal Computers 5
1.3 Typical Network Components 7
1.4 Examples of Three Computer Systems 11

2.1 Services Provided Through County Computer Collaborations, 2001 17
2.2 Services Provided by Local Government Information Systems (LOGIS) 18
2.3 Services Available Through Region 1-ESV 21
2.4 Intergovernmental Collaborations Used for Computer System Upkeep, by Type and Size of Local Government, 2001 23
2.5 Computer Vendors Used for Computer System Upkeep, by Type and Size of Local Government, 2001 27
2.6 In-House Staff Used for Computer System Upkeep, by Type and Size of Local Government, 2001 31
2.7 Actions for Preparing to Assess Management Options 34
2.8 Items for Which Total Costs Should Be Estimated 36
2.9 Practices for Good Contract Management 39

3.1 Best Practices for Managing Computer Systems 44
3.2 Sample Hardware Inventory 45
3.3 Key Management Program Components 47
3.4 User Support Strategies 52
3.5 Elements of a Computer Use Policy 55
3.6 Elements in a Password Policy 55
3.7 Activities in Developing a Disaster Recovery Plan 59

Figures

1.1 Local Governments Using Personal Computers or Workstations, 2001 6
1.2 Local Governments Using Minicomputers or Mainframes, 2001 6
1.3 Local Governments With Networked Personal Computers or Workstations, 2001 8
1.4 Local Governments With File Servers, 2001 12

2.1 TIES Member School Districts and Geographic Areas Served by Regional Management Information Centers, 2001 20
2.2 Local Governments Using Intergovernmental Collaborations to Maintain Computer Systems, 2001 22
2.3 Local Governments Using Vendors to Maintain Computer Systems, 2001 26
2.4 Local Governments Using In-House Staff to Maintain Computer Systems, 2001 30

Summary

Local governments may manage their computer systems in-house, by outside vendors, by an intergovernmental computer collaboration, or by a combination of these three approaches. This report recommends that counties, cities, and school districts adopt certain best practices as they consider how they want to manage their computer systems.

Local governments should evaluate how well each option for managing computers addresses security, staffing, and control policies.

Recommended Best Practices:

- Before deciding how to manage their computer systems, local governments should make sure that: information technology has the support of top officials, staff have the capacity to estimate total costs and manage contracts, jurisdictions identify the services that should be automated, staff plan for computer system replacements, and jurisdictions know where information technology fits within their organizations (pp. 34-40).

- Local governments should judge a management option based on whether it has complete inventories of equipment, sets standards for computer hardware and software, follows a clearly documented program to control the day-to-day operations of the computer system, communicates computer system policies and procedures to people using the system, and monitors compliance with the policies (pp. 44-48).

- Local governments should also ensure that the computer systems are managed by staff who have sufficient expertise, receive ongoing training, and provide training and support to computer users (pp. 49-52).

- Finally, local governments should look for management options that use trained professionals to assess the computer system's security risks, develop security policies based on the risks, manage user accounts and employee access to the system, install and monitor firewalls and antivirus software, develop backup procedures and disaster recovery plans, and test security procedures (pp. 53-60).

In addition to these recommendations, the review found that:

- All of Minnesota's counties, school districts, and large cities use personal computers and have computer networks, but 27 percent of cities with 500 or fewer residents do not use any personal computers (pp. 5, 8).

- Nearly all of Minnesota's local governments use their own staff to manage some part of their computer systems, but most also rely on computer vendors or intergovernmental computer collaborations to maintain parts of their hardware or to support software applications (p. 33).

Report Summary:

Most local governments already have computer systems in place.

The core elements of a computer system are its hardware, software, and data, but to be complete, a computer system also needs the staff, facilities, and a management program to support the core. While most local governments have computer systems in place, the systems' complexity varies. Most counties, school districts, and large cities have computer networks, but just 11 percent of cities with populations under 500 have networked computers and 27 percent reported having no personal computers at all.

Local governments' options for managing their computer systems are to rely on their own staff, join an intergovernmental computer collaboration, work with computer vendors, or use a mix of these options.

Minnesota Local Governments Use a Variety of Options to Manage Their Computer Systems

An intergovernmental computer collaboration is a group of local governments cooperating on common technology objectives and governed by a joint powers agreement. All Minnesota counties belong to one or more of three computer collaborations designed to meet certain data processing needs unique to counties, such as computing property taxes. One city-oriented computer collaboration exists and offers a range of automated services from business licensing to utility billing. School districts may receive technology services from collaborations known as "service cooperatives" and regional management information centers, which exist around the state.

Most local governments use their own staff to maintain some portion of their computer systems' daily operations.

Based on a fall 2001 survey of local governments, counties and school districts were more likely than cities to report using computer collaborations to manage at least some of their computer systems. The computer collaborations provide local governments with specialized technological expertise, staff networking opportunities, chances to avoid purchasing certain equipment or software, and a degree of control over the design of customized software applications. At the same time, local governments that use collaborations have to spend more time and effort to plan and work with other members of the group, and they need to be aware that relying on a third party for their core technology services holds some risks. Plus, there is a loss of individual control inherent with group decision making.

By contrast, computer vendors are private firms that sell or coordinate hardware, software, management expertise, and support for networks and computers. Forty percent of cities, compared with 22 percent of counties and 14 percent of school districts, reported using computer vendors for most or all of their computer systems' updating, security, and daily operations. Computer vendors offer local governments specialized expertise and opportunities to avoid hiring their own staff or purchasing certain equipment or software. On the other hand, local governments that work with vendors need to follow careful contract management practices and be aware of the risks involved with relying on a third party for technology services. Further, they may have little control over pricing, schedules, and service features.

Most local governments use their own staff to manage at least some of the daily operations of their computer systems. About 84 percent of counties, 71 percent of cities, and 86 percent of school districts reported that their own staff perform most or all of their computer systems' upkeep. Using their own staff to manage computer systems

gives local governments a high degree of control over the services but carries the costs of employing highly skilled personnel.

Most of Minnesota's local governments use a mix of options to manage their computer systems. About three-quarters of the local governments surveyed, including most counties and school districts, reported using two or three management options to maintain their computer systems. About one-quarter, mostly small and medium-sized cities, reported using a single option to maintain computer systems, and that option was most often a jurisdiction's own staff.

Local Governments Should Prepare to Evaluate Options for Managing Computer Systems

Before local governments decide which options work best for their computer systems, they should prepare themselves to evaluate the options. Preparation means, first, that the local governments' top officials should understand and support the role of information technology in getting the governments' work done. Second, local governments should determine where technology staff best fit within their jurisdiction's organization. Third, they should be prepared to fully estimate computer systems' costs, which requires estimates of total costs over the life cycle of equipment as well as the hiring, compensation, and ongoing training costs for staff. They also need the capacity to set spending priorities among competing technology projects.

Evaluating management options for computer systems is complex and requires preparation.

Fourth, because managing computer systems often involves working with external providers, local governments should be prepared to follow appropriate contract management practices and assess providers' financial stability. Fifth, local governments should determine what services need to be automated because only the technology that clearly supports their programs and data should be used. Sixth, because technology evolves rapidly, and to avoid fragmented computer systems, local governments need to follow planned computer replacement programs. Finally, local governments should be prepared to assess management options within the context of their own unique demographic, financial, and political characteristics. For example, jurisdictions in some rural areas of the state may have limited opportunities to hire appropriately trained technology staff, forcing them to consider other options.

Local Governments Should Follow Best Practices in Evaluating Management Options

The report identifies three best practices that are important when evaluating options for managing computer systems. It recommends that, regardless of which options are under consideration, local governments use the best practices to help judge the options' effectiveness.

1. A Framework Should Be in Place to Guide the Management of a Computer System

Good asset management requires use of an up-to-date inventory of computer system equipment that describes hardware and equipment configurations. Local governments should ensure that whoever manages their computer system maintains complete inventories. Those who maintain computer systems should follow documented management programs with clear and specific procedures for daily operations and control of the system. They need to communicate technology policies and procedures to the jurisdictions' staff who use computers, and they should monitor adherence to the policies.

Periodically, the policies and procedures need to be updated.

***Example**: The city of **Fergus Falls** developed policies to communicate acceptable computer uses to city staff. Developed jointly by managers and staff, the policy covers various procedures, including security measures that forbid the reproduction of software and require users to change passwords every 90 days. All employees who use the computer system must sign a statement indicating that they have read the policy. The city's information systems staff supplement the written guidelines with activities such as using inventory software to track which software applications reside on the computer network.*

2. Knowledgeable Staff Should Maintain and Use the Computer System

In determining who should manage computer systems, local governments should look for options with properly trained staff who bring a high level of expertise to operating the computer system. Local governments should determine that a process is in place to recruit and retain technology staff. They need assurances that technology staff receive ongoing training to keep their skills current in a world of rapidly changing technologies. Similarly, they need to determine that whoever manages the computer system has an adequate plan for user training and will provide user support to local government staff expected to work with computers.

Local governments should ensure that their computer system managers control security risks.

***Example:** In the **Robbinsdale Area School District,** the technology and media services department offers financial incentives to keep their staffs' technology skills up-to-date. Employee contracts contain provisions for certification stipends, which are awarded whenever staff successfully complete training programs as part of their approved training plans. The district also pays registration fees for technology-related courses that staff attend.*

3. Computer Systems Should Be Secure

Local governments should look for computer system managers who understand and can control security risks. In assessing their options, local governments should seek computer managers who conduct risk assessments of the systems' security and base security policies on the identified risks. Computer managers should limit users' access to certain computers and data and actively manage users' password accounts. They need to install and monitor "firewalls" and antivirus software, have procedures in place to backup data, and develop a disaster-recovery plan. Because security risks change over time as new vulnerabilities arise, computer system managers should monitor and periodically audit their security procedures. Whoever manages the computer system must have staff who are appropriately trained to protect it.

***Example: Anoka County** contracted for an extensive assessment of its computer system, with one component focusing on security. Among other tests, the assessment included "penetration" testing whereby consultants tried to circumvent security controls to gain access to the computer system. Following the assessment, information systems staff developed a plan to systematically implement specific recommendations, such as formally documenting procedures for data backups.*

Introduction

In Minnesota, counties, school districts, and most cities use computer systems to collect information, generate reports, and help provide services to citizens. Local governments have several options to manage their computer systems, ranging from in-house staff, to computer vendors, to groups of local governments that jointly manage certain data processing needs.

Because the range of computer systems in local government is broad, this report is written for a fairly broad audience. Although most local governments already have computer systems in place, this report explains the best practices necessary for effectively managing those systems. Local governments with very complex computer systems face additional considerations that go beyond the scope of this report; for these jurisdictions, the best practices identified in the study are still relevant, but they are not an exhaustive list. The report is also intended to help local government managers and information technology directors understand differences among the options for managing computer systems, as well as the circumstances under which each option is beneficial. It does not provide technical detail about what local governments' computer systems should look like. Nor does the report rank the existing management options. Each local government has to decide for itself how best to manage its computer systems, based on criteria such as those suggested herein.

In May 2001, the Legislative Audit Commission directed our office to study how local governments manage their computer systems and what factors influence those decisions. The study addresses these research questions:

- **What infrastructure is necessary to support local government computer systems?**

- **What are the options used by Minnesota local governments to manage their computer systems? What services does each option provide?**

- **What are the advantages and disadvantages for local governments to either (a) manage their own computer systems, (b) join collaborations to provide the services, or (c) use outside vendors?**

- **What best practices lead to efficient and effective management of computer systems?**

In answering these questions we reviewed literature and Web sites that describe practices necessary for the effective and efficient use of computer systems. We interviewed local government officials as well as staff from computer vendors and intergovernmental computer collaborations. During the course of the study, we consulted with a technical advisory panel of local officials involved with

computer systems in their own jurisdictions. More information on the methodology of the study is available in Appendix A.

This report has three chapters. Chapter 1 provides basic background information on the components of computer systems and some differences among computer systems in Minnesota's local governments. Chapter 2 describes the options for managing computer systems and their advantages and disadvantages. The chapter also explains how local governments should prepare to evaluate the management options. In Chapter 3, we explain best practices that local governments should consider when evaluating computer management options. This chapter also offers examples of local governments using the best practices.

At the same time this study was underway, we researched best practices in how local governments provide information and services on-line, known as e-government. Although these two studies covered some similar ground, each was distinct enough to warrant a separate report. The report on e-government is available on-line at www.auditor.leg.state.mn.us/ped/2002/pe0208.htm.

1 Background on Computer Systems

SUMMARY

Computer systems consist of hardware, software, and data, which need to be supported by staff, facilities, and management programs. Although most local governments use personal computers, counties are more likely than cities or school districts to use mainframe computers or minicomputers. About 27 percent of cities with populations under 500 do not have personal computers. Counties, school districts, and large cities typically have more complex computer systems than medium and small cities.

Because the complexity of local government computer systems varies, this chapter begins by defining the major components of computer systems for readers who may not be familiar with them. Experienced computer users, however, may wish to bypass this basic information. This chapter also describes some differences and similarities we found in the computer systems used by Minnesota's counties, cities, and school districts. In the chapter we ask:

- **What does a computer system include? What infrastructure is necessary to support computer systems, however complex they may be?**

To answer the questions we reviewed national literature and Web sites from organizations that focus on computer system management. We also surveyed Minnesota local governments in the fall of 2001 for basic information on their computer systems. Information about our survey methodology is in Appendix A. Aggregate results of the survey are available on-line at www.auditor.leg.state.mn.us/ped/2002/pe0209.htm.

COMPUTER SYSTEM OVERVIEW

Although early government computer systems were typically large computers isolated from most staff, information technology (IT) now comprises much more than large, stand-alone computers. Today, many local government staff use personal computers to perform a range of functions. Software applications designed to work together can link citizens to services and provide information across departments. Recent studies suggest that gains in worker productivity

during the last decade are in part due to IT, more so as organizations change how they do business to take advantage of available technologies.[1]

For the purpose of this study, we defined computer systems broadly:

- **Computer systems consist of a core of hardware, software, and data and the infrastructure necessary to support that core.**

Computer support requires staff, facilities, and a maintenance program.

As shown in Table 1.1, the **core system** includes:

- All **computer equipment or hardware**, such as desktop computers and network and telecommunications equipment;
- **Software**, including application programs (to process payroll, for instance) and operating systems software (to control a computer's central processing); and
- **Data** and information that are used and stored within the computer system.

Table 1.1: Computer System Components

Core
- Computer hardware and equipment
- Software
- Data

Support
- Staff
- Facilities
- Program for managing the computer system

SOURCE: Office of the Legislative Auditor.

The **support infrastructure** includes:

- **Staff** that manage and use the equipment;
- **Facilities** to house both equipment and staff; and
- A **comprehensive program** for managing computer systems, including procedures for planning, maintaining, and monitoring the system and providing security.

1 McKinsey Global Institute, B. Solow *et al.*, *US Productivity Growth 1995-2000: Understanding the Contribution of Information Technology Relative to Other Factors* (Washington, D.C.: October 2001); www.mckinsey.com/knowledge/mgi/reports/pdfs/productivity/IT_implications_10_12_last.pdf; accessed January 15, 2002.

Core System

Computer Hardware

Perhaps the most visible part of the computer system is its equipment or hardware, including mainframe computers, minicomputers, personal computers, computer workstations, and computer networks. Mainframe computers are large relative to other types of computers and have the massive memory and processing power needed for very large, complex business applications. Minicomputers are mid-range machines, physically smaller than mainframes and with less power, but substantially more powerful than other computers. Individual personal computers, often referred to as "PCs," are the most easily recognized computer. Table 1.2 lists the typical hardware components of PCs. Computer workstations are similar to PCs but typically have additional computing power or storage for specialized applications.

Table 1.2: Typical Hardware Components of Personal Computers

- Central processing unit (CPU)
- Primary storage, usually a hard disk drive
- Secondary storage, such as a floppy disk drive, zip drive, or rewritable CD
- Input devices, such as the keyboard or mouse
- Output devices, such as the printer or video display
- Communications devices, such as a modem or network connection

SOURCE: Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Organization and Technology in the Networked Enterprise 6th ed.* (NJ: Prentice Hall, 2000), 163.

According to our survey:

- **With the exception of about 27 percent of small cities, nearly all local governments in Minnesota use at least one personal computer or computer workstation.**

In a few cities, staff use their own computers for city work.

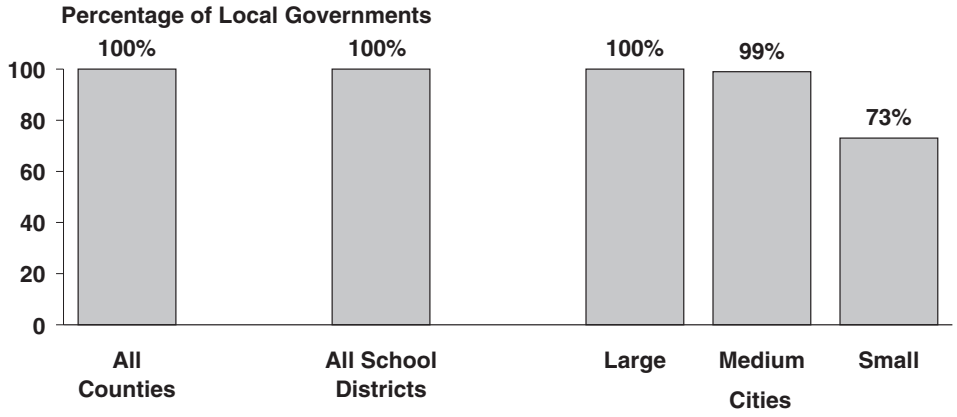
As shown in Figure 1.1, virtually all counties, school districts, and medium to large cities have personal computers or workstations, according to our 2001 survey. However, 27 percent of cities with fewer than 500 residents reported that they did not have any personal computers. Twelve small cities reported that while the city owned no computers, for some city business, staff used computers they owned themselves.

The use of PCs sharply contrasts with the use of minicomputers and mainframe computers. Figure 1.2 shows that:

- **Counties were far more likely than school districts or cities to report using minicomputers and mainframe computers.**

For the most part, only small cities reported having no computers for use in city operations.

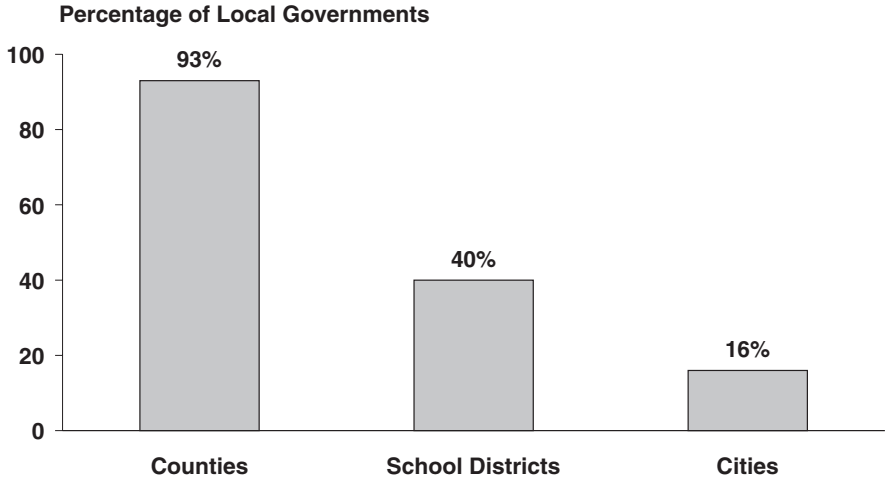
Figure 1.1: Local Governments Using Personal Computers or Workstations, 2001



NOTES: The question read: "Which of the following best describes the computers currently used in your [jurisdiction]?" A "large" city has a population of 5,000 or greater, a "medium" city has a population between 500 and 4,999, and a "small" city has a population under 500.

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Figure 1.2: Local Governments Using Minicomputers or Mainframes, 2001



NOTE: The question read: "Which of the following best describes the computers currently used in your [jurisdiction]?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

County use of mainframes or minicomputers was higher than that reported for school districts of any size and much higher than that for cities, even among large cities.

Computer Networks

A network is a collection of compatible hardware and software arranged to communicate information (text, graphics, voice, or video) from one computer to others or to peripheral equipment such as printers. Among other purposes, computer networks are used to increase communications and share data files or equipment such as scanners.

Networks vary in complexity. Simple networks may link several PCs and a printer. More sophisticated "client/server" computing is widely used to (1) distribute the task of inputting data to various "client" software and computers and (2) centralize data storage and processing in one or more "server" computers, managed by the server software.[2]

A network can serve a few computers in a room, dozens of computers in a building, or several different governmental units crossing several counties.[3] Table 1.3 lists typical components of a network. Local-area networks or LANs are limited in range to a few thousand feet (although fiber optic cables are expanding the range). Wide-area networks or WANs connect multiple sites or computer networks at high speed across a broad geographic area using switched and dedicated lines (wire, cable, or fiber), microwave, or satellite communications. As the complexity of a computer network increases, so do its support costs, as is discussed at the end of this chapter.

Table 1.3: Typical Network Components

- Cabling or wireless equipment to link computers with other devices
- File servers to store and process data (and possibly manage the network)
- Network interface cards (special adapters that connect computers to the network cable)
- Routers to direct packets of data through the network
- Gateways (usually communications processors to connect to public computer networks)
- Network operating system software that routes and manages communication on the network and coordinates network resources
- Security hardware and software, such as firewalls

SOURCE: Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Organization and Technology in the Networked Enterprise 6th ed.* (NJ: Prentice Hall, 2000), 270-71, 511.

2 Servers may be powerful personal computers with large hard-disk capacity, minicomputers, mainframe computers, or specialized computers designed specifically as servers. They share resources, such as files and printers, with other computers on a network.

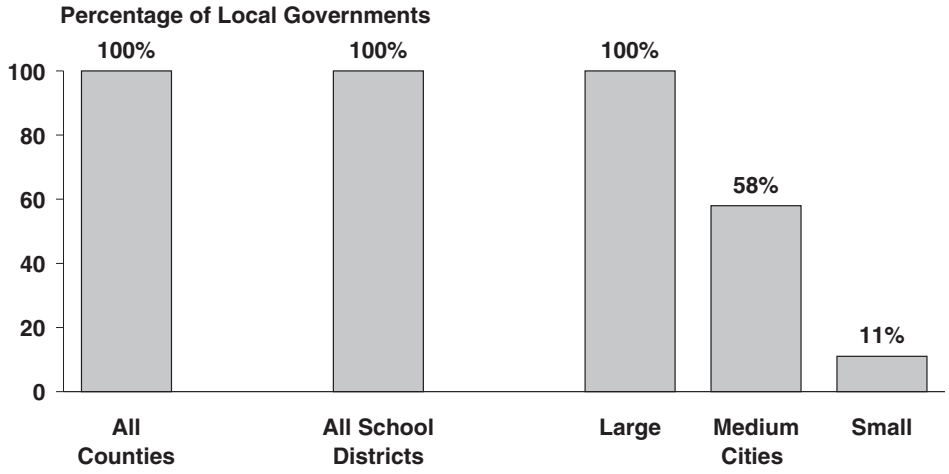
3 In addition, by using Internet networking standards, local governments may create private internal networks called "intranets" that are useful for sharing information among staff in a single government unit. See: Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Organization and Technology in the Networked Enterprise 6th ed.* (NJ: Prentice Hall, 2000), 298.

As shown in Figure 1.3,

- **All counties, school districts, and large cities reported that their personal computers were partially or fully networked, compared with 58 percent of medium-sized cities and 11 percent of small cities.**

Small cities tend to have less complex computer systems than do other local governments.

Figure 1.3: Local Governments With Networked Personal Computers or Workstations, 2001



NOTES: The question read: "Which of the following best describes the computers currently used in your [jurisdiction]?" A "large" city has a population of 5,000 or greater, a "medium" city has a population between 500 and 4,999, and a "small" city has a population under 500.

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Telecommunications Equipment

Telecommunications systems contain computers and additional technology equipment needed for electronic transmission of data, voice, or video between and among computer networks. Within telecommunications systems, communication channels, such as those provided via cable, telephone wire, fiber optics, or satellite, provide the means to transmit data. Using telecommunications infrastructure, computer users connect to the Internet and communicate with other computer networks around the globe.[4]

Software

Software is a set of detailed instructions that controls the operation of a computer. "Operating system" software manages the computer resources, such as the central processing unit (or CPU).[5] Users are often unaware of the system software because it works in the background. In contrast, "application" software provides tools to complete specific tasks, such as word processing. Unlike system

4 The Internet is a worldwide system of computer networks interconnected for communications.

5 Laudon, *Management Information Systems*, 194-195.

software, most users are familiar with the application software that allows them, for instance, to compose a letter or create a map. Some specialized software, known as systems development software, allows programmers to develop their own application programs.

Most local governments with computers use application software to provide common functions, such as processing financial data. Beyond that, some applications are unique to specific functions of cities, counties, or school districts. Unless a local jurisdiction develops its own application, it usually pays yearly license fees to use software, with fees commonly based on the number of users.

Data

Governments collect and produce a large amount of information, and they face many decisions about their electronic data: what information to collect; what information to keep; how to preserve what is kept; whether the data are private or confidential (implying that access to them must be restricted); whether data should be shared and with whom; how the data will be retrieved; what level of protection is needed; and where to locate data. Answers to these questions vary and will affect computer management decisions. For example, storage of health records may require more secure computer management procedures than e-mail records because they involve a higher level of confidentiality.

Support Infrastructure

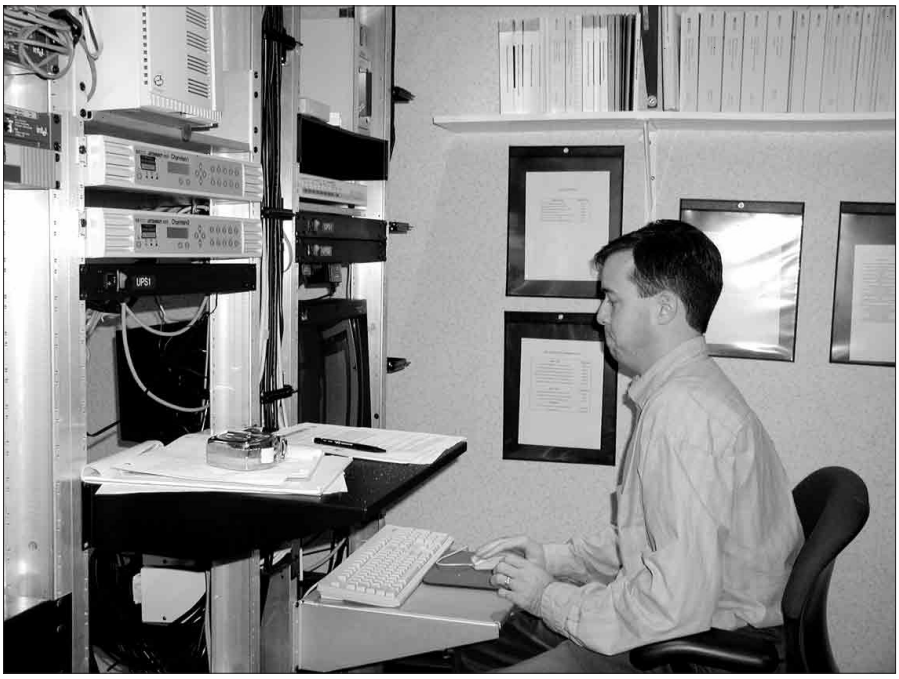
Computer System Staff

Computer system staff operate hardware and software, train and support users, and plan for system management. Many functions, such as high-level network design and operation, require advanced training. In some cases, specially trained staff may focus on specific functions such as computer security or network administration. In other cases, such as in small local governments, one person may perform many computer-related tasks. In yet other cases, staff with special expertise from outside a local government may manage the jurisdiction's computer system or part of it.

Facilities

Secure facilities can help protect computer systems.

The facilities that house computer equipment are an important part of the system. Most computer hardware is valuable, easily damaged, and sensitive to temperature and humidity levels, making the facilities that house computers an important part of protecting technology investments. Similarly, appropriate facilities can help prevent data and software from being inadvertently changed or destroyed. When remodeling or constructing buildings, the computer network needs are an important part of the planning. If technology considerations are not planned up front, the facilities may not support the computer network's cabling or other infrastructure needs, or the facilities may need to be changed later at additional cost.


Highly trained staff are needed to support computer systems.

Computer-System Management Program

The ongoing maintenance of a computer system should be detailed in a management program.

Operating and maintaining a computer system may be complicated. A computer system-management program brings together policies and procedures for the implementation, operation, maintenance, and ongoing control of the computer system.[6]

A management program typically addresses the components discussed in this chapter—hardware, software, data, and facilities, as well as support for system users. It also includes security measures to protect the computer system. The management program might include software that automates certain procedures, such as requiring password changes. How the program looks will depend upon the local government's size, technical capabilities, budget, staff resources, and the degree to which the government relies on technology.[7] Computer management programs are more fully described in Chapter 3.

COMPUTER SYSTEM COMPLEXITY

Although all computer systems have core components of hardware, software, and data, and all need infrastructure to support that core, the systems vary in complexity. The complexity of a computer system is a function of the system's hardware configuration, software programs, and the local government's data

6 Gartner Research, "Guidelines for the Content of IT Policies," *Research Note* TU-13-9550, July 26 2001, 1-2.

7 Right Track Associates, Inc., "IT Management Strategies in Small Business," *ITToolkit;* www.ittoolkit.com; accessed January 17, 2002.

requirements. For instance, hardware configurations range from a single stand-alone computer to multiple computer networks connecting hundreds of desktop computers and several computer servers housed at multiple locations.

Computer systems around the state vary in complexity.

Computer systems that connect users across many buildings scattered over a broad geographic area require more sophisticated hardware and have more demanding support needs than less complex systems. Table 1.4 illustrates three systems in Minnesota of differing complexity. For some local governments, a computer "system" may actually consist of multiple discrete computer systems that serve different government programs and that may not "talk" to one another or share data.

As mentioned earlier, counties, school districts, and large cities have computer systems that are fully or partially networked, but computer networks are far less common in small cities. Another indication of computer system differences is the use of file servers (computers that share files, printers, and other resources with other computers on a network). More complex computer systems have

Table 1.4: Examples of Three Computer Systems

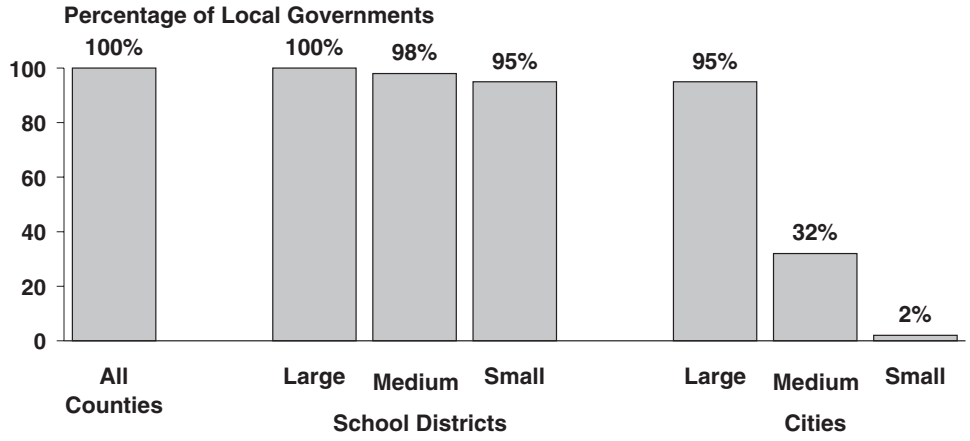
City of Mantorville	Swift County	Anoka County
Mantorville has one computer and two printers; one printer is used for faxing and scanning. A single staff person uses a software package purchased from a vendor in Texas (from whom the city also purchased the computer), which covers most of the city's computing needs. All remaining computing is done using word processing and spreadsheet programs or the software that came with the computer. Staff and elected officials use the single computer but also receive e-mail at home regarding city business.	In Swift County, each office is responsible for its own hardware and software purchases and maintenance. There is no centralized inventory or standards for purchasing computer equipment. An internal network connects several file servers and a number of personal computers. In addition, the county contracts with a vendor who provides the software applications and user support for six county programs (property tax calculations, fixed assets, vital statistics, payroll, finances, and library systems). For these applications, county staff connect to computers housed at the vendor's work site. The vendor maintains and protects the databases.	Anoka County employs 54 IT staff to provide operations, maintenance, development, and user support for over 1,800 PCs, a large number of servers, a minicomputer, and a mainframe computer. A wide area network connects more than a dozen county work sites to a central network. County staff developed and continue to support several large applications including the property tax program. While the county has also purchased several software applications, in most cases county IT staff provide user support. IT services are centralized in one countywide IT department and are organized into four sections: infrastructure, applications services, PC systems tech services, and help desk, which also includes imaging and records management.

SOURCE: Office of the Legislative Auditor.

networks with file servers that centralize data storage and processing. As shown in Figure 1.4,

- **Minnesota counties, school districts, and large cities are more likely to use file servers than medium or small cities.**

Figure 1.4: Local Governments With File Servers, 2001



NOTES: The question read: "Which of the following best describes the computers currently used in your [jurisdiction]?" A "large" school district has 3,000 or more students, a "medium" district has between 800 and 2,999 students, and a "small" districts has fewer than 800 students. A "large" city has a population of 5,000 or greater, a "medium" city has a population between 500 and 4,999, and a "small" city has a population under 500.

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

According to our survey, all counties, nearly all school districts, and most cities with populations over 5,000 reported using file servers. In contrast, less than one-third of medium-sized cities and almost no small cities reported using them. Further, as described earlier, many small cities have no computers at all, with about 27 percent of small cities reporting that they have no computers.

2 Assessing Options for Managing Computer Systems

SUMMARY

While nearly all of Minnesota's local governments use in-house staff to manage some part of their computer systems, most also rely on computer vendors or intergovernmental computer collaborations to maintain hardware, manage network operations, or support various applications. Each management option has its own advantages and disadvantages. Before deciding among options for managing computer systems, local governments should assess their readiness to make this decision. Readiness includes understanding and supporting the role of information technology, knowing where technology staff fit within the organization, having the capacity to estimate full costs and manage contracts, identifying services that need automation, and planning for computer replacements.

This chapter describes options for managing computer systems and the advantages and disadvantages of each. It also discusses the need for preparedness to evaluate these options.

In this chapter we address the following questions:

- **What are the advantages and disadvantages for local governments of different sizes to either (a) manage their own computer systems, (b) join with other jurisdictions to provide the services, or (c) use outside vendors? What services does each option offer?**

- **What is needed to prepare to assess differences among computer management options?**

To answer these questions, we relied on information collected while interviewing several computer vendors, all county and city computer collaborations, and several school district collaborations. We also interviewed certain local government staff in charge of their jurisdiction's computer system. We reviewed Minnesota Statutes; documents from the Department of Children, Families, and Learning; information from several private and government organizations; and literature specific to computer management options. Finally, we gathered information about local government arrangements for updating, securing, and operating computer systems in our survey of counties, cities, and school districts.

We attempted to compare the costs of the management options for specific services but were unable to do so for several reasons. In many cases it was difficult to identify the costs for the services used by a local government. Costs varied by type of service or product, and they were often buried in individual program budgets. Local government staff frequently performed a variety of

services including some technology-oriented ones, but their time could not be easily allocated to computer management functions. Although costs for joining a collaboration or using a vendor were generally known, it was difficult to identify related costs, such as the administrative cost of managing the vendor contract or entering data. Also, the fees that vendors and collaborations charge differ by type of service and from jurisdiction to jurisdiction. Without good information about the true cost of various services, it was not possible to accurately compare the cost-effectiveness of options for managing computer systems.

MANAGEMENT OPTIONS

Local governments can manage their computer system services in several ways. They have four options: rely on in-house staff, join an intergovernmental computer collaboration, work with computer vendors, or use a mix of these options.

Computer systems can be managed by in-house staff, computer vendors, intergovernmental computer collaborations, or a mix of these options.

While most local governments rely on their own staff for managing some parts of their computer systems, many have turned to computer vendors and intergovernmental computer collaborations for specific computer services. For instance, most counties have joined computer collaborations for data processing related to property tax computations.[1] The following sections describe intergovernmental computer collaborations and computer vendors in Minnesota and the services they provide. As a point of comparison, we also discuss how local governments rely on in-house staff for computer services. We focused on three broad types of services: (1) set-up, repair, and user support for personal computers; (2) network support, including operations, security, and maintenance; and (3) application support including user support and assistance with specialized reports or data. We did not include purchases of computer equipment or other hardware in this analysis.

Intergovernmental Computer Collaborations

In this report, an intergovernmental computer collaboration is a group of local governments that is governed by a joint powers agreement and shares certain technology objectives, allowing members to jointly use certain technology services, such as a computer application for financial accounting. Collaborations have legal standing to hire staff, enter into contracts, and provide services for their members, and boards of directors elected by the membership govern them. Membership may be a requirement to receive services, or nonmembers may purchase some services on a fee basis.

Not all collaborations offer the same services; even within a single collaboration, not all members use each service. We found that:

1 There are exceptions, generally for large jurisdictions that initially developed an application years ago and continue to support it. For example, Anoka County developed its own property tax application on its mainframe computer and has no immediate plans to discontinue its use.

- **Services offered by computer collaborations vary, and individual members typically have the opportunity to select only those services that meet their own needs. But all computer collaborations offer support or equipment for common functions, such as financial services software or computer network management.**

Beyond the collaborations discussed in this study, it is common for local governments to participate in technology-related partnerships, some for long periods of time and others for brief, one-time functions. For instance, a city may have an agreement with a school district to share computer servers for hosting their Web sites. While such arrangements may be beneficial, they are not the focus of this report. Nor are other collaborative groups, such as the Western Area City County Cooperative (WACCO), a joint powers arrangement of 16 cities and 9 counties in the western half of Minnesota. Although its primary functions are not related to information technology (IT), WACCO provides workshops and discussions for those who share technology interests. Similarly, the Minnesota Counties IT Directors Group, which historically included only the largest counties but more recently has begun including smaller counties with similar IT concerns, shares information on technology, vendors, and state initiatives. While useful to their members, such groups are not the focus of this study.

Computer collaborations offer technology services needed by numerous local government members.

County Collaborations

All counties are members of one or more computer collaborations.

All Minnesota counties choose to use services from one or more of three computer collaborations. The collaborations developed independently to serve their member counties' computing needs, many of which are driven by state statutes and rules. Because many of the state's requirements are subject to frequent legislative changes that require modifying related computer applications, counties have found efficiencies by joining collaborations to compute and report these data. One of the most common functions offered by these collaborations is the software and support for property tax computations, which is a large and complicated application requiring annual modifications due to statutory changes.

The Minnesota Counties Computer Cooperative (MCCC) is a joint powers organization founded in 1975. MCCC currently employs three staff and serves all counties in some capacity. MCCC contracts with vendors for development and support of its applications, which range from payroll to court-services tracking. Members may subscribe to any of several applications, and they provide oversight and guidance by participating in user groups organized around each application.

The Minnesota Counties Information Systems (MCIS) is a joint powers organization with 13 member counties and 11 staff. While MCIS maintains a minicomputer in-house for developing applications, all member counties now have their own hardware in-house.[2] MCIS develops some applications in-house and contracts for others through vendors. Four user groups provide input to MCIS to guide application development.

All three county collaborations support property tax processing.

The MidState Computer Cooperative is a joint powers organization that currently includes 20 western Minnesota counties, largely agricultural in nature and of similar size. The collaboration itself has no employees. Instead, each member contracts individually with Computer Professionals Unlimited, a vendor that provides a variety of computer services. Computer Professionals Unlimited coordinates five user groups. With two exceptions, all member counties process data on their own computers. Under separate contracts, Swift and Big Stone counties use one of Computer Professional Unlimited's three minicomputers located off county premises.

Members of all three collaborations receive software applications and support for property tax calculations. Table 2.1 lists services offered by the Minnesota Counties Computer Cooperative and Minnesota Counties Information Systems and includes services offered to members of the MidState Computer Cooperative through Computer Professionals Unlimited.

All three groups make at least some use of software developed and supported by vendors. Some of the software they use is specific to Minnesota, such as the Integrated Financial System application designed for auditors and human services agencies in counties. Each collaboration also offers special services. For example, Minnesota Counties Information Systems offers its County Recorder Indexing System to 11 nonmember counties, 13 North Dakota counties, and 1 Florida county.

City Collaborations

Compared with counties and school districts, cities face fewer requirements to provide data to state agencies or to connect to state agency databases. This may partially explain why fewer computer collaborations exist for cities in Minnesota. The Local Government Information Systems (LOGIS) consortium is the only joint powers organization for computer management that primarily serves cities. However, any Minnesota unit of government may join LOGIS. Founded in 1972, LOGIS members now include 26 cities and several agencies, located mainly in the Twin Cities metropolitan area.

---

2 Chippewa and Lac Qui Parle counties share a computer.

Table 2.1: Services Provided Through County Computer Collaborations, 2001

Service	Minnesota Counties Computer Cooperative	Minnesota Counties Information Systems	MidState Computer Cooperative[1]
PC Support	No direct service, but a formal Information Services Support Group meets	Yes, also for AS/400 minicomputers	Yes[2]
Network Support	No direct service, there is a formal Information Services Support Group	Yes	Yes[2]
Applications			
Property Taxes/ Mass Appraisal	Yes	Yes	Yes
Finance	Yes	Yes	Yes
Human Resources/ Payroll	Yes	Yes	Yes
Other Applications	Cash Register and Receipts System Fixed Assets Treasurer's Financial System Law Enforcement Corrections Community Health Motor Vehicle Registration DNR Off-Road Vehicle Registration	Miscellaneous Receipts Highway Cost Accounting County Recorder Indexing System (also used by counties outside Minnesota)	Highway Cost Accounting Grantor/Grantee Fixed Assets Treasurers' Financial System Motor Vehicle Registration
Fees	Flat fee for full members, associate member fee is based on number of applications used	Flat fee is based on number of services used; for property tax, a percentage of the fee is based on county size	Flat fee
User Groups	Six—Tax/CAMA, Finance/General Government, Community Health Services, Law Enforcement, Corrections, Information Services	Four—Assessor, Auditor/Treasurer, AS/400 Network, Payroll/Financial	Five—Property Tax, Finance, Payroll, Highway, Welfare
Host Data for Counties	Counties use their own computers	Two counties share a computer; other counties use their own, but MCIS has the capacity to support county operations in case of an emergency	Most counties use their own computers; two counties use a computer housed at the vendor's site
Provide Internet Access	No	No	No
Web Site	www.mnccc.org/home/	www.mcis.cog.mn.us/	http://morris.state.mn.us/cpui.htm
Newsletter	Yes	Yes	No
User Support	Provided by application vendor	Provided by MCIS staff and application vendor	Provided by Computer Professionals Unlimited staff and application vendor
User Training	Yes	Yes	Yes

NOTES: Some computer applications have additional optional modules. Most applications were developed by vendors. Collaborations work with vendors to direct modifications.

[1]Services offered to county members of MidState Computer Cooperative are provided by the vendor Computer Professionals Unlimited.

[2]Services are available through a vendor separate from Computer Professionals Unlimited but related to it.

SOURCE: Office of the Legislative Auditor.

Computer collaborations offer some services that are specific to county, city, or school district functions.

As shown in Table 2.2, LOGIS offers a wide range of services including data management for city services (such as utility billing), as well as Internet service, e-mail, and technical assistance for local area networks. The number of member cities subscribing to each service varies. Some of the services are similar to those offered by county collaborations, such as the financial and human resource and payroll applications. Other services, such as software applications for permits and inspections, are specific to city functions.

School District Collaborations

School districts may join and obtain technology services from one or more computer collaborations, including service cooperatives and regional management

Table 2.2: Services Provided by Local Government Information Systems (LOGIS)

PC Support: Yes

Network Support: Yes

Applications (listed alphabetically):

- Business License and Code Enforcement
- Human Resources/Payroll
- Financial
- Fixed Assets
- Fleet Management
- Geographic Information System
- Parks and Recreation
- Permits and Inspections (developed by LOGIS)
- Police Computer Aided Dispatch
- Police Mobile System
- Police Record Management System
- Property Data (developed by LOGIS)
- Special Assessments
- Utility Billing (developed by LOGIS)

Fees:

Flat fee for Internet services and a tiered fee for applications; network support fees reflect usage. Users are assessed for application development.

User Groups:

Each software application has a user group, with the exceptions of Finance, which has two user groups (one for daily end users and a second for finance officers), and Police, also with two user groups. Management information systems coordinators have a networking group.

Host Data for Cities: Data for most applications are hosted at LOGIS

Provide Internet Access: Yes, also wide area network support

Web Site: www.logis.org/

Newsletter: Yes

User Support: LOGIS staff support all applications

User Training: Yes

SOURCE: Office of the Legislative Auditor.

information centers.[3] State statutes require school districts to submit certain financial, teacher, and student data to the Department of Children, Families, and Learning. For instance, the Uniform Financial Accounting and Reporting Standards dictate how school districts are to record transactions and report financial activity. Because all Minnesota school districts must report standardized data to the state, most have found it efficient to join with other districts to compute and report these data.

The Legislature established nine service cooperatives within subregions of the state in 1976 and opened their customer base to all local governments in 1992. Some service cooperatives offer technology services in addition to other services such as insurance and cooperative purchasing. For instance, the Northeast Service Cooperative offers wide-area network services and desktop computer repair services, and it operates as an Internet service provider. The Southeast Service Cooperative offers wide-area network service and certain technical services, such as monitoring of computer usage and line capacity, as well as technical support for acquiring and maintaining local computer networks. In southwestern Minnesota, the SW/WC Service Cooperative is co-located with a regional management information center (described below). Besides offering technology training, the cooperative helps school districts integrate new equipment, operate their networks, and design local Web sites.

Most school districts belong to a computer collaboration for reporting data on students and finances.

Many school districts in Minnesota are members of one of five regional management information centers or the Technology and Information in Educational Services (TIES) consortium, all of which offer financial and human resources services and reporting services for financial, student, and teacher data. The regional management information centers (RMICs) are nonprofit joint powers organizations that provide technology and information resources to member school districts.[4]

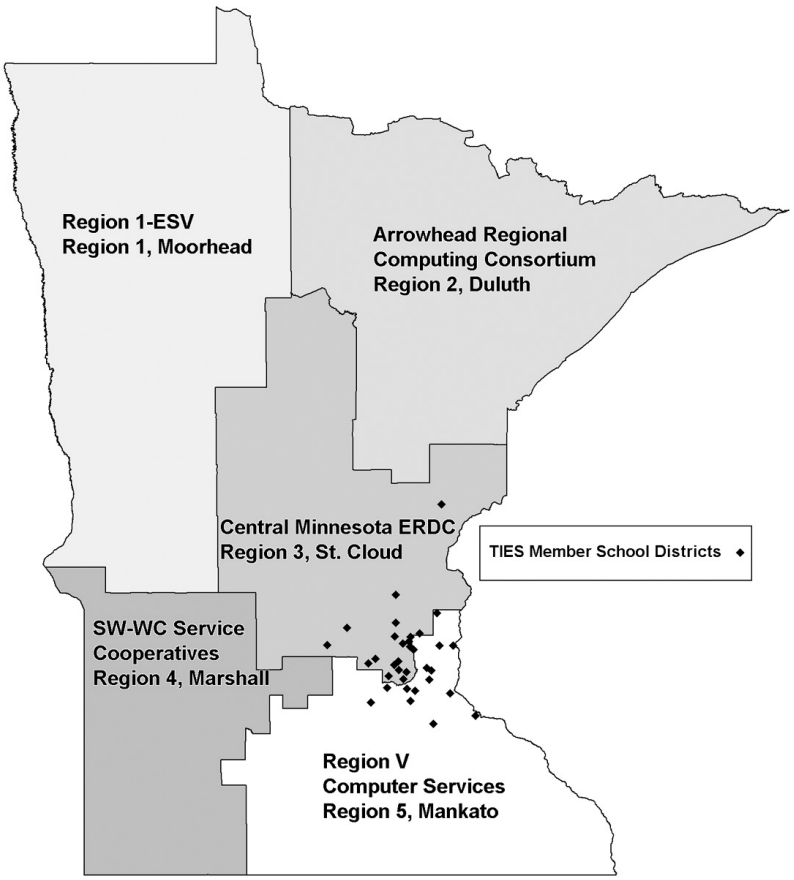
These collaborations manage school districts' finance, payroll, and human resources data, and they may also offer computer network installation and network management services. While school districts use a variety of applications to manage student data, the RMICs provide support for reporting each district's student data to the Department of Children, Families, and Learning. As shown in Figure 2.1, each of the five RMICs generally serves school districts within a distinct geographic region, although these boundaries are not legislatively mandated.[5] Schools that wish to use a RMIC's wide-area network must be located within its regional boundary, although schools from outside a region may also use

3 School districts may also be involved in other cooperative ventures related to technology services, but these fall beyond the scope of this report. For instance, "telecommunications access clusters" have helped coordinate telecommunications networks for groups of school districts and public libraries. Additional information about these services may be found in: Department of Children, Families, and Learning, *Permanent Funding for K-12 School and Public Library Telecommunications Access* (St. Paul, February 2002).

4 At one time, the RMICs were the only sources for certain types of software and support, but this is no longer the case. Currently the Department of Children, Families, and Learning recognizes a number of vendors as well as the five regional information management centers and TIES for student and financial reporting.

5 When the RMICs were first established, school districts in the seven-county metropolitan area were served by TIES and a RMIC known as Metro II. When Metro II was dissolved in the late 1990s, RMIC Regions 3 and 5 expanded their service areas to include those metropolitan school districts that wanted to purchase RMIC services.

Figure 2.1: TIES Member School Districts and Geographic Areas Served by Regional Management Information Centers, 2001



NOTE: The service areas are not legislatively mandated, although at one time similar boundaries were defined in law.

SOURCE: Adapted by Office of the Legislative Auditor staff from a document from Marilyn Raske, Executive Director, Region V, electronic mail, marilynr@regionv.k12.mn.us; accessed January 23, 2002.

certain services. TIES is not assigned a specific geographic region although most of its members are from the seven-county Twin Cities metropolitan area.

Regional Management Information Centers share certain software applications.

The five RMICs use the same application software for collecting and analyzing financial and payroll data and reporting these data to the Department of Children, Families, and Learning or other government agencies. They also work together to develop these applications. Most RMICs store and manage school district financial and payroll data on information management center computers and require school districts to connect via a high-speed, wide-area computer network. In addition, some regional centers offer unique applications. For example, Region 1-ESV in Moorhead supports specialized applications such as student information

and management of school districts' cafeteria meal plan accounts. Table 2.3 lists services provided through Region 1-ESV.

TIES is a joint powers organization formed in 1967, several years prior to the legislation forming the RMICs. School district members may use TIES' software applications for analyzing and reporting student information, accounting, and payroll and human resources. In addition to these applications that TIES developed, the consortium offers other technology services. Several are Internet based, such as curriculum projects designed to meet state education standards; templates allowing teachers to create their own customized Web pages; and a

Table 2.3: Services Available Through Region 1-ESV

Services	Description
PC Support	Optional support at school district buildings, including telephone support
Network Support	Optional support at school district buildings, including telephone support Support of databases centralized at Region 1-ESV facility is part of the members' fees
Applications	
Finance	SMART Finance, developed with four other regions and directly supported by Region 1-ESV
Human Resources	SMART HR, developed with four other regions and directly supported by Region 1-ESV
Student Accounting	SASIxp, developed by a vendor; Region 1-ESV provides telephone support and training
Reporting financial, teacher, and student data to the Department of Children, Families, and Learning	Training, manuals, telephone support, data and error checks, and submitting reports; districts generally submit their teacher reports in a format prescribed by the state
Lunch program	Café Terminal, developed by a vendor; Region 1-ESV provides telephone support and training
Flexible benefits	Region 1-ESV sets up and manages reimbursement accounts for school districts and service cooperatives
Host Data For School Districts	Yes
Provide Internet Access	No
Web Site	www.region1.k12.mn.us/main.htm
Newsletter	Bimonthly issues address (at a minimum) the finance, payroll, and student programs
User Training	Offered for all applications on-site at school districts, at the region's Moorhead offices, or during the annual meeting

SOURCE: Office of the Legislative Auditor.

service allowing teachers to securely enter student grades, attendance, schedules, and contact information from home computers or other remote locations. To facilitate communication among its members, TIES organizes user groups around particular interests, including an accounts payable interest group and an Internet/Webmaster interest group. TIES also offers Internet access, computer certification training, network support and consulting, and bus routing technology.

Use of Computer Collaborations in Minnesota

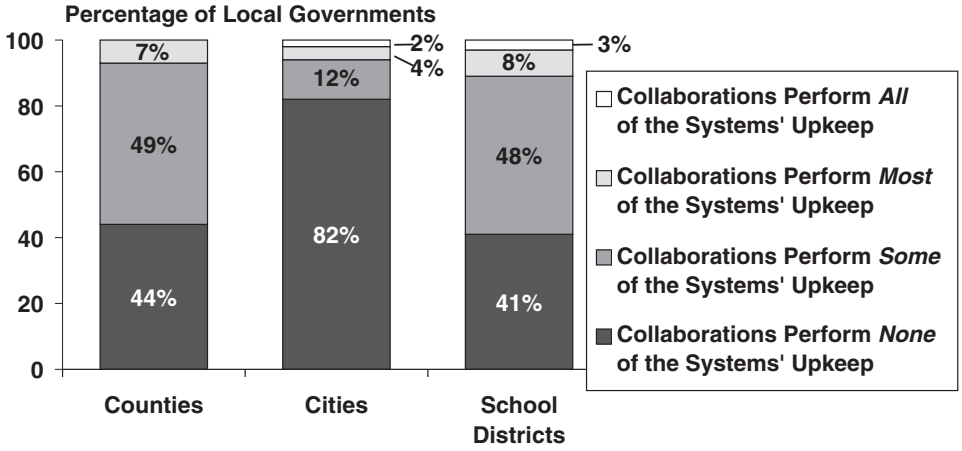
In our survey, we asked local governments about their use of collaborations for maintaining computer systems.[6] Their responses reflect the pattern of computer collaboration availability around the state.

- **While few local governments overall reported using computer collaborations for *all* of their computer systems' upkeep, counties and school districts were more likely than cities to report using collaborations for *some* computer systems' upkeep.**

As shown in Figure 2.2, counties and school districts reported similar use of computer collaborations to help maintain computer systems. Nearly half of the counties and school districts reported using collaborations for *some* of the computer systems' upkeep, and somewhat fewer reported that they used collaborations for *none* of the systems' upkeep. Since fewer city collaborations exist, it is not surprising that 82 percent of cities reported using collaborations for none of their systems' upkeep.

Unlike counties and school districts, most cities are not members of computer collaborations.

Figure 2.2: Local Governments Using Intergovernmental Collaborations to Maintain Computer Systems, 2001



NOTE: Data do not reflect the use of collaborations for supporting software applications. The question read: "What arrangements does your school district have for the updating, security, and daily operations of all the computer system(s) in your jurisdiction?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

6 The question addressed the updating, security, and daily operations of computer systems. It did not specifically ask how local governments manage the use of their software applications per se.

However, as shown in Table 2.4, the size of the jurisdiction was significant. Although no counties reported using collaborations for *all* of their computer systems' maintenance, smaller counties were more likely than medium or large ones to report using collaborations for *most* of that maintenance.[7] More of the large cities (populations of 5,000 or more) than other cities reported using collaborations for *some* or *most* of their maintenance functions; many LOGIS cities are larger cities, with populations up to 60,000. Smaller school districts were somewhat more likely than other school districts to report using collaborations for *most* or *all* of their systems' upkeep.

Few local governments rely on a computer collaboration for all of their computer systems' maintenance.

Table 2.4: Intergovernmental Collaborations Used for Computer System Upkeep, by Type and Size of Local Government, 2001

	All Systems' Upkeep	Most Systems' Upkeep	Some Systems' Upkeep	No Systems' Upkeep
Counties				
Small (fewer than 16,000 residents) (*N*=27)	0%	15%	41%	44%
Medium (16,000 to 49,999 residents) (*N*=31)	0	3	58	39
Large (50,000 or more residents) (*N*=14)	0	0	43	57
Cities				
Small (fewer than 500 residents) (*N*=85)	2	4	5	89
Medium (500 to 4,999 residents) (*N*=152)	2	2	12	84
Large (5,000 or more residents) (*N*=61)	0	10	25	66
School Districts				
Small (fewer than 800 students) (*N*=108)	7	12	46	34
Medium (800 to 2,999 students) (*N*=103)	0	7	47	47
Large (3,000 or more students) (*N*=48)	0	2	54	44

NOTE: Data do not reflect the use of collaborations for supporting software applications. The question read: "What arrangements does your [jurisdiction] have for the updating, security, and operations of all the computer system(s) in your jurisdictions?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Advantages and Disadvantages of Using Collaborations

We identified several benefits that local governments have found when using a computer collaboration. In Minnesota:

- **Intergovernmental computer collaborations provide local governments with specialized expertise, networking opportunities, chances to avoid purchasing certain equipment or software, and a degree of control over the design of computer applications.**

7 For this analysis, we divided jurisdictions by population into three groups. Small counties had populations of less than 16,000; mid-size counties had populations between 16,000 and 49,999; and large counties had populations of 50,000 or more Small cities had populations of less than 500; mid-size cities had populations between 500 and 4,999; and large cities had populations of 5,000 or more. School districts were divided as follows: small districts had enrollments of less than 800; mid-size districts had enrollments of between 800 and 2,999; and large districts had enrollments of 3,000 or more.

Most of these advantages listed below come from combining resources and achieving economies of scale. They tend to apply to jurisdictions of all sizes but some may be less useful to the very largest jurisdictions if these local governments need specially tailored applications or if they have their own in-house computer expertise.

- Computer collaborations provide access to expertise for developing and modifying sophisticated software applications. This is particularly cost-effective for applications subject to frequent changes, such as for school district financial reporting, and for common applications that can be used across numerous jurisdictions, such as for human resource services. The benefit of the expertise may be less for those local governments that need highly customized applications and can afford to develop their own.

- By relying on collaborations, local governments have less need to hire and retain specially skilled in-house computer staff. Small and medium-sized local governments may be less able to afford such positions and may not need them on a full-time basis.

- Where the computer collaboration provides services using sophisticated equipment or software with extended features, working with the collaboration avoids the need to acquire such equipment or software in-house.

Computer collaborations offer their members stability.

- Compared with computer vendors, collaborations offer a higher level of control over applications and computer functions because members of the joint powers organizations control decision making.

- Because computer collaborations are by definition member based, they offer stability. That is, a collaboration will typically stay in business as long as it meets members' needs. Members control what services the collaboration provides. This may be of particular benefit to small and medium-sized local governments that lack their own IT staff.

- Collaborations offer intercommunications and networking among employees who come from different local governments but share similar concerns. The educational value of these interactions applies to employees in governments of all sizes.

- Local governments can fairly easily and accurately identify the costs for using collaborations because fees are typically charged according to the specific services used.

At the same time, computer collaborations have some disadvantages. We learned that:

- **The downsides of intergovernmental computer collaborations relate to the additional time and effort needed to work with collaboration members, the loss of individual control inherent with group decision making, and the risks involved with relying on external organizations for technology services.**

The disadvantages of computer collaborations listed below do not appear to vary by size of jurisdiction, but the downsides would be greater for local governments with unique needs requiring highly customized computer services or those that rely extensively on collaborations for core functions.

A collaboration typically focuses on meeting the technology needs of its entire group of members.

- Planning and working with other members of the collaboration takes time.
- There is less flexibility to tailor a software application since it usually must meet the needs of the entire group.
- Individual local governments lose some control over the timing of service upgrades because schedules for improvements or changes reflect the decisions of the group.
- For collaborations that sell services as a package, there may be incentives for local governments to use multiple services that may not best fit their needs.
- Local governments must manage their collaboration agreements to ensure adequate service and avoid unrealistic expectations.
- Relying on a collaboration for technology services involves certain risks, especially when the services are critical to a local government's operation. Although members control a collaboration to a large extent, certain factors beyond their control could disrupt a collaboration's ability to continue offering services. Local governments must be prepared to assess a collaboration's financial stability and claims about the level of its services.

Computer Vendors

Many computer vendors sell or coordinate hardware, software, management expertise, and support for networks and computers. As mentioned earlier, in this discussion we are focusing on vendors that supply computer services as opposed to those that only sell hardware and equipment. Vendors are businesses, and local governments do not "own" them in the same way that members "own" collaborations. We interviewed several vendors but did not attempt to evaluate the quality of their services or compare costs among them.

Some vendors provide or coordinate several services, such as network support and software applications; their services may be available statewide. For example, several vendors on the "master roster" maintained by the Office of Technology provide a range of PC, network, and applications to local governments throughout Minnesota.[8]

Other vendors provide a specific application or service. Common business applications are those for finance and payroll. Some applications are designed

8 The Office of Technology maintains an on-line, searchable master roster of more that 170 technology providers at www.ot.state.mn.us/mastercontract/mrinfo.html. To qualify for the roster, vendors must provide written information about their experience, references, rates, and methods used to ensure project success, and they must accept certain state requirements, such as affirmative action requirements.

especially for a certain type of local government. As an example, one vendor works with a county collaboration providing county-specific applications, including one for processing property taxes. Another vendor developed financial software widely used by Minnesota counties.

Many other vendors provide trained staff for PC and network support. How vendors provide services depends in part on the type of service. PC support usually requires a vendor to sometimes be at a local government's site, although telephone support may also be available, and some vendors analyze network and PC problems remotely by computer. Using their own computers, some vendors run applications and manage data on behalf of local governments; in these cases, the local jurisdictions do not own the computer. On the other hand, local governments using their own computers may run licensed applications and use vendors to provide user support via telephone, e-mail, or even Web sites.

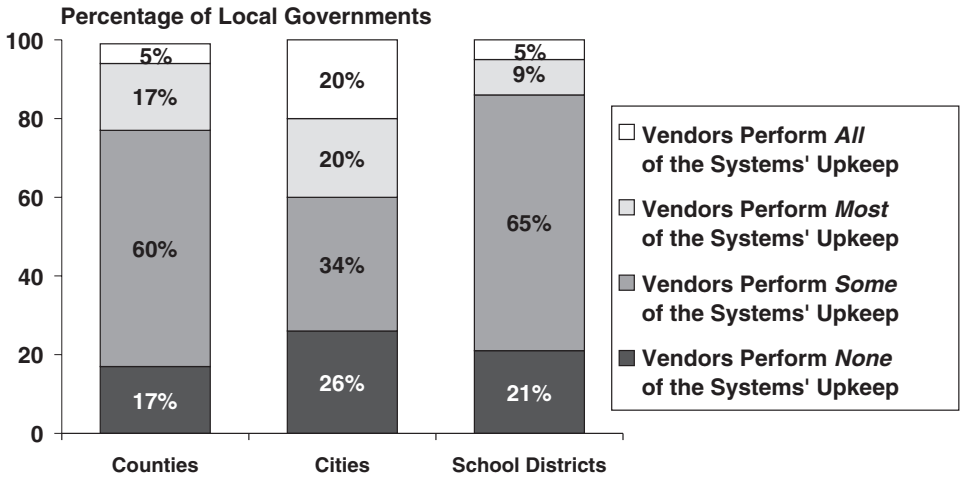
Based on the results of our survey:

- **Although a relatively small proportion of local governments overall reported using vendors for all of their computer systems' upkeep, cities were more likely than counties and school districts to report having done so.**

As shown in Figure 2.3, 20 percent of cities reported that vendors performed *all* of their computer system upkeep, compared with 5 percent each of counties and school districts. Patterns for counties and school districts were similar with 60 percent of counties and 65 percent of school districts reporting that they used

Most local governments use computer vendors for at least some of their computer systems' maintenance.

Figure 2.3: Local Governments Using Vendors to Maintain Computer Systems, 2001



NOTE: Data do not reflect the use of vendors for supporting software applications. The question read: "What arrangements does your school district have for the updating, security, and daily operations of all the computer system(s) in your jurisdiction?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

vendors for *some* computer system maintenance. Just 34 percent of cities used vendors for *some* computer system maintenance.

Local government size appears related to the use of vendors, with smaller jurisdictions more likely to rely heavily on vendors. Small counties were more likely than other counties to report using vendors for *most* or *all* of their computer system maintenance, as shown in Table 2.5. Compared with large cities, small and medium-size cities were more likely to report using vendors to maintain *all* of their computer systems. School districts also varied somewhat by size, with few large school districts using vendors for *most* or *all* of their computer systems' maintenance.

Smaller jurisdictions are more likely to rely heavily on computer vendors.

Table 2.5: Computer Vendors Used for Computer System Upkeep, by Type and Size of Local Government, 2001

	All Systems' Upkeep	Most Systems' Upkeep	Some Systems' Upkeep	No Systems' Upkeep
Counties				
Small (fewer than 16,000 residents) (*N*=30)	10%	23%	53%	13%
Medium (16,000 to 49,999 residents) (*N*=31)	3	16	65	16
Large (50,000 or more residents) (*N*=14)	0	7	64	29
Cities				
Small (fewer than 500 residents) (*N*=95)	21	11	18	51
Medium (500 to 4,999 residents) (*N*=169)	22	29	34	15
Large (5,000 or more residents) (*N*=66)	12	11	58	20
School Districts				
Small (fewer than 800 students) (*N*=114)	10	11	64	16
Medium (800 to 2,999 students) (*N*=106)	3	10	63	24
Large (3,000 or more students) (*N*=48)	0	4	69	27

NOTE: Data do not reflect the use of vendors for supporting software applications. The question read: "What arrangements does your [jurisdiction] have for the updating, security, and operations of all the computer system(s) in your jurisdictions?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Advantages and Disadvantages of Using Vendors

Local governments described several benefits from using computer vendors, some of which are similar to those identified for intergovernmental collaborations. In Minnesota:

- **Computer vendors may provide local governments with specialized expertise or opportunities to avoid purchasing certain software or equipment.**

Many of the advantages listed below come from the economies of scale achieved by working with a company that sells similar services to many other units of government.

- Vendors can supply the technological expertise needed to develop or manage sophisticated applications when local governments would not otherwise have access to such expertise. Some vendors are especially useful when local governments cannot use "off-the-shelf" applications but instead need some degree of specialization. The relative size of the benefit may be less for very large local governments that may be able to afford to develop their own applications.

Computer vendors can provide specialized technological expertise.

- Computer vendors can hire and retain skilled staff, reducing the local governments' need for placing similarly skilled staff on their payrolls. Especially for small and medium-sized local governments, or governments of any size that require specialized computer skills, using vendors' staff may reduce what they would otherwise have to pay. Further, smaller local governments are less likely to need these positions on a full-time basis.

- If a vendor provides services on sophisticated equipment or software with extended features, working with that vendor avoids the need for a local government to acquire such equipment or software.

- To the extent that the vendor supports user groups, there may be opportunities for intercommunications and networking among employees from different jurisdictions.

- Local governments can fairly easily and accurately identify the costs for using vendors because costs are tied to the specific services provided.

External service providers may allow local governments to avoid purchasing certain computer hardware.

At the same time, working with vendors can present certain disadvantages. We observed that:

- **The downsides of working with computer vendors include the need for careful contract management, the risks involved with relying on external organizations for technology services, and the loss of control over pricing, schedules, and service features.**

Many of the disadvantages that follow relate to the challenges of having limited control over the service. With one exception as noted below, the downsides do not tend to vary by size of local government. The downsides could be greater for those jurisdictions that rely heavily on computer vendors for core services.

- Local governments need to have the personnel and the administrative skills to carefully write and manage vendor contracts. This is necessary to ensure that the vendors are held to contractual obligations and meet local governments' expectations for the product or service. While local governments of all sizes are often involved with contracts, smaller jurisdictions may lack the number of staff needed to actively manage vendor contracts.

- There are risks involved with relying on computer vendors for technological services, especially when the services are critical to a local government's operation. If the financial viability of a vendor is unknown, local governments may risk having their technology services disrupted and their data inaccessible should the vendor go out of business. Local governments must be prepared to assess a vendor's financial stability as well as any claims the vendor makes about the level of its services, such as the security it provides or the expertise of its staff. They also need assurances that sensitive data will be adequately protected.

Local governments should assess a vendor's financial stability.

- To the extent that there are few suppliers for a particular computer service, local governments may have little choice but to pay a vendor's asking price for applications or services.

- Local governments lose some control over service improvements, because vendors may not be immediately available as local problems arise. The vendor may take more time than is desirable from the local government's perspective to fix equipment or make substantial changes, such as integrating an application with other applications. To some degree this downside can be managed through agreements in the contract specifying the intervals within which vendors will respond to local government needs.

- Local governments may have to abide by applications or services designed to meet the needs of the vendor's full client base, unless the vendor is hired to completely customize an application.

In-House Staff

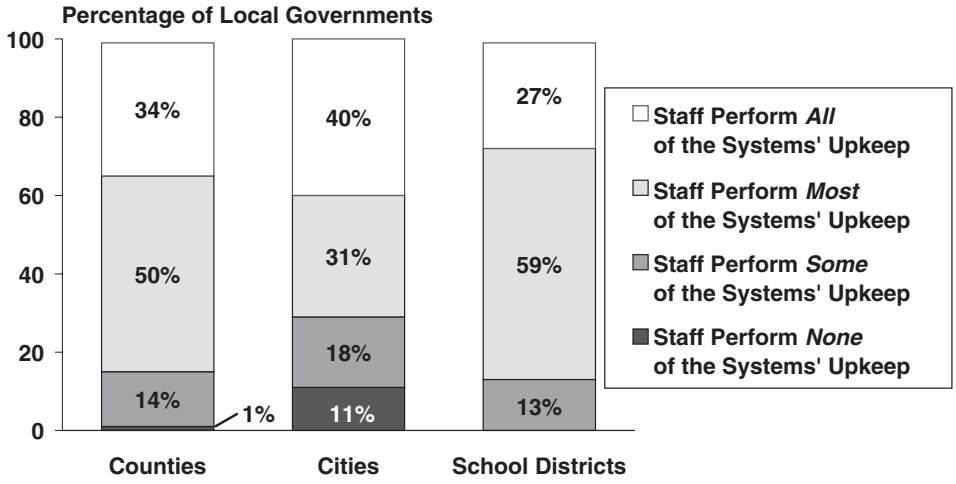
Local governments could choose to bypass vendors and collaborations and develop their own applications and support their computers and networks entirely with their own staff. While many local governments use in-house staff for some computer-related activities, few manage every part of their systems by themselves. For example, the city of Lakeville relies on two staff to manage day-to-day operations of its computer system and to do long-range planning, but it is also a member of a computer collaboration for specific software applications.

In our survey, we asked local governments about their arrangements for computer system updating, security, and daily operations. As shown in Figure 2.4,

- **A majority of counties and school districts used in-house staff to perform *most* of their computer systems' upkeep, while a plurality of cities said their own staff performed *all* computer systems' upkeep.**

Only a few cities and one county reported that their own staff perform none of their computer systems' maintenance.

Figure 2.4: Local Governments Using In-House Staff to Maintain Computer Systems, 2001



NOTE: Data do not reflect the use of in-house staff for supporting software applications. The question read: "What arrangements does your [jurisdiction] have for the updating, security, and daily operations of all the computer system(s) in your jurisdiction?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Higher percentages of cities than counties or school districts reported using in-house staff for *all* of their computer systems' upkeep. At the same time, cities were more likely than counties and school districts to use in-house staff for *none* of their computer systems' maintenance.

As shown in Table 2.6, the size of jurisdictions was somewhat related to the use of in-house staff for computer system operations, particularly for cities. Small cities were far more likely than cities of other sizes to report using in-house staff for *all* of their systems upkeep. As noted in Chapter 1, the small cities were most likely to have simple computer systems (with few computer networks or file servers), which may partially explain why they rely less on outside expertise. In contrast, small school districts were somewhat less likely than larger school districts to report using in-house staff for *all* of their computer systems' maintenance. Medium-and large-sized counties were somewhat more likely than small counties to report using in-house staff to maintain *most* or *all* of their computer systems.

Table 2.6: In-House Staff Used for Computer System Upkeep, by Type and Size of Local Government, 2001

	All Systems' Upkeep	Most Systems' Upkeep	Some Systems' Upkeep	No Systems' Upkeep
Counties				
Small (fewer than 16,000 residents) (*N*=30)	27%	43%	27%	3%
Medium (16,000 to 49,999 residents) (*N*=31)	39	52	10	0
Large (50,000 or more residents) (*N*=15)	40	60	0	0
Cities				
Small (fewer than 500 residents) (*N*=101)	60	18	8	13
Medium (500 to 4,999 residents) (*N*=170)	35	34	21	11
Large (5,000 or more residents) (*N*=65)	23	45	26	6
School Districts				
Small (fewer than 800 students) (*N*=111)	21	57	23	0
Medium (800 to 2,999 students) (*N*=107)	31	61	8	0
Large (3,000 or more students) (*N*=48)	35	63	2	0

NOTE: Data do not reflect the use of in-house staff for supporting software applications. The question read: "What arrangements does your [jurisdiction] have for the updating, security, and operations of all the computer system(s) in your jurisdictions?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Small cities were very likely to use their own staff for all computer system maintenance.

Advantages and Disadvantages of Using In-House Staff

Local governments identified several benefits that they found when using in-house staff to provide a specific service or computer system component. We observed that:

- **In-house technology staff provide local governments with a high degree of control over computer services, and they avoid the necessity of compromising to meet the needs of a group.**

Most of the advantages listed below arise due to local government staff setting their own priorities for computer services. The advantages do not vary by size of local government.

- A local government can determine the extent of the features its applications will offer and set its own timelines for modifying applications or equipment.

- A local government can rely on staff to perform specific services as soon as needs arise; if priorities shift, staff can refocus their attention in response.

- A local government can avail itself of specialized applications tailored to its unique needs.

- Local government management can avoid having to write and manage contracts for computer services with external organizations.

- A local government can have direct control over sensitive information.

We also learned about certain disadvantages arising from the use of in-house computer staff.

- **For jurisdictions with computer systems of some complexity, the downsides of using in-house computer staff relate to the cost of employing highly skilled personnel.**

Local governments that are small yet have relatively complex computer systems may feel the downsides of using in-house computer staff more than larger jurisdictions. At the same time, local governments with fairly simple computer systems may have less need for specialized support or applications and would be less susceptible to any negative consequences.

Small jurisdictions may not be able to afford or justify their own full-time technology staff.

- Moderately complicated services or networks would require specially trained staff who may be costly to hire and difficult to retain (although the costs would vary by labor market conditions). Technical staff need ongoing training to stay skilled in their craft. Smaller jurisdictions may have more difficulty affording the expense of their own computer staff or justifying them on a full-time basis.

- Specialized applications require certain skills that can be expensive and time consuming to develop.

- Opportunities for intercommunications and networking with other local government staff may not exist. Local governments that rely on in-house computer staff would have to proactively seek networking opportunities for their staff or construct their own to share common computer concerns. This may be particularly difficult for staff in more remote jurisdictions.

- Employing too few IT staff could jeopardize the effectiveness of a computer system. It may be difficult to determine the number of staff needed to support a computer system over time, and there is no formula for determining the correct number (as discussed in Chapter 3). In times of financial stress, jurisdictions may view eliminating staff as a budget-balancing option, but insufficient staff could affect the quality of technology services, threaten the technology investments, and disrupt the jurisdiction's ability to finish its work.

Managing Computer Systems With a Mix of Options

Many local governments have decided that a mix of management options best meets their needs. For instance, a county may be a member of one collaboration

for a property-tax application, contract with a vendor for network maintenance, and use in-house staff to operate and maintain its PCs and other hardware.

According to our survey,

- **Most local governments, and particularly counties and school districts, rely on a mix of options to manage their computer systems.**

Three-fourths of all local governments, including most counties and school districts, reported using two or three management options just to maintain their computer systems. Nearly all jurisdictions that reported using more than one option to manage their computer systems used in-house staff as one of the options. Beyond the survey results, we learned that nearly all counties and many school districts obtain support for certain applications from intergovernmental collaborations. Many local governments also pay license fees to vendors for software, such as financial and human resource applications.

Nearly all of the jurisdictions using a mix of management options used their own staff to perform some functions.

At the same time, we found that about one-fourth of all jurisdictions, mostly small and medium-sized cities, reported using a single option to maintain their computer systems. Seventy percent of those jurisdictions used in-house staff as the single option. However, when considering the use of software applications (which was not asked on the survey), even these smaller local governments probably use more than a single management option because many are likely to use licensed applications supported by a vendor.

PREPARING TO EVALUATE MANAGEMENT OPTIONS

As we have noted, each option for managing computers has advantages and disadvantages. But before local government managers decide which options would work best for them, they should prepare themselves to make this decision. The following section explains what local governments should have in place before evaluating their options for managing computer systems.

Assess Readiness Before Evaluating Management Options

In advance of deciding how to manage their computer systems, local governments should assess their readiness to rely on their own staff, join intergovernmental collaborations, or use computer vendors. As detailed in Table 2.7, local governments should undertake certain activities, such as identifying government services that need automation, to prepare themselves to adequately assess their options.

Table 2.7: Actions for Preparing to Assess Management Options

- Information technology needs the support of elected officials and program managers
- Local governments should determine where information technology fits in their organizations
- Local governments should have the capacity to estimate life-cycle costs and set spending priorities
- Planning should drive decisions on replacing or upgrading a computer system
- Local governments should follow accepted contract management practices and understand the risks of externally provided services
- Local governments should identify services that need automation
- Local governments should assess special circumstances affecting management options

SOURCE: Office of the Legislative Auditor.

RECOMMENDATION

Before evaluating options for managing computer systems, local governments should (1) make sure that information technology has the understanding and support of top officials, (2) determine where IT staff fit within their organization, (3) have the capacity to estimate total costs and manage contracts, (4) decide for which services technology is appropriate, (5) plan for computer system upgrades, and (6) consider other political and demographic factors.

Information Technology Needs the Support of Elected Officials and Program Managers

Before evaluating computer management options, local governments should make sure that top officials understand and support the role of IT. Elected officials who control the budget and are accountable to taxpayers must know the costs and benefits of IT. Similarly, local government program managers must be able to explain to employees who use the computer system how IT will help accomplish the government's critical tasks.[9] The person responsible for the computer system is uniquely positioned to facilitate this communication. He or she can help others understand the costs and benefits of technology within the constraints of limited resources. Adequate communication may help justify IT expenditures, motivate program managers to explore new uses of technology in delivering services, and

9 Ronald J. Raumer, "Strategic Planning for Technology Investments," *Government Finance Review* (December 2001), 33. Also see Thom Rubel, *Promoting Excellence in Electronic State Government* (Washington, D.C.: National Governors Association Center for Best Practices, February 8, 2001); www.nga.org/center/divisions/1,1188,C_ISSUE_BRIEF^D_2153,00.html; accessed February 11, 2002; Office of Program Policy Analysis and Government Accountability, *Administrative and Instructional Technology Best Practices Goal A* (Tallahassee: Florida Legislature, October 2000); www.oppaga.state.fl.us/reports/pdf/admintech.pdf; accessed February 14, 2002; and Center for Technology in Government, *Tying a Sensible Knot* (Albany, NY: Center for Technology in Government, June 2001), 48; www.ctg.albany.edu/resources/pdfrpwp/iis1.pdf; accessed February 14, 2002.

encourage those who use the computers to abide by necessary restrictions, such as procedures to ensure security.

For example, **Mille Lacs County's** information services director used comparative information about county IT services to gain support from elected officials for additional staff. The county's information services department had consisted of one full-time staff person to support 170 computers and several networks. Before approaching the county board with the most recent request for additional staff, the information services director wanted the board to understand the department's role and the variety of its work. To accomplish this, the department director researched information technology standards and resources in adjoining counties. Then the director listed the various departments and software with which she worked and compared it with information from other counties. Along with the support of the county coordinator, this information contributed to the board's approval of a new part-time information services position. For more information contact Michelle Malley, Information Services Director, at michelle.malley@co.mille-lacs.mn.us or 320/983-8276.

Local Governments Should Determine Where Information Technology Fits Within Their Organizations

As part of preparing to evaluate computer system options, local governments should analyze where their own technology staff best fit within their jurisdiction's organization. This factor is of concern only for those jurisdictions that employ technology staff or plan to. Responsibility for IT services may be centralized into one department, decentralized across several departments, or managed in a hybrid fashion with only certain services centralized. The IT unit may be under the authority of another department or it may stand on its own. There is no single correct arrangement, and it is important that each local government determine which organizational structure will best meet its technology and service delivery goals.

There is no single correct organizational structure for organizing technology staff within a jurisdiction.

A centralized organizational structure offers a high level of control over IT operations and a high degree of consistency among IT services.[10] It has the advantages of economies of scale and volume purchasing, which may lower support costs. At the same time, a centralized structure may be less attuned to user needs and more resistant to changes from normal operating procedures. A decentralized organizational structure may offer greater flexibility, focus more on the specific technology needs of individual departments, and be more closely aligned with end users' needs. On the other hand, it may be prone to administrative redundancies and incompatible technology platforms across departments. Compared with an independent IT unit, IT employees that are organized under and report to the authority of a certain department may be able to serve that department well but may have less understanding of how technology could assist other departments.

10 Right Track Associates, Inc., "IT Organizations by Design," *ITToolkit;* www.ittoolkit.com; accessed April 4, 2002.

In considering the best fit for IT staff, a local government should first identify its technology needs and know what it wants IT to be in its jurisdiction.[11] Identifying its technology needs means articulating what services require technology to meet local objectives, the potential for growth among those services, the size and number of the government's work sites, existing hardware and other equipment, and the technical expertise of computer users. Then a jurisdiction has to match its identified needs with the organizational arrangement offering the best fit. As one example, a local government with employees that have fairly sophisticated technical skills may have less need for a decentralized IT department and its proximity to end users' needs.

Local Governments Should Have the Capacity to Estimate Life-Cycle Costs and Set Spending Priorities

To make informed decisions, local governments need to estimate total costs of computer systems.

Another consideration in assessing readiness to compare management options is the capacity of the local government to fully estimate computer systems' costs and set spending priorities for the systems. A fair comparison of management options requires a clear understanding of the benefits and costs of each option. Local governments should have the know-how to estimate the total costs over the life cycle of equipment, including all capital, operating, and replacement costs.[12] For staff, total costs include not only salaries and benefits but also hiring and ongoing training. Another element of total costs relates to the expense of change: local governments that have acquired certain equipment to be part of a provider's wide-area network, for example, could encounter additional equipment expenses by switching providers. Table 2.8 presents a list of items for which total costs should be estimated. Fully estimating computer system costs can be difficult because some costs, such as ongoing security costs, are not necessarily obvious. Yet, these costs are important because more than half of the costs over the life of a computer system can be attributed to ongoing operations and maintenance.[13]

Table 2.8: Items for Which Total Costs Should Be Estimated

- Hardware and software, including replacements and upgrades
- Staff salaries, overtime pay, benefits, recruitment, hiring, and training
- Infrastructure, such as cabling and facilities
- Contracts for technology services, such as network management
- Ongoing maintenance and security

SOURCE: Center for Technology in Government, *Untangle the Web: Delivering Municipal Services Through the Internet*, 2001, 8. View on-line at www.ctg.albany.edu/resources/pdfrpwp/utw.pdf.

11 Ibid.

12 Life-cycle cost analysis is an economic method of project evaluation in which all costs arising from owning, operating, maintaining, and disposing of a project are considered important to the decision. Federal Emergency Management Program, *Guidance on Life-Cycle Cost Analysis Required by Executive Order 13123* (April 26, 2000); www.eren.doe.gov/femp/resources/lifecycleguide.html.

13 U.S. Department of Justice, Justice Management Division, *The Department of Justice Systems Development Life Cycle Guidance Document Chapter 11: Operations And Maintenance Phase* (Washington, D.C.: Department of Justice, March 2000), 1; www.usdoj.gov/jmd/irm/lifecycle/ch11.htm; accessed February 14, 2002.

Local governments should also have the capacity to set spending priorities for computer systems. This implies having criteria in place to set rational priorities among competing projects, whether they are technology projects or related to other services. To do this, local governments should have a capital planning process in place that makes explicit how their technology investments will support their organization's objectives.[14] To reflect maintenance and daily support for computer systems, local governments should also have the capacity to rationally set priorities among programs in annual operating budgets.

Anoka County established a process to set priorities among the technology needs of the county's 13 divisions. The process is designed to coordinate technology efforts across the county and to allocate county IT resources prudently. An IT management committee, made up of the heads of each division, meets monthly to review IT projects of certain sizes, with medium-sized projects ranging between $20,000 and $100,000. The committee follows a five-step process that offers a structured way to analyze each proposal qualifying for review. During the committee's review, proponents describe their proposal and assess its benefits and costs, including the level of support the project would require from the information services department. Because proponents are required to use a specific form to present their proposal, committee members receive approximately the same type of information on each project. The process requires proponents to build a case for their projects and defend them before the committee. Because the committee can make an informed decision about which projects receive priority, the process allows the county to avoid funding projects based merely on how aggressively proponents promoted them. For more information contact Cindy Kevern, Director of Information Services, at cindy.kevern@co.anoka.mn.us or 763/323-5368.

Local governments should plan for computer replacement.

Planning Should Drive Decisions on Replacing or Upgrading a Computer System

Before evaluating the options for managing computer systems, local governments need an informed process for planning system changes. Technology evolves rapidly, and a planned replacement program is necessary to avoid fragmented, inadequate, or

Planned replacement programs are needed for up-to-date computer systems that fully meet a jurisdiction's technology needs.

14 Federal CIO Council, *Smart Practices in Capital Planning* (October 2000), 7, 32; www.cio.gov/Documents/smart_practices_book.pdf; accessed February 28, 2002.

outdated computer systems. Local governments need long- and short-term planning that tie technology investments to their core functions and lay out specific criteria for selecting projects.[15]

New or replacement computers should be compatible with the existing capacity to support them.

Within its planning process, a local government should consider the financial, organizational, operational, and technological advantages and disadvantages of its technology initiatives. For example, when purchasing new computers, a jurisdiction should consider whether new equipment would be compatible with the existing computer network and whether current staff have the expertise to support the new machines. Because a change to a computer system can affect the rest of the system's reliability, security, or ease of use, local governments should be able to assess how the change fits into the current technical environment.[16]

As an example of a planning process for computer upgrades, the **Hopkins School District** developed standards in 2001 for its hardware and software. For instance, one of the standards is that all computers in the labs used by students should have CD drives and all staff and faculty computers should have DVD drives. A committee with districtwide representation developed the standards, which are to guide future purchases of computers, peripheral equipment such as printers, and software for classroom and business uses. Its objectives were to create greater consistency and compatibility among the technology around the district because much of the existing equipment was obsolete and prevented users from sharing files. Further, maintaining and upgrading numerous different applications and computers was inefficient. In developing the standards, the committee wanted to be environmentally conscious by avoiding disposable technology and purchasing only computers with sufficient flexibility that they could serve other district functions after meeting their original purpose. Although the district's information services staff set a ten-year schedule for fully implementing the standards in all elementary, junior high, and senior high schools, they realized that the standards themselves would need updating in a few years. For more information contact Lee Rodel, Technology & Information Services Coordinator, at lee_rodel@hopkins.k12.mn.us or 952/988-4101.

Local Governments Should Follow Accepted Contract Management Practices and Understand the Risks of Externally Provided Services

Because managing computer systems often involves working with external providers in some capacity, local governments should be prepared to follow appropriate contract management practices. This means they should have the capacity to exercise financial oversight, including the ability to evaluate the provider's financial stability and the validity of the provider's claims about its services.[17] This is especially important for contracts related to mission-critical systems because failure of those systems could be costly. Following good

---

15 Information Technology Resources Board, *Practical Strategies for Managing Information Systems;* http://itrb.gov/documents/itrbps%2Ehtm; accessed August 27, 2001.

16 Right Track Associates, Inc., "The Upgrade Assessment Process," *ITToolkit;* www.ittoolkit.com; accessed February 4, 2002.

17 Gartner Research, "Staffing Requirements Before and After Outsourcing," *Research Note* QA-OUT-063, January 17, 1997, 2; and Information Technology Resources Board, *Practical Strategies for Managing Information Systems*.

contract management, such as actively monitoring a provider's performance, allows local governments to protect the integrity of their contracted services. Table 2.9 lists accepted practices for preparing, executing, and overseeing contracts.

Relying on service providers external to a local government may entail risks due to the uncertainties of the technology business environment. Business failures cannot be easily predicted, but they do occur, and local governments that rely on others for technology related to their core services face higher risks simply because more is at stake. Consequently, local governments should take steps to protect themselves. They need to be prepared to assess the financial stability of providers as well as plan fallback procedures to ensure they can retrieve their data and still offer services in the event that a contracted provider fails to produce as

Local governments should assess the financial stability of potential technology providers.

Table 2.9: Practices for Good Contract Management

Preparation

- Verify that contracting is an appropriate method to obtain the needed service or good
- Explicitly state the nature of the problem for which the contract is sought
- Seek out multiple potential providers
- Assess the potential providers' suitability, financial stability, and quality

Execution

- Be specific and draft a clearly worded contract
- Include provisions to hold provider accountable for the work
- List the provider's duties, required qualifications, expected work, and final product quality
- List specific costs for the work
- Include an effective date for the contract
- Specify expected security provisions or data practices requirements
- Specify back-out clauses, refunds, and conditions for terminating the contract
- Include measures to determine how the government will know it received what it wanted
- Determine how the government will enforce contract provisions
- Detail requirements for transferring knowledge to government staff to continue service delivery if needed, should the provider become unavailable
- Avoid relying on a provider's contract language, which may differ from the government's objectives
- Before signing, review all contracts (relying on an attorney when needed for large or complicated contracts)

Oversight

- Monitor and inspect the provider's performance
- Direct the provider during the course of the work
- Keep records of the contract, work provided, and how that work was performed

SOURCE: Minnesota Department of Administration, *Professional and Technical Services Contract Manual* (St. Paul, September 2001).

promised.[18] They should also include safeguards in their contracts such as back-out clauses and conditions for refunds.

Local Governments Should Identify Services That Need Automation

Technology should be used to improve services, not simply because it is available.

Before they can evaluate options to manage their computer systems, local governments should understand what services need to be automated. Computer systems can make key work processes more efficient, but automation may not always make sense, and local governments must make this judgment for their own services. Local governments should align their use of computerization with the services they deliver so that the technology clearly supports their programs and data. They should focus on using technology to increase value, not adding technology simply because it is available.[19] When determining what ought to be automated, local governments should take into account the abilities of those who will be implementing and maintaining the computer system to understand what may be needed in terms of adding or training staff.[20]

Mantorville is a city of just over 1,000 residents in southeast Minnesota that chose to automate some of its business functions using the single computer it purchased in 1998. To support the city's utility billing, fund accounting, and payroll functions, the city licenses software applications from a vendor in Texas. With these applications, the city clerk can quickly generate utility bills and track city payments. The software also allows the clerk to accurately calculate employee pay, deductions, and benefits, as well as generate paychecks and federal reports. Besides the accuracy and time savings that came with automating these functions, Mantorville wanted a system that could be easily maintained. Consequently, the city has a maintenance contract whereby the city clerk can obtain technical support by telephone or from the vendor's Web site. With certain software, the vendor can also remotely diagnose computer problems. The clerk receives software upgrades by e-mail or downloads them from the vendor's Web site. For more information contact Cheryll Selle, City Clerk-Treasurer at mantor21@aol.com or 507/635-5170.

Local Governments Should Assess Special Circumstances Affecting Management Options

In preparation for evaluating options to manage computer systems, local governments must assess their readiness in the context of their own unique demographic factors, technological resources, financial constraints, and political considerations. During the course of our study, we learned from local governments about several considerations that affected the feasibility of their choice of computer system services. The considerations follow, although the extent to which they apply will vary for each local government.

---

18 Tim Couldrick, "Keys to Successful Outsourcing Contracts," *ZDNet (UK)* (September 27, 2001). Also see Debbie DeVoe, "Weeding Out Weak Vendors," *InfoWorld.com* (September 21, 2001); www.infoworld.com/articles/pe/xml/01/09/24/010924pevendor.xml. In addition, Minnesota's Uniform Municipal Contracting Law, which applies to counties, cities, and school districts, outlines requirements for pursuing sealed bids or direct negotiations; see *Minn. Stat.* (2000) §471.345.

19 Information Technology Resources Board, *Practical Strategies for Managing Information Systems*.

20 Center for Technology in Government, *Tying a Sensible Knot,* 60.

The location of a local government may limit its computer management options.

- **Hiring and retaining qualified in-house staff**. The opportunity to locate and hire appropriately trained staff may vary around the state. Especially in certain rural areas, the labor market may not offer qualified candidates for specialized technology positions, forcing local governments to consider other management options.

- **Need for customization.** Local governments with needs for software designed to their particular requirements may have fewer management options available. For example, if a local government uses a highly customized software application linked to a database for producing specialized reports, replacing it with a more broadly based application may not be desirable.

- **Geographic access to computer service providers.** Some intergovernmental collaborations or computer vendors provide services only within a specific geographic area or to local governments of a particular size. Lack of access to alternative providers may force some local governments to continue existing service arrangements simply because other options do not exist.

- **Concerns about loss of control.** Local governments with strong preferences for working with their own staff have less potential for successfully joining a group to make collaborative technology decisions.

- **Equipment to reliably transfer data to an outside provider.** Some computer service providers may have minimum connection requirements, such as the need to link to a wide-area network. Local governments may need additional technological equipment to use those services, which represents an added cost. The needs to keep electronic data secure and maintain privacy for sensitive data may also add costs.

- **Preferences that limit the number of local government staff.** Local governments that are under restrictions to tightly limit the number of employees they hire may be forced to consider options other than hiring permanent in-house staff.

3 Best Practices for Managing Computer Systems

SUMMARY

When evaluating options for managing computer systems, local governments should determine whether the options they are considering follow the best practices of conducting inventories, adopting computer policies, and communicating policies to staff who use the computers. Local governments should also consider whether the management options have sufficient technical expertise and provide training and support for users. Finally, they need to assess whether the options provide adequate computer security.

This chapter describes best practices necessary for effective and efficient computer system management. It also features a number of school districts, cities, and counties that use the best practices. In this chapter, we address the following question:

- **What best practices lead to efficient and effective management of computer systems?**

We identified the best practices from a review of computer management literature, including resources on the Web sites of management and security organizations. To validate the best practices, we discussed them with a technical advisory panel of 16 people involved with managing computer systems in Minnesota's cities, counties, and school districts. We also interviewed officials from a small number of school districts, cities, and counties, chosen in part to represent a mix of jurisdiction sizes and geographic locations. Appendix A contains additional information on the methodology we followed for the study.

BEST PRACTICES AND ACTIONS

We identified best practices that are important when evaluating options for managing computer systems and organized them into three groups. As shown in Table 3.1, they deal with computer system policies, staff, and security. The best practices help define what is needed for effectively managing computer systems in ways that optimize the systems' use and control their risks. While these best practices are important for computer systems of all types, local governments with complex computer systems will have additional considerations. Local governments should ensure that the best practices are in place whether the computer system is managed by local government staff, an intergovernmental collaboration, a computer vendor, or some mix.

Best practices for managing computer systems address policy, staffing, and security issues.

Table 3.1: Best Practices for Managing Computer Systems

1. A Framework Should Be in Place to Guide the Management of a Computer System
   - Inventories should clearly identify computer equipment and software, and standards should be set
   - Key policies, procedures, and the current operating environment should be documented
   - Policies and procedures should be communicated to staff
   - Adherence to computer system policies and procedures should be monitored
   - Policies and procedures should be regularly reviewed and updated
2. Knowledgeable Staff Should Maintain and Use the Computer System
   - The expertise of technology staff should be assessed
   - A recruitment and retention process should be in place for technology staff
   - Training for technology staff should be ongoing
   - User training should be available
   - User support should be provided
3. Computer Systems Should be Secure
   - A risk assessment should be conducted and security policies should be based on it
   - User accounts should be managed and procedures should identify who may modify equipment or system data
   - Firewalls and antivirus software should be employed and monitored
   - A disaster recovery plan should be developed and back-up procedures should be conducted
   - The security plan should be tested
   - Trained professionals should plan, monitor, and enforce security

SOURCE: Office of the Legislative Auditor.

1. A Framework Should Be in Place to Guide the Management of a Computer System

The basis for effectively managing a computer system (or part of one) is having a framework that includes inventories of the system's components and policies to guide the system's use.

Inventories Should Clearly Identify Computer Equipment and Software, and Standards Should Be Set

Whoever manages a computer system should have complete inventories of its hardware and software. Good asset management requires an up-to-date inventory of computer system equipment to track what is owned and for financial accounting purposes. The inventory should both describe assets and document equipment configurations. Table 3.2 lists a sample inventory for computer

Table 3.2: Sample Hardware Inventory

A database of hardware inventory might include the following elements:

- Information on the manufacturer, model, and serial number (or some other unique identification number)
- Equipment description (possibly with a menu of predefined choices to preserve consistency) by category, such as desktop computer, laptop computer, or printer
- Comment field (may include a history of who has had the equipment or, in the case of lost or stolen equipment, details of what occurred and pointers for police reports)
- Information on the purchase date and purchase order number to establish time period for the warranty
- Configuration information, including disk size and amount of memory, based on the device machine name, if any
- Internet protocol (IP) name and IP address
- Location code and physical location, such as room number
- User name and ID (does not apply for network and multi-user components)
- Organizational affiliation, such as the department or unit
- Owner history, if applicable
- Usability code or condition (e.g., in current use, ready to reassign, ready to dispose of, scrapped for parts, retired, lost, stolen)

SOURCE: CERT® Coordination Center, *Establishing and Maintaining a Physical Inventory of Your Computing Equipment*, (Pittsburgh: Carnegie Mellon University, March 2000), http://www.cert.org/security-improvement/implementations/i043.02.html; accessed January 30, 2002.

hardware. By documenting software purchases, inventories (along with receipts) help in complying with the legalities of licensing requirements.[1] For licensing compliance, software programs are available to scan computers over the network and create an inventory of all applications residing on those computers.[2] When computer systems change, administrators should update the inventories.

To the extent possible, the manager of a computer system should standardize its hardware and software. Using standards to guide purchasing decisions ensures that new hardware and software satisfy user needs and are compatible with the rest of the computer system.[3] Standards for hardware and software can also simplify user and hardware support because technicians need maintain only one type of computer rather than several.

For example, the **Cloquet Public School District** follows several standards when purchasing computers. For a recent acquisition, the district decided to purchase a

1 Right Track Associates, Inc., "The Asset Management Needs Assessment," *ITToolkit;* www.ittoolkit.com; accessed February 2, 2002.

2 Loretta W. Prencipe and Stephanie Sanborn, "Cutting Costs," *InfoWorld.com* (September 28, 2001); http://staging.infoworld.com/articles/fe/xml/01/10/01/011001feitspend.xml?Template=/storypages/ctozone_story.html; accessed March 15, 2002. Monitoring software use can reduce operating costs, such as the licensing fees saved when unused software is removed from a computer.

3 Gartner Research, "Desktop PC Life: Four Years For The Mainstream," *TechRepublic* (December 19, 2001); www.techrepublic.com/article_guest.jhtml?id=r00320011219ern01.htm; accessed March 15, 2002. Also available from Gartner as *Research Note* T-13-8045.

single type of desktop computer from a single manufacturer, allowing technology staff to maintain them more efficiently. Another standard it followed was to first assess what computing power was actually needed and then match the hardware to the identified computing needs. That is, if computers were only to be used for word processing or basic spreadsheet capabilities, they did not need to be as high powered as others where more complex processing was required. Further, to acquire desktop computers within a limited budget, the district adopted a standard of purchasing refurbished computers for its computer labs, saving approximately $800 per unit. For more information contact Yvette Maijala, Technology Coordinator, at ymaijala@cloquet.k12.mn.us or 218/879-6721.

Key Policies, Procedures, and the Operating Environment Should Be Documented

Computer management programs govern hardware and software use as well as training, security, and user support.

Those who maintain computer systems should follow documented management programs, detailing the ongoing operation and control of the computer system.[4] A management program should contain policies and procedures that govern how the computer network hardware and software will be managed as well as how user support, training, security, and controls on user access will be provided. It should describe priorities for decisions on day-to-day system procedures, such as giving precedence to restoring network operations over installing a new CD drive in a user's desktop computer. Management programs are valuable for increasing productivity, maintaining system stability, and reducing operational costs by limiting computer downtime. Table 3.3 lists elements of a sample management program.

To be effective, management programs should be aligned with the organization's technology needs and contain procedures that are enforceable without being overly restrictive.[5] Because they include standards for computer facilities and security procedures, management programs help protect the safety of technology equipment and data. The cost and detail of a management program should be proportionate to the complexity of the computer system and level of its benefits.

Although the responsibility for setting policies and procedures may vary among jurisdictions, for local governments relying on their own staff to maintain computers, policy makers, technology staff, and end users all have a role to play. Because policies on managing computer systems require decisions on allocating resources, and because they present tradeoffs between the needs of technology staff and those who use the computers to do their work, a local government's top officials should be involved in adopting computer system policies. By contrast, technology specialists should, with input from users, set procedures that both implement the policies and support the needs of staff using the system.

---

4 Right Track Associates, Inc., "IT Management Strategies in Small Business," *ITToolkit;* www.ittoolkit.com; accessed February 2, 2002; Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Organization and Technology in the Networked Enterprise 6th ed.* (NJ: Prentice Hall, 2000), 506-507; and Gartner Research, "Guidelines for the Content of IT Policies," *Research Note* TU-13-9550, July 26, 2001, 1-2.

5 Right Track Associates, Inc., "IT Management Strategies in Small Business," *ITToolkit;* and Gartner Research, "Guidelines for the Content of IT Policies," 1-2.

Policies are needed on many issues, from managing computer assets to planning for disaster recovery.

Table 3.3: Key Management Program Components

Component	Description
Asset Management	Track hardware and software owned and whether they are in use
Technology Standards Management	Set product standards that ensure system reliability and compatibility
Software Licensing Control	Ensure compliance with licensing laws
Systems Management	Ensure that hardware and software configurations are current, documented, and performing as expected
Systems Administration	Ensure that user IDs are current, access is appropriate, and that storage capacity is kept at required levels
Change Management	Ensure that system changes do not interfere with reliable operation and availability
Security Management and Virus Protection	Protect the jurisdiction from data loss and systems damage due to hacking, theft, or virus attacks
Disaster Recovery and Contingency Planning	Protect the jurisdiction in the event of a systems outage or loss of critical data
End-User Support	Resolve technical problems and assist in the use of technology

SOURCE: Right Track Associates, Inc., "IT Management Strategies in Small Business," *ITToolkit;* http://www.ittoolkit.com; accessed January 30, 2002.

Some of the policies in a management program will be driven by state and federal laws. For example, Minnesota's Data Practices Act sets parameters on which data are available to the public, requiring local governments to set policies and establish operating procedures that protect sensitive electronic data. The security-related elements of a computer management program are described in more detail later in this chapter.

The **Robbinsdale Area School District,** which serves more than 13,000 students, developed a technology plan encompassing many elements of a sound computer management program.[6] The plan addresses user training and support, district computer standards, a technology inventory, and technology policies and procedures. For example, in the plan the district identifies specific technology needs, such as the need for additional staff technical training, and it presents strategies to fill the gaps between what is needed and what is available. The plan also differentiates among management duties for different levels of staff. It specifies, for instance, that technology associates within school buildings have responsibilities for installing software and administering local-area networks while district technology personnel coordinate technology classes for staff and plan the district's future technology uses. For more information contact Dennis Beekman, Executive Director of Technology, at dennis_beekman@rdale.k12.mn.us or 763/504-8055.

6 To be eligible for certain technology funding, Minnesota school districts must develop technology plans containing specified information. See the Robbinsdale School District technology plan at www.rdale.k12.mn.us/dist/services/techplan.pdf.

Policies and Procedures Should Be Communicated to Staff

Technology policies and procedures should be communicated to staff.

The managers of a computer system should ensure that staff using the computers know about relevant policies and procedures, including the priorities that guide technology staff managing the computer system. They should communicate policies and procedures to new employees when they are hired as well as to current employees when changes occur.[7] Policies and procedures should be available in printable form, such as e-mail, so that employees can refer to them when needed. For large policy changes that are likely to be controversial, giving users an opportunity to voice questions and discuss issues may be useful.

Policies should cover security measures, such as requiring users to change passwords periodically.

The city of **Fergus Falls** developed policies to communicate acceptable computer uses to city staff. A committee of managers and staff jointly developed the policies, and the city council approved them. The policy document covers security procedures, such as forbidding users to share passwords and requiring them to change passwords every 90 days. It describes the city's software licensing agreements and prohibits the use of employee-owned software for city work unless approved in advance. Among other items covered are procedures related to virus scanning and downloading files or software from the Internet. All employees who use computers in the course of their work receive the document. One of the city's personnel policies requires employees to affirm with their signature that they have read the computer use policy. Information systems staff supplement the written guidelines with various procedures, such as setting up new user accounts for employees who have forgotten their passwords and using inventory software to track which software applications reside on the computer network. For more information, contact Tony Neville, Information Systems Manager, at tony.neville@ci.fergus-falls.mn.us or 218/739-2251 or Kirsten Danielson, Information Systems Programmer, at kirsten.danielson@ci.fergus-falls.mn.us or 218/739-2251.

Adherence to Computer System Policies and Procedures Should Be Monitored

Local governments should ensure that their own users adhere to computer policies and procedures. Through monitoring, local governments help employees avoid using their computers in ways that could create negative impacts on the computer

---

7 Mandy Andress, "Effective Security Starts with Policies," *InfoWorld.com* (November 16, 2001); www.infoworld.com/articles/tc/xml/01/11/19/011119tcpolicy.xml; accessed March 15, 2002. Also see Step 6 for planning and implementing a management program in *IT Toolkit*, "IT Management Strategies in Small Business."

system.[8] For example, some jurisdictions have policies prohibiting users from downloading programs off the Internet, and monitoring helps ensure that users comply. Some monitoring may be done with software applications, such as those that strip certain attachments from all e-mail messages to prevent harmful files from corrupting the system.[9] Other monitoring may be done by assigning specific enforcement responsibilities to technology staff.

Policies and Procedures Should Be Regularly Reviewed and Updated

Those who manage computer system services should occasionally review and update the system's policies and procedures.[10] For example, because of ever changing risks to the computer system, security policies must be periodically updated to remain timely and effective. Computer users should have input on updating policies and procedures, even when external providers are managing the computer system and developing the procedures. Surveying users is one way of systematically allowing them to suggest changes and identify computer system problems.

2. Knowledgeable Staff Should Maintain and Use the Computer System

For optimal performance, computer systems require properly trained staff to operate and maintain them. In addition, computer users need training and support to use the systems efficiently and responsibly.

The Expertise of Technology Staff Should Be Assessed

Computer systems require properly trained staff for optimal performance.

Managers of computer system services should know the strengths of their information technology (IT) staff, and local governments must understand the extent of these strengths when considering computer management options. Sophisticated technology services require a high level of staff expertise to ensure that the computer system performs correctly. In evaluating management options, local governments should assure themselves that the providers' staff expertise is adequate for local computer system needs.

When evaluating their own technology staff needs, local governments should consider such factors as the complexity and sophistication of the computer system, dependence on external providers, size of the jurisdiction, dispersion of equipment around the jurisdiction (including remote sites), the degree to which

---

8 Richard Mackey and Jonathan Gossels, "Mastering Fundamentals, Part 3," *Information Security* (March 2000); www.infosecuritymag.com/articles/march00/features3.shtml; accessed March 15, 2002.

9 Andress, "Effective Security Starts with Policies." Also see Step 7 for planning and implementing a management program in *IT Toolkit*, "IT Management Strategies in Small Business."

10 Mackey and Gossels, "Mastering Fundamentals, Part 3."

the government is centralized, and the number of users.[11] Because there is no formula to establish "correct" IT staffing ratios, local governments have to consider these factors in light of all the IT work they need to accomplish, which means balancing the sometimes competing needs of maintaining computer security and supporting end users. Identifying gaps in computer system support needs will also help identify necessary staff training.

The number of technology staff should reflect what needs to be accomplished.

A Recruitment and Retention Process Should Be in Place for Technology Staff

Managers of computer systems should be aware of the need to actively recruit and retain technology staff. For example, internships or partnerships with local educational institutions can help recruit potential employees. Local governments need to determine whether the computer system managers they are considering follow recruitment and retention practices. Local governments that choose to manage systems with their own personnel will be competing with private business for skilled workers, and they should recognize that qualified IT staff can be difficult to find and keep (although this varies with labor market conditions).[12] Local governments often face a special challenge because of relatively lower pay scales for IT staff when compared with the private sector.

Training for Technology Staff Should Be Ongoing

Because technology evolves quickly, IT staff need training on an ongoing basis to provide efficient and effective services.[13] In considering computer management options, local governments should determine whether ongoing training is available to technology staff. A variety of information for keeping technology staff updated is available on the Internet. For instance, the CERT® Coordination Center at Carnegie Mellon University offers a variety of security-related resources on-line. It recommends that IT staff review on-line resources daily to learn about new developments in computer system security and prepare themselves to take action as necessary.[14]

---

11 Gartner Research publishes survey-based ratios of staff-to-users and guidelines for various services, although most are applicable to private businesses. For example, staffing for security is a function of system complexity and the likelihood it will change. See Gartner Research, "Distributed Security Staffing Levels," *Research Note* TG-06-4474, November 17, 1998. Guidelines on ratios of PC support staff range from 1 staff for 80 PCs in entities with high technical requirements to 1 for 1,100 PCs in entities with low technical requirements; see Gartner Research, "PC Staffing Guidelines - Taking Out the Guesswork," *Research Note* TG-08-6052, October 25, 1999.

12 Gartner Research, "2002: Government in Transition," *Research Note* AV-15-1207, December 21, 2001. Gartner Group estimates that through 2007, 75 percent of government agencies will face chronic staff shortages unless they implement a comprehensive staffing plan that addresses compensation, civil service reform, and expanded use of outsourcing.

13 Gartner Research, "The Justification of IT Training," *Research Note* DF-11-3614, July 10, 2000, 2. Gartner Group quantifies the relationship between training and productivity for IT professionals and end users, suggesting that each hour of training saves five hours of time spent experimenting, requesting help, and reworking tasks.

14 CERT® Coordination Center, "Maintaining Currency by Periodically Reviewing Public and Vendor Information Sources," (January 2001); www.cert.org/security-improvement/implementations/i040.01.html; accessed March 15, 2002. The CERT® Coordination Center (www.cert.org/nav/index.html) is a major reporting center for Internet security problems and is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Technology staff should receive ongoing training.

For example, the **Robbinsdale Area School District** uses salary incentives to encourage ongoing training of its technology staff. The district's technology and media services department supports about 4,500 computers in the district's schools and administrative buildings, requiring high levels of technical expertise. To keep staff skills up-to-date, the district has included a "certification stipend" in employee contracts. The stipends offer financial rewards to technology staff who successfully complete technical certification programs as part of their approved training plans. In 2001 the stipends amounted to $6,000. The district will also pay for some of the technology-related training, which totaled $11,000 that year. These incentives help to hone staff skills, and retain the district's 18-member technical staff. For more information contact Dennis Beekman, Executive Director of Technology, at dennis_beekman@rdale.k12.mn.us or 763/504-8055.

User Training Should Be Available

Local governments should ensure that whoever manages the computer system has an adequate plan for training local government staff expected to use the system. Training saves time that users would otherwise spend experimenting with software applications. It increases productivity by minimizing the need to rework tasks.[15] Good training also reduces demand for support from IT staff. User training should focus on "how-to" issues, such as how to make effective use of software capabilities. In addition, users need to be educated on the importance of computer system security.

The city of **Lakeville** has used an innovative way of training its computer users. Lakeville has contracted with a technology-training firm to provide user training when the city upgrades software. When the city upgraded its productivity

15 Gartner Research, "The Justification of IT Training," 2.

software, the training firm brought to city hall a "mobile computer lab" consisting of several laptops, connected them to the city network, and provided user training based on the city's existing documents. Using their own computer files, employees typically learned the software more quickly and gained a deeper understanding of its utilities. For more information contact Danny Barth, Information Systems Manager, at dbarth@ci.lakeville.mn.us or 952/985-2641.

User Support Should Be Provided

In addition to user training, local governments should ensure that computer system managers offer an appropriate type and level of ongoing user support. New users will need support as they become acquainted with the computer system, and experienced users will require support when new applications are added or other changes are made.[16] The system manager's plan for supporting users should address both what will be supported (such as hardware and applications) and how it will be supported (such as methods to resolve technical problems). Because users learn in different ways and need help at different times, a variety of help options may be necessary, such as those listed in Table 3.4.[17] Documenting the key support information provides consistent information from user to user.

The **Robbinsdale Area School District** uses an internal computer network to provide user support. The district's Technology and Media Services Department

Supporting the users of a computer system may require multiple strategies.

Table 3.4: User Support Strategies

- Awareness meetings to introduce computer system goals and features
- Easy to follow, one-page "cheat sheets" for common activities
- Small group training, review, and support sessions
- Frequently-asked question and answer brochures
- On-line help features including discussion groups, e-mail, video, and intranets
- Designated learning time for new employees
- Individual tutoring or peer tutoring
- A help newsletter
- Full-scale documentation manuals
- Videotaped step-by-step instruction
- Computer system maps presented graphically and in color
- A staffed help desk

SOURCE: Center for Technology in Government, *Tying a Sensible Knot* (Albany, NY: Center for Technology in Government, 1997), 77; http://www.ctg.albany.edu/resources/pdfrpwp/iisfnlrp.pdf; accessed February 14, 2002.

16 U.S. Department of Justice, Justice Management Division, *The Department of Justice Systems Development Life Cycle Guidance Document Chapter 11: Operations And Maintenance Phase* (Washington, D.C.: Department of Justice, March 2000), 1; www.usdoj.gov/jmd/irm/lifecycle/ch11.htm; accessed February 14, 2002. Also see Derek Simmel *et al.*, *Securing Desktop Workstations* (Pittsburgh: Carnegie Mellon University Software Engineering Institute, February 1999), 46; www.sei.cmu.edu/pub/documents/sims/pdf/sim004.pdf; accessed March 15, 2002.

17 Center for Technology in Government, *Tying a Sensible Knot: A Practical Guide to State-Local Information Systems* (Albany, NY: Center for Technology in Government, June 2001), 77; www.ctg.albany.edu/resources/pdfrpwp/iis1.pdf; accessed February 14, 2002.

has created information modules that staff can access over the district's intranet. For example, one module instructs staff on changing passwords. The district supplements its modules with "pdf" files from vendors that provide information on different software applications.[18] Technicians located at the school buildings also offer user support. The district expanded its user-support options because teachers had difficulty finding time outside of the classroom to help them take full advantage of available technology. For more information contact Dennis Beekman, Executive Director, Technology and Media Services at dennis_beekman@rdale.k12.mn.us or 763/504-8055.

3. Computer Systems Should Be Secure

Interference with the security and reliability of government information threatens governments' effectiveness and credibility and increases system costs. Managing computer systems means understanding and controlling risks, which is necessary whether computers are managed by in-house staff, computer vendors, or intergovernmental technology collaborations.

A Risk Assessment Should Be Conducted and Security Policies Should Be Based on It

Managers of computer systems should have security policies based on identified risks. Whether local governments use external providers or manage their own computers systems, they should understand the risks inherent to the system. Risk is a function of the value of the computer assets, the computer system's vulnerability, the likelihood and possible outcomes of an attack, and the acceptable cost that managers are willing to bear.[19] That is, high-value computer systems that are connected to the Internet and integral to a government's ability to perform its duties face higher risks than others.

Computer security risks arise from both inside and outside an organization.

Security risks come from both outside and inside local governments and may threaten physical property or the availability and quality of data. For example, opening e-mail attachments without protecting against computer viruses exposes an organization's data and computers to possible hazards.[20] Statistics kept since 1990 by the CERT® Coordination Center at Carnegie Mellon University show computer security incidents more than doubling each year.[21] Many risks come from disgruntled employees within an organization or from those who have recently left the organization.

Consequently, computer system managers should assess the risks to their systems. Results of the risk assessment will help in understanding the systems' vulnerabilities and developing strategies to mitigate them. Local governments

18 A "pdf" file format captures a printed document as an electronic image that can be viewed by anyone using Acrobat Reader, which is available as a free program at www.adobe.com/support/downloads/main.html.

19 Gary C. Kessler, "Gary Kessler's Musings About Network Security," *Vermont Telecom News* (July 2001); www.vtac.org/newsletter.htm; accessed March 15, 2002.

20 A virus is programming code that automatically spreads itself, potentially infecting files, specific applications, or the computer system itself. Unknown to users, viruses can be present on a diskette or CD, transmitted as attachments to an e-mail note, or downloaded from files off the Internet.

21 See www.cert.org/stats/ for specific statistics from the CERT® Coordination Center.

should understand the risks involved with their own computer systems as well as those of any external providers with whom they do business. Depending upon a computer system's size and complexity, risk assessments can be expensive, but free on-line resources are also available.[22]

Computer security policies should address identified risks.

A local government should ensure that whoever manages its computer services has security policies based on the results of a risk assessment. The goal of the security policy is to prevent unauthorized access, theft, or alteration of information systems, and the level of security should be commensurate with the identified risks. Security policies and procedures should identify what can go wrong, determine measures to reduce the likelihood of problems, lay out steps for detecting and responding to security breaches, and specify who will undertake the steps when needed. Because of the need to balance security against issues of privacy, access, and costs, it is important to have senior officials of an organization involved with setting security policies.[23]

In 2001, **Anoka County** contracted for an extensive assessment of its computer network. One focus of the assessment was security, and the second addressed network infrastructure performance. As part of the security assessment, consultants evaluated internal and external threats to the network through firewall "penetration" testing (trying to circumvent security controls to gain access to the computer system) and attempting to gain physical access to computers housed at a particular county facility. They tested servers looking for specific risks, and they reviewed the county's existing security policies and procedures. As a result of the assessment, information systems staff developed a plan and have been systematically implementing responses to the consultants' observations. Part of the response was updating certain security policies, such as formally documenting procedures for data backups and off-site storage of backups. For more information contact Cindy Kevern, Anoka County Director of Information Services, at cindy.kevern@co.anoka.mn.us or 763/323-5368.

User Accounts Should be Managed and Procedures Should Identify Who May Modify Equipment or System Data

Managers of computer systems should require user accounts that specify who can access certain computers and data.[24] Local governments should verify that these controls are in place when evaluating computer management options. In most cases, limited numbers of staff should have access rights to production programs and data. For managing security risks due to employee use of the system, computer system managers should set procedures that define acceptable and unacceptable user behavior. For example, a policy may prohibit employees from downloading Internet files to the local network. Table 3.5 lists possible elements

---

22 The Center for Internet Security's benchmarks for testing operating system security are at www.cisecurity.org/. The National Institute of Standards and Technology has a guide for conducting IT risk management at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. Microsoft TechNet produces *Security Planning*, which includes a section on basic risk assessment at www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secplan.asp.

23 Harvard Policy Group on Network-Enabled Services and Government, *Eight Imperatives for Leaders in a Networked World Imperative 5: Protect Privacy and Security* (Cambridge, MA: Kennedy School of Government, 2001), 9.

24 Simmel *et al.*, *Securing Desktop Workstations*, 16.

Table 3.5: Elements of a Computer Use Policy

A computer use policy should define the extent to which users may:

- Make hardware changes
- Install or remove software
- Perform work outside the ordinary scope of business or their job description
- Use specific network services, such as e-mail and Internet access
- Transmit information across the network, including e-mail, attachments, and downloaded files
- Make configuration changes if employees are given higher levels of access

Plus, the policy should describe how users are to operate the computer in line with specific security requirements, such as using a password-protected screen saver or turning the computer off at the end of the work day.

SOURCE: Derek Simmel, *et al.*, *Securing Desktop Workstations* (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, February 1999), 45-46; http://www.sei.cmu.edu/pub/documents/sims/pdf/sim004.pdf; accessed February 14, 2002.

of a computer use policy. The policy should be developed with user and IT staff input and updated as needed to reflect computer system changes.

Another control over internal access to a computer system is requiring user authentication through passwords. Procedures for password administration should address closing dormant accounts, requiring difficult-to-crack passwords, changing passwords periodically, and limiting the number of times a user may retry entering a password.[25] Such procedures are important because loosely controlled passwords may provide hackers with easy points of access to the computer system. Table 3.6 includes common elements of a password policy. Managers should test the rigor of user passwords with any of several password-cracking tools.[26] They can use other automated tools that prevent

Loosely controlled passwords may provide hackers with easy points of access to the computer system.

Table 3.6: Elements in a Password Policy

- **Length**: Set a minimum length for passwords, such as eight characters.
- **Complexity**: Require a mix of characters, such as requirements to contain both uppercase and lowercase letters and at least one nonalphabetic character.
- **Aging**: Determine how long a password may remain unchanged. For instance, require users to change their passwords every 30 to 45 days.
- **Reuse**: Decide whether a password may be reused to prevent employees from repeatedly using the same passwords. Limit the number of times a person may reenter passwords to prevent unauthorized users from gaining access to the system.
- **Authority**: Determine who is allowed to change passwords and delete user accounts when users leave an agency.

SOURCE: Derek Simmel, *et al.*, *Securing Desktop Workstations* (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, February 1999), 16; http://www.sei.cmu.edu/pub/documents/sims/pdf/sim004.pdf; accessed February 14, 2002.

25 *Ibid.*, 16.

26 For a discussion of several password-cracking tools, see Greg Shipley, "Tools From the Underground," *Network Computing*, (May 29, 2000); www.networkcomputing.com/1110/1110ws1.html; accessed February 14, 2002.

unauthorized users from reentering multiple passwords in attempts to gain access to the system.

Sensitive data require higher levels of security.

Passwords offer a first level of authenticating users, but for high-risk systems, managers may need to consider second-level authentication controls, such as requiring multiple passwords. Other controls include tokens, keys, and biometric devices that recognize a person based on biological characteristics, such as fingerprints.[27] For sensitive information, such as confidential medical records, computer system managers need to prevent unauthorized access to the data, for example, by encrypting the data.[28]

In the city of **Lakeville**, employees' access to computer files and directories is limited according to their job duties. The computer network allows employees to use only those files to which their user account has been granted access rights. Employees are assigned user names and must use passwords to gain access to the computer network. Every 90 days, users are required to change their passwords, and they are not allowed to reuse any of their five previous passwords. In addition, the city's computer system policies contain guidelines to help employees protect data and the network. For example, one procedure instructs users to scan all files for virus infections before installing them on city-owned computers. Others include a recommendation to log off the network at the end of each workday and a proscription against using any user name other than the one assigned. Regarding use of the Internet, the policies spell out what uses are appropriate, and they also discuss security procedures. As an example, a policy prohibits the sharing of user IDs and passwords for gaining access to Internet sites and forbids installing software from the Internet unless done under the direction of technology staff. For more information contact Danny Barth, Information Systems Manager, at dbarth@ci.lakeville.mn.us or 952/985-2641.

Controlling physical access to the computer systems is also important. Computer system managers should secure computer equipment and network connections in locked facilities away from heavy foot traffic.[29] As an example, the city of **Plymouth** secures its network servers and other critical equipment in a

Facilities can help protect technology investments.

27 Simmel *et al.*, *Securing Desktop Workstations,* 7.

28 *Ibid.*, 20. Also see Julia Allen *et al.*, *Securing Network Servers* (Pittsburgh: Carnegie Mellon University Software Engineering Institute, April 2000), 50; www.sei.cmu.edu/pub/documents/sims/pdf/sim010.pdf; accessed February 14, 2002. Encryption involves converting data into a form that is not understood by unauthorized people.

29 Simmel *et al.*, *Securing Desktop Workstations*, 43-44.

large, well-ventilated room with windows that face into a general work area. Technology staff can easily view all activity in the computer room. The work area is off-limits to the public and the computer room is locked at all times. For more information contact Jeff Hohenstein, Information Technology Service Manager, at jhohenst@ci.plymouth.mn.us or 763/509-5060.

Firewalls and Antivirus Software Should Be Employed and Monitored

Computer networks of any size are vulnerable to external and internal security incidents. As a first line of defense, local governments should ensure that whoever manages a computer system uses antivirus software and firewalls (hardware and software placed between the Internet and a computer network to prevent unauthorized access).[30] However, installing the equipment and software is only the beginning: To protect computer systems and data from constantly evolving threats, computer system managers must ensure that staff actively monitor firewalls and regularly use antivirus software.[31]

Because computer threats continue to evolve, updated antivirus programs are essential.

In addition, administrators must keep firewalls and antivirus software up-to-date.[32] Updating is a continuous process as new threats occur daily. Firewalls often need "patches" and upgrades to operate effectively.[33]

Depending on a computer system's identified risk levels, it may need applications that detect intrusions. Intrusion detection systems identify attempts to compromise a computer or network. The attacks can come from outside attackers using the Internet or unauthorized insiders. Intrusion detection systems must be part of a larger framework of IT security because they are virtually useless unless monitored and analyzed.[34]

---

30 Antivirus or virus "scanning" software works by comparing the data on a computer against a collection of virus "signatures." Each signature is characteristic of a particular virus, and when the scanner finds data in a file or e-mail that matches the signature, it concludes that it has found a virus. Information and guidelines on firewalls are available from the National Institute of Standards and Technology at http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf. Readers who want periodic bulletins on technology security, such as firewall policy and IP security, should view http://csrc.nist.gov/publications/. The CERT® Coordination Center publishes a module on deploying firewalls. See William Fithen, Julia Allen, and Ed Stoner, *Deploying Firewalls* (Pittsburgh: Carnegie Mellon University Software Engineering Institute, May 1999); www.sei.cmu.edu/pub/documents/sims/pdf/sim008.pdf.

31 Microsoft Security Response Center, "The Ten Immutable Laws of Security: Law 8," *Microsoft TechNet* (Undated); www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/10imlaws.asp; accessed March 15, 2002. Also see Gartner Research, "Staffing for Firewall Support," *Research Note* TU-05-2362, September 10, 1998, 2. Plus, free on-line sources are available to test firewalls once installed, such as at www.grc.com.

32 Antivirus software can only scan for the viruses it knows about, and new viruses are created every day. According to the Microsoft Security Response Center, an out-of-date virus scanner is only marginally better than no virus scanner at all. Microsoft Security Response Center, "The Ten Immutable Laws of Security: Law 8." Also see Mackey and Gossels, "Mastering Fundamentals, Part 2," *Information Security* (February 2000); www.infosecuritymag.com/articles/february00/features3.shtml.

33 A patch is a quick "fix" to repair software. The fix is often temporary until developers find a better solution that is included in the next product release.

34 Peter Mell, Auerbach Analysis, "Intrusion Detection: A Guide To The Options," *TechRepublic* (Nov 6, 2001); www.techrepublic.com/article.jhtml?id=r00620011106ern01.htm&src=search; accessed 01/08/02.

Lakeville is an example of a city that runs antivirus software on all of its servers and computer workstations. Technology staff there have responsibility for keeping antivirus software current. When a virus is detected, the city's technology staff are alerted and the user is locked out of the network. The city also uses two firewalls to protect its information systems. Lakeville is a member of the intergovernmental computer collaboration LOGIS, to which all of the city's e-mail is routed. At LOGIS the firewall and "gateway" server scan e-mail for viruses and filter it for potentially troublesome e-mail attachments and content. Lakeville's e-mail then passes to the city's own firewall and e-mail server. The city's server is configured to accept traffic coming only from the LOGIS e-mail gateway and no other system. In the city's computer system, filters actively watch for and delete certain attachments. With this configuration, if the antivirus software fails to detect a newly released virus, LOGIS is able to stop the virus from spreading by closing the e-mail gateway. For more information contact Danny Barth, Information Systems Manager, at dbarth@ci.lakeville.mn.us or 952/985-2641.

A Disaster Recovery Plan Should Be Developed and Backup Procedures Should Be Conducted

Local governments must ensure that whoever manages the computer system has a plan to continue computer services in case of an emergency or disaster.[35] Having a clearly documented recovery plan is critical to successfully resuming computer services following a disruption. Table 3.7 lists some key activities for developing a plan. Once in place, the disaster recovery procedures should be tested to ensure that they work and to help avoid unexpected problems.[36]

Local governments should store backed-up data at a second site.

Data backups are an important part of the disaster recovery plan. Properly done, they allow administrators to restore data and system operations following security breaches or other accidents. Providers should develop backup procedures, select and install backup tools, schedule backups, and confirm that backups are successful. Storing backed-up data offsite ensures that the data are available when needed, even if fire or other disaster strikes the facility that houses the computer system.[37]

Data backups and disaster-recovery plans should be part of broader plans to restore the local governments' core functions, should they be interrupted. As with disaster-recovery planning, jurisdictions should (1) understand what incidents (e.g., power failure, fire, hardware malfunction) could occur, (2) measure the impacts such incidents would have on various work processes, (3) set priorities

---

35 Matt Sarrel, "Building a Disaster Recovery Plan," *PC Magazine* (January 15, 2002); www.pcmag.com/article/0,2997,s%253D1579%2526a%253D19894,00.asp; accessed March 15, 2002. The disaster recovery plan may be part of a larger business recovery plan that goes beyond computer needs to include steps for restarting service delivery.

36 Justice Management Division, *The Department of Justice Systems Development Life Cycle Guidance Document Chapter 11: Operations And Maintenance*, 2.

37 Allen *et al.*, *Securing Network Servers*, 41-43. Also see Karen J. Bannan, "Be Prepared," *PC Magazine* (January 15, 2002); www.pcmag.com/article/0,2997,s%253D1579%2526a%253D19894,00.asp.

Local governments should plan how they will restore computer operations in the event of a disaster.

Table 3.7: Activities in Developing a Disaster Recovery Plan

- Secure support from senior management for developing the plan
- Assess what needs to be saved and for how long
- Assign priorities to operations to determine what should be restored first
- Determine procedures for electronic data backup including:
  - Developing a file backup and restoration plan that specifies procedures and type of media
  - Selecting technology, such as use of a virtual private network or the Internet
  - Developing a schedule on frequency and timing of data backups
  - Requiring off-site data storage
  - Providing security for the backup data
- Create a comprehensive written plan that lists who is responsible for each step of the recovery
- Develop test procedures
- Install file backup tools for electronic data
- Confirm that data are collected as planned and can be restored as needed
- Reassess the plan whenever there are changes to infrastructure
- Reassess backup methods when technology changes

SOURCES: Matt Sarrel, "Building a Disaster Recovery Plan," *PC Magazine* (January 15, 2002); http://www.pcmag.com/article/0,2997,s%253D1579%2526a%253D19894,00.asp; accessed March 15, 2002; Harish Setty, *System Administrator Security Best Practices* (SANS Institute, August 16, 2001); http://rr.sans.org/practice/sysadmin.php; accessed March 15, 2002; Karen J. Bannan, "Be Prepared," *PC Magazine* (January 15, 2002); http://www.pcmag.com/article/0,2997,s%253D1579%2526a%253D19894,00.asp; accessed March 15, 2002; Julia Allen, *et al.*, *Securing Network Servers* (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, April 2000), 41-43; http://www.sei.cmu.edu/pub/documents/sims/pdf/sim010.pdf; accessed February 14, 2002.

among which work processes need to be restored first, and (4) define the tasks that need to be undertaken to restore work processes to predisaster levels.[38]

The Security Plan Should Be Tested

System administrators should continually monitor and periodically audit security procedures to ensure that computer systems meet security needs.[39] When assessing computer management options, local governments should verify that security procedures have been tested. Because technology changes rapidly and hackers look for new attacks as old vulnerabilities are corrected, reviewing and testing security measures should be ongoing.

Beyond testing security procedures, managers of computer services should have an independent, third-party review of their security plans. Research shows that the most effective way of understanding security vulnerabilities involves tests

38 Gartner Research, "Top Concerns of Government Business Continuity Planners," *Research Note* QA-13-5355, June 19, 2001, 2-3.

39 Andress, "Effective Security Starts with Policies."

taken independently of the system when those being tested do not know the test will occur.[40]

Security testing should occur when those being tested are unaware that the test is underway.

Concerns about external threats motivated **Mille Lacs County** to undertake an independent security review of its computer system in 2001 for about $8,000. The reviewers also assessed internal vulnerabilities. Recommendations based on the review, such as addition of a firewall, are being implemented over time as the county's budget allows. The county may consider redoing the review every few years to keep up with new threats and changes to the county's computer system. For more information contact Michelle Malley, Information Services Director, at michelle.malley@co.mille-lacs.mn.us or 320/983-8276.

Trained Professionals Should Plan, Monitor, and Enforce Security

Whoever manages the computer system must have staff trained to protect it.[41] Technology staff need special expertise to plan adequate security, regularly monitor security measures, and take appropriate steps when security breaches occur. Because security concerns are ever changing, it is especially important that technology staff remain current on these issues, and many on-line resources are available to this end.[42]

---

40 Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (Washington, D.C.: National Academy Press, 2002), 17.

41 Microsoft Security Response Center, "The Ten Immutable Laws of Security: Law 10."

42 The CERT® Coordination Center has information on assessing risks and best practices at www.cert.org/nav/index_green.html. The center also includes an extensive list of resources at www.cert.org/other_sources/ that includes links to network security information and guides, security related groups, U.S. government resources, a glossary, and tools for secure system administration. The Computer Security Resource Center of the National Institute of Standards and Technology at http://csrc.nist.gov/ covers many issues and has a useful newsletter. The ITToolkit (Right Track Associates, Inc. at www.ittoolkit.com) has a variety of resources suitable for large and small organizations. The Microsoft TechNet Security Center includes a list of reports and best practices on a variety of security topics at www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp. The SANS Institute's Information Security Reading Room has hundreds of articles in more than 50 categories, including a lengthy article on model security policies at http://rr.sans.org/index.php. Also see the Institute's article *The Twenty Most Critical Internet Security Vulnerabilities*, (October, 2001) at www.sans.org/top20.htm. The "Tech Library" at Network Computing (part of the TechWeb Business Technology Network) has many research articles on risk management, encryption, and data and network security at http://techlibrary.networkcomputing.com/. Managers can check for specific vulnerabilities using tools like the ICAT Metabase, a searchable list of vulnerabilities of various hardware and software with links to patch information, which can help system administrators evaluate the security of system components at http://icat.nist.gov/icat.cfm.

Study Methodology

APPENDIX A

This appendix explains the process we followed to conduct the best practices review of managing computer systems. It describes the steps we took, the timeline we followed, and the involvement of local government representatives.

BACKGROUND RESEARCH

To explore issues relevant to managing computer systems, we gathered information from a variety of sources. We began with an extensive review of literature and Web sites, reviewing materials from professional associations, academic and private research centers, and other groups with expertise in computer system management, such as Gartner, Inc. and the CERT® Coordination Center at Carnegie Mellon University.

At the beginning of the study in June 2001, we held a roundtable discussion to help define the scope of the review. We invited individuals representing a variety of viewpoints, including administrators and information technology managers from school districts, cities, and counties; state officials, including the Office of Technology; legislators and legislative staff; and others interested in managing computer systems. At this meeting, 26 participants offered ideas.

To supplement our background research, we conducted personal interviews. We visited and interviewed representatives of most intergovernmental computer collaborations in the state, including three county groups, one city consortium, a school district collaborative, two service cooperatives, and two regional management information centers. Those we did not visit in person were interviewed via telephone or electronic mail. We also interviewed state officials about the state's role in providing a telecommunications infrastructure backbone.

We participated in seminars and Web-based training on computer management, with a particular focus on digital security. Seminars included a National State Auditor Association conference on information technology security in September 2001 and the Minnesota Government Information Technology Symposium in December 2001. Web-based events included sessions on computer system architecture and security.

TECHNICAL ADVISORY PANEL

Early in the project we formed a technical advisory panel to provide expertise and comment on draft materials throughout the review. As shown in Table A.1, the

Table A.1: Technical Advisory Panel Members, 2001-2002

Merton Auger, City Administrator, City of Buffalo

Jim Campbell, Information Technology Director, Dakota County

Barbara Gallo, Technology Services Director, League of Minnesota Cities

Mike Garris, Director, Local Government Information Systems (LOGIS)

Tom Hannon, Information Technology Director, City of St. Cloud

Bob Hanson, Information Technology Director, Hennepin County

Doug Johnson, Technology Administrator, Mankato Area Schools

Bob Knafla, Information Systems Director, Sherburne County

Fred Logman, Chief Information Director, Department of Information Services, Ramsey County

Marcia Love, Superintendent, Plainview Public Schools

Rhonda Lynch, Information Services Director, Carver County

Gail Miller, County Recorder, Renville County

Rae Montgomery, Extension Educator, University of Minnesota Extension Service

Patrick Plant, Director of Technology, Anoka-Hennepin Independent School District #11

Mike Ryan, System Architect, Office of Technology, Minnesota Department of Administration

Lee Whitcraft, Co-Executive Director, Technology and Information in Education Services (TIES)

16-member panel consisted mainly of county, city, and school district staff who were either information technology professionals or otherwise involved in technology issues. They came from jurisdictions representing a mix of sizes and geographic regions. Other members represented the state's Office of Technology, the University of Minnesota Extension Services, intergovernmental computer collaborations, and the League of Minnesota Cities.

Panelists volunteered their time for five meetings to offer their feedback as the study progressed. They reviewed and commented on the draft report. We are grateful to panel members for their advice and help. Panel members may or may not agree with the recommendations of our study, and the Legislative Auditor's Office remains responsible for the report's contents.

INDICATORS OF PERFORMANCE FOR MANAGING COMPUTER SYSTEMS

To help identify effective practices for managing computer systems, we researched guidelines and standards recommended by organizations involved in computer system management and Internet security. From this research, we compiled indicators of performance related to effectively planning and

maintaining computer systems. In September 2001, our technical advisory panel reviewed the indicators, and we later modified some based on its feedback.

The best practices for successful computer system management discussed in Chapter 3 evolved from the performance indicators. In November 2001 our technical advisory panel reviewed and commented on the best practices, and we modified them accordingly.

SURVEY METHODOLOGY

As part of a related study on e-government, we surveyed counties, cities, and school districts to understand the degree to which they offer e-government. Although the survey was primarily on e-government, it included several questions about local governments' use of computers and computer networks. We also asked about arrangements for daily maintenance of the computer system, including reliance on in-house staff, vendors, or computer collaborations. Copies of the survey instruments and their aggregate results are available on our Web site at http://www.auditor.leg.state.mn.us/ped/2002/pe0209.htm.

We developed two formats for the survey and gave respondents the choice of either completing it on-line using the Internet or filling out a paper version and returning it by mail. The survey questions were identical in both formats. Before mailing the surveys, we pretested survey questions as well as the use of the on-line survey with members from our technical advisory panel and with other staff in our office.

In early October 2001, we mailed the questionnaires along with cover letters explaining the study and requesting recipients' help. The surveys went to either information technology directors or county administrators (or their equivalent) in each of the 87 counties.

For cities and school districts, we selected random samples based on size and geographic region. To survey cities and school districts, we grouped them by six geographic regions. Within each region, we further grouped first cities and then school districts by size to achieve a balance of smaller, mid-sized, and larger jurisdictions. From within these groups divided by region and then by size, we randomly selected 521 of Minnesota's 854 cities and 310 of 345 school districts. We sent the city surveys to information technology managers or other technology contacts; where we did not have names for those individuals we mailed the survey to city managers, administrators, or clerk-treasurers and asked them to forward the survey to the appropriate persons. The school district surveys went to technology coordinators in districts where we had those coordinators' names; otherwise, the surveys went to district superintendents with requests to forward the survey to the appropriate individuals.

The deadline for completing surveys was October 23, 2001. We mailed follow-up letters and surveys to counties, cities, and school districts that had not responded by the first due date and extended the deadline to November 6, 2001.

Seventy-eight of the 87 counties responded to the survey (with 44 of them responding on-line), for a response rate from counties of 89.7 percent. Table A.2 lists the counties that responded to the survey. We received responses from 429 of the 521 cities surveyed (with 117 responding on-line), for a city response rate of

Table A.2: Counties Receiving Survey

*Aitkin County	*Freeborn County	*Meeker County	*Scott County
*Anoka County	*Goodhue County	*Mille Lacs County	*Sherburne County
Becker County	*Grant County	Morrison County	*Sibley County
*Beltrami County	*Hennepin County	Mower County	*Stearns County
*Benton County	Houston County	*Murray County	*Steele County
*Big Stone County	*Hubbard County	*Nicollet County	*Stevens County
*Blue Earth County	Isanti County	*Nobles County	*Swift County
*Brown County	*Itasca County	*Norman County	*Todd County
*Carlton County	*Jackson County	*Olmsted County	*Traverse County
*Carver County	*Kanabec County	Otter Tail County	*Wabasha County
*Cass County	*Kandiyohi County	Pennington County	*Wadena County
*Chippewa County	*Kittson County	*Pine County	*Waseca County
*Chisago County	*Koochiching County	*Pipestone County	*Washington County
Clay County	*Lac Qui Parle County	*Polk County	*Watonwan County
*Clearwater County	*Lake County	*Pope County	*Wilkin County
*Cook County	*Lake of the Woods County	*Ramsey County	*Winona County
*Cottonwood County	Le Sueur County	*Red Lake County	*Wright County
*Crow Wing County	*Lincoln County	*Redwood County	*Yellow Medicine County
*Dakota County	*Lyon County	*Renville County	
*Dodge County	*Mahnomen County	*Rice County	
*Douglas County	*Marshall County	*Rock County	NOTE: Asterisks (*) depict counties from which we received completed surveys in time for analysis.
*Faribault County	*Martin County	*Roseau County	
*Fillmore County	*McLeod County	*St. Louis County	

82.3 percent. Table A.3 lists the cities receiving the survey and denotes those that responded. Of 310 school districts surveyed, we received responses from 272 (with 156 responding on-line), for a school district response rate of 87.7 percent. Table A.4 lists the school districts receiving the survey and denotes those that responded.

Based on the response rates and degree of variation in responses, the margin of error for the county survey is plus or minus 3.6 percentage points; for the city survey it is 3.3 percentage points; for the school district survey it is 2.9 percentage points. The margin of error may be larger for responses to particular questions where the number of respondents is low. Survey results may also reflect additional sources of error that cannot be measured. For example, the wording and order of the survey questions can affect results.

In a limited number of cases, we called jurisdictions when information they reported appeared to conflict. Beyond that, we did not independently verify the accuracy of the information respondents provided.

Table A.3: Cities Receiving Survey

*Ada
*Adams
*Afton
*Akeley
*Albert Lea
*Alden
*Alexandria
*Alpha
*Alvarado
*Amboy
*Andover
*Anoka
*Arco
*Arden Hills
Arlington
*Ashby
*Atwater
*Audubon
*Aurora
*Austin
[1]Avoca
*Avon
*Backus
[1]Barnesville
*Barnum
*Barry
*Baxter
*Bayport
*Beardsley
*Beaver Bay
*Beaver Creek
*Becker
*Bejou
*Belgrade
*Belle Plaine
Bellingham
*Beltrami
*Belview
*Bemidji
*Benson
Bertha
Big Lake
*Bigelow
*Bingham Lake
*Birchwood
*Bird Island
*Biscay
*Blackduck
*Blaine
Blomkest
*Bloomington
*Blue Earth
Bluffton
*Bock
Borup
*Bovey
*Boyd
*Breckenridge
*Bricelyn
*Brooklyn Center
*Brookston
*Brooten
*Browerville
Browns Valley
*Brownsdale
*Bruno
*Buckman
*Buffalo
*Buffalo Lake
*Burnsville
*Burtrum
Butterfield
*Byron
*Callaway
*Calumet
Canby
*Carlos
*Carlton
*Cass Lake
*Cedar Mills
*Center City
*Centerville
*Champlin
*Chandler
*Chatfield
*Chisholm
Circle Pines
*Claremont
*Clarissa
*Clarkfield
*Cleveland
*Climax
Clinton
Clontarf
*Cloquet
*Coates
*Cobden
*Cohasset
*Cokato
Coleraine
*Columbia Heights
*Comfrey
[1]Comstock
*Corcoran
*Correll
Cottage Grove
Cottonwood
Crookston
*Crosslake
*Crystal
*Currie
*Cyrus
*Dakota
[1]Dalton
*Danube
*Darfur
*Darwin
*Dawson
*Dayton
*De Graff
*Deephaven
Deer River
Delhi
*Dellwood
*Denham
*Dennison
*Dent
*Dodge Center
*Doran
Dover
*Duluth
*Dumont
Dundee
*Dunnell
Eagan
*Eagle Bend
East Grand Forks
[1]Easton
*Echo
*Edgerton
*Eitzen
*Elgin
*Elkton
*Ellendale
*Ellsworth
*Elmdale
*Ely
*Erskine
Evan
*Evansville
*Eveleth
*Excelsior
*Fairmont
Faribault
*Farwell
*Fergus Falls
*Fertile
Fifty Lakes
*Finlayson
Fisher
*Flensburg
*Floodwood
Forest Lake
*Foreston
*Fosston
*Franklin
Frazee
*Freeport
*Fridley
*Garfield
*Garvin
*Gary
*Geneva
*Georgetown
*Gibbon
*Glencoe
Golden Valley
*Goodhue
*Goodview
*Graceville
*Granada
Grand Marais
*Grand Rapids
*Granite Falls
*Grasston
*Green Isle
*Greenbush
*Greenfield
*Greenwald
*Hadley
*Hallock
*Halma
*Ham Lake
*Hamburg
*Hammond
*Hampton
*Harding
[1]Hardwick
*Harmony
*Hartland
*Hastings
*Hawley
Hayward
*Hazel Run
*Hector
*Heidelberg
*Henderson
*Hendricks
Hendrum
*Henning
*Henriette
*Hermantown
[1]Heron Lake
Hillman
*Hills
*Hilltop
*Hinckley
*Hitterdal
*Hokah
*Hollandale
*Holloway
*Holt
*Hopkins
*Howard Lake
*Hoyt Lakes
*Hugo
*Humboldt
*Hutchinson
*Ihlen
*Inver Grove Heights
Iona
*Iron Junction
*Ironton
*Ivanhoe
*Jackson
*Janesville

Table A.3: Cities Receiving Survey (continued)

*Jasper
*Jeffers
*Karlstad
*Kasota
*Kasson
*Keewatin
*Kennedy
[1]Kent
*Kenyon
*Kerkhoven
*Kilkenny
*Kimball
*Kinbrae
*Kingston
Kinney
*La Crescent
*La Prairie
*La Salle
*Lafayette
Lake Benton
*Lake Bronson
*Lake City
*Lake Crystal
*Lake Elmo
[1]Lake Henry
*Lake Park
*Lake Shore
*Lake Wilson
*Lakeland
*Lakeland Shores
*Lakeville
*Lancaster
*Lastrup
*Lauderdale
*Le Roy
*Le Sueur
*Leonidas
*Lester Prairie
*Lewisville
*Litchfield
Little Canada
*Littlefork
[1]Long Beach
*Longville
*Lonsdale
*Loretto
*Lowry
*Lucan
[1]Luverne
*Lyle
*Madelia
*Madison
*Madison Lake
*Manchester
[1]Manhattan Beach
*Maple Lake
[1]Marble
*Marietta
*Marine On St. Croix
*Mayer
Maynard
*Mazeppa
*McIntosh
Meadowlands
*Meire Grove
*Menahga
Mendota
*Mendota Heights
Middle River
Miesville
*Milaca
*Milan
*Millerville
*Millville
*Milroy
*Minneapolis
Minneiska
Minnetrista
*Montevideo
*Montgomery
*Monticello
*Montrose
*Moorhead
Mora
*Morristown
*Motley
*Mound
*Mounds View
Mountain Lake
*Nevis
*New Hope
*New London
*New Market
*New Prague
New Trier
*New Ulm
*New York Mills
*Newport
*Nicollet
*Nimrod
*Nisswa
*Norcross
*North Branch
North St. Paul
*Northfield
*Northrop
*Oak Park Heights
*Oakdale
*Odin
*Ogilvie
*Onamia
*Orono
*Oronoco
*Orr
*Osakis
*Oslo
Osseo
*Ottertail
*Owatonna
*Palisade
*Parkers Prairie
*Paynesville
*Pelican Rapids
*Pemberton
*Perham
Perley
*Pierz
*Pillager
*Pine City
*Pine Island
*Pine River
*Pine Springs
*Plainview
*Plummer
*Plymouth
Preston
*Princeton
Prinsburg
*Prior Lake
*Proctor
*Racine
*Ramsey
Red Lake Falls
*Regal
Rice
*Richmond
*Riverton
*Rochester
*Rockford
*Rockville
*Rollingstone
Ronneby
Roscoe
*Roseau
*Rosemount
*Rothsay
*Round Lake
*Royalton
*Rush City
*Rushford
*Rushford Village
[1]Rutledge
*Sabin
*St. Augusta
*St. Bonifacius
*St. Clair
*St. Hilaire
*St. Leo
*St. Louis Park
*St. Martin
St. Mary's Point
*St. Paul
*St. Rosa
*St. Stephen
*St. Vincent
*Sanborn
*Sandstone
*Sargeant
*Sartell
*Sauk Centre
*Sedan
*Shafer
*Shelly
*Sherburn
*Shevlin
*Shoreview
Silver Bay
[1]Silver Lake
[1]Skyline
*Sleepy Eye
Sobieski
*Solway
*South Haven
*South St. Paul
*Spicer
*Spring Grove
*Spring Hill
Spring Lake Park
*Spring Valley
*Springfield
*Squaw Lake
*Starbuck
*Steen
Stephen
*Stewart
*Stewartville
Storden
*Strandquist
*Strathcona
Sturgeon Lake
*Sunfish Lake
Swanville
*Taconite
*Tamarack
*Taopi
*Taylors Falls
Tenney
*Thomson
*Tonka Bay
*Tower
*Trail
*Trommald
*Trosky
Twin Lakes
*Tyler
*Ulen
*Underwood
[1]Upsala
*Urbank
*Utica
Vadnais Heights
[1]Vergas
*Vermillion
*Verndale
*Vernon Center
*Victoria

Table A.3: Cities Receiving Survey (continued)

Villard
*Vining
Wabasha
*Wabasso
*Wadena
*Wahkon
*Waite Park
*Waldorf
*Walker
*Walnut Grove
*Waltham
*Warren
*Warroad
*Waseca
Watertown
*Waterville
*Watson
Waubun
*Waverly
*Wayzata
*Wendell
*West St. Paul
*West Union
*Westbrook
*Whalan
Wheaton
*White Bear Lake
*Wilder
*Willernie
Williams
*Willmar
*Willow River
*Wilmont
*Wilton
*Windom
*Winger
*Winnebago
*Winton
*Wolf Lake
*Woodland
*Woodstock
*Worthington
*Wrenshall
*Wykoff
*Wyoming
*Zemple
*Zimmerman
*Zumbro Falls
*Zumbrota

NOTE: Asterisks (*) depict cities from which we received completed surveys in time for analysis.

[1]Returned survey too late to be included in our analysis.

Table A.4: Independent and Special School Districts Receiving Survey

*A.C.G.C.
*Ada-Borup
*Adrian
*Aitkin
*Albany
Albert Lea
[1]Alden
*Alexandria
*Annandale
*Anoka-Hennepin
*Ashby
*Austin
*Badger
*Bagley
*Balaton
*Barnesville
Barnum
*Battle Lake
*Becker
*Belgrade-Brooten-Elrosa
Belle Plaine
*Bemidji
*Benson
*Bertha-Hewitt
*Bird Island-Olivia-Lake Lillian
*Blackduck
*Blooming Prairie
Bloomington
*Blue Earth Area
*Braham
*Brainerd
*Brandon
*Breckenridge
*Brewster
Brooklyn Center
*Browerville
*Browns Valley
*Buffalo
*Buffalo Lake-Hector
*Burnsville
*Butterfield
*Cambridge-Isanti
*Campbell-Tintah
*Canby
*Cannon Falls
*Carlton
*Cass Lake
*Cedar Mountain
*Chaska
Chatfield
*Chisago Lakes
*Clearbrook-Gonvick
*Cleveland
*Clinton-Graceville-Beardsley
*Cloquet
Columbia Heights
*Comfrey
*Cook County
*Cromwell
*Crookston
*Cyrus
*Dassel-Cokato
*Dawson-Boyd
*Deer River
*Delano
*Detroit Lakes
*Dilworth-Glyndon-Felton
*Dover-Eyota
*Duluth
*Eagle Valley
*East Grand Forks
*Eden Prairie
*Edgerton
*Edina
*Elgin-Millville
*Elk River
*Ellsworth
*Ely
*Evansville
*Eveleth-Gilbert
*Fairmont Area
*Faribault
Farmington
*Fillmore Central
*Fisher
*Floodwood
*Foley
Forest Lake
*Fosston
*Franconia
*Frazee
Fridley
*Fulda
G.F.W.
*Glencoe-Silver Lake
*Glenville-Emmons
*Goodridge
*Granada Huntley-East Chain
*Grand Meadow
*Grand Rapids
*Greenbush-Middle River
Greenway
*Grygla
*Hancock
*Hawley
*Hayfield
*Hendricks
*Henning
Herman-Norcross
*Hermantown
*Heron Lake-Okabena
*Hibbing
*Hills-Beaver Creek
*Hinckley-Finlayson
*Holdingford
*Hopkins
*Houston
*Howard Lake-Waverly-Winsted
*Hutchinson
*International Falls
*Inver Grove
*Isle
*Ivanhoe
Jackson County Central
*Janesville-Waldorf-Pemberton
*Jordan
*Kasson-Mantorville
*Kelliher
*Kenyon-Wanamingo
*Kerkhoven-Murdock-Sunburg
*Kimball
Kingsland
*Kittson Central
*Lac Qui Parle Valley
La Crescent-Hokah
*Lake Benton
*Lake City
*Lake Crystal-Wellcome Memorial
*Lake Of The Woods
Lake Park Audubon District
*Lake Superior
*Lakeview
*Lakeville
*Lancaster
*Lanesboro
Laporte
*Le Center
*Le Roy

Table A.4: Independent and Special School Districts Receiving Survey (continued)

*Lester Prairie
[1]Le Sueur-Henderson
*Lewiston
*Litchfield
*Little Falls
*Littlefork-Big Falls
Long Prairie-Grey Eagle
*Luverne
*Lyle
*Lynd
*M.A.C.C.R.A.Y.
*Mabel-Canton
*Madelia
*Mahnomen
*Mahtomedi
*Maple Lake
*Maple River
*Marshall
*Marshall County Central
*Martin County West
*McGregor
*McLeod West
*Melrose
*Mesabi East
*Milaca
Milroy
*Minneapolis
*Minneota
*Minnetonka
*Minnewaska
Montevideo
*Monticello
*Moose Lake
[1]Mora
*Morris
*Mounds View
*Mountain Iron-Buhl
*Mountain Lake
Murray County Central
*N.R.H.E.G.
*Nashwauk-Keewatin
*Nett Lake
*Nevis
*New London-Spicer
*New Prague
*New Ulm
*New York Mills
*Norman County East
*Norman County West
*North Branch
*North St. Paul-Maplewood
*Northfield
*Norwood
*Ogilvie
*Oklee
*Onamia
Orono
*Ortonville
*Osakis
*Osseo
*Owatonna
*Park Rapids
*Parkers Prairie
*Paynesville
*Pelican Rapids
*Pequot Lakes
*Perham
Pierz
*Pine City
*Pine Island
*Pine Point
*Pine River-Backus
[1]Pipestone-Jasper
*Plainview
*Plummer
*Princeton
Prinsburg
*Prior Lake
*Proctor
*Randolph
*Red Lake
*Red Lake Falls
*Red Rock Central
*Red Wing
*Redwood Falls
*Renville County West
*Richfield
*Robbinsdale
Rochester
*Rockford
*Rocori
*Roseau
*Rosemount-Apple Valley-Eagan
*Roseville
*Rothsay
*Round Lake
*Royalton
*Rush City
*Rushford-Peterson
*Russell
*Ruthton
*St. Anthony-New Brighton
*St. Charles
*St. Clair
*St. Cloud
St. Francis
*St. James
St. Louis County
St. Louis Park
*St. Michael-Albertville
*St. Paul
*St. Peter
*Sartell
*Sauk Centre
Sebeka
*Shakopee
Sibley East
*Sleepy Eye
*South St. Paul
South Washington County
Southland
*Spring Grove
*Spring Lake Park
*Staples-Motley
*Stephen-Argyle Central
*Stewartville
*Swanville
Thief River Falls
*Tracy
*Tri-County
*Triton
*Truman
*Tyler
*Ulen-Hitterdal
*Underwood
*United South Central
*Upsala
*Verndale
*Wabasha-Kellogg
*Wabasso
*Waconia
*Wadena-Deer Creek
*Walker-Hackensack-Akeley
*Warren-Alvarado-Oslo
*Warroad
*Watertown-Mayer
*Waterville-Elysian-Morristown
*Waubun
*Wayzata
*West Central Area
*West St. Paul-Mendota Heights-Eagan
*Westbrook
*Wheaton Area
*White Bear Lake
*Willmar
*Windom
*Win-E-Mac
*Winona
*Worthington
*Wrenshall
*Yellow Medicine East
*Zumbrota-Mazeppa

NOTE: Asterisks (*) depict school districts from which we received completed surveys in time for analysis.

[1]Returned survey too late to be included in our analysis.

SITE VISITS OF SELECT LOCAL JURISDICTIONS

For information on how local governments made their arrangements for managing computer systems, we selected ten jurisdictions to visit for in-depth interviews: three each of counties and cities and four school districts. Half were smaller jurisdictions; four were located in the seven-county metropolitan area and six were in outstate Minnesota. The mix included jurisdictions with simple computer systems and others with very complex systems. The examples of best practices in chapters 2 and 3 are based on information gathered during these visits.

We visited the sites in October and November 2001. On these visits, we asked about staff use of computers, policies for managing the computer system, security procedures, information technology staffing, training and user support, and arrangements with vendors or collaborations. To collect the information systematically, we used a standard questionnaire with ten open-ended questions. All of those we interviewed had an opportunity to review and correct the summaries written for the report.

LOCAL GOVERNMENT ADVISORY COUNCIL

In April 2001, this study was recommended by the Local Government Advisory Council, along with a study on e-government. Table A.5 lists the individuals currently serving on the council. When the Minnesota Legislature established the best practices reviews program in 1994, it created the council and charged it with recommending local government services for review. The Advisory Council recommended the topics of managing computer systems and e-government to the Legislative Audit Commission, which approved the council's recommendation in May 2001. Council members also reviewed and commented on a draft version of this report.

Table A.5: Local Government Advisory Council Members, 2001-2002

Charles Meyer (chair), St. Louis Park City Manager
Don Helmstetter, Spring Lake Park Schools Superintendent
Tim Houle, Morrison County Coordinator
Kay Kuhlmann, Red Wing City Council Administrator
Scott Neal, Northfield City Administrator
Jack Paul, Hubbard County Coordinator
Doug Reeder, South St. Paul City Administrator
Terry Schneider, Minnetonka City Councilman
Dave Unmacht, Scott County Administrator
Lothar Wolter, Jr., Norwood Young America Township Clerk

Glossary

APPENDIX B

This appendix defines terms used in the report. These terms represent a small subset of the many technology-related terms involved with managing computer systems. For definitions and descriptions of additional terms, readers may want to consult one of numerous on-line glossaries including:

- Whatis?com at http://whatis.techtarget.com/, which features technology-related terms and includes a useful search function;
- Marshall Brain's HowStuffWorks at http://www.howstuffworks.com/, which provides easily understood, detailed descriptions of computers and technology (among many other categories of subjects);
- Network Working Group's Internet Security Glossary, at ftp://ftp.isi.edu/in-notes/rfc2828.txt, describes information technology security terminology, and it is a reference suggested by the CERT® Coordination Center at Carnegie Mellon University;
- Corporate Computer Consultants Limited Jargon Buster at http://www.cccl.net/information/JargonBusterHome.asp, which focuses on information security terms and offers numerous links for more in-depth information; and
- Precidia Technologies Glossary at http://www.precidia.com/technical_support/glossary.html, which defines a limited but useful list of technology terms.

The following are technology-related terms used in this report.

Antivirus programs: Software installed to search a hard drive, floppy disks, or particular files for any known or potential viruses. The software compares data on a computer or file against a collection of known virus "signatures."

Application programs: Software that provides tools to complete specific tasks, such as word processing. For example, Microsoft Word is a type of application program.

Backup: Copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. Backups may be performed locally, over a network, or over the Internet.

Broadband: Service that allows high-speed access to the Internet through the use of equipment such as cable modems and lines, DSL service, fiber optics, and wireless transmission systems. These telecommunication channels provide the means to transmit data electronically at speeds far faster than the traditional channel (which is a modem connected to copper telephone wires to dial in and connect to the Internet at a speed of up to 56 kilobits per second).

Browsers: Software programs allowing users to find and explore files on Internet Web sites. Common browsers are Netscape Navigator, Internet Explorer, and Mosaic.

Client/server computing: A model of computer program interactions whereby one program, acting as the client, makes a request and a second program, acting as the server, fulfills the request. In network computing, typically one computer acts as the server awaiting requests from client computers; multiple client computers may share the services of a single server program. The server centralizes data storage and processing and the tasks of entering data or requesting services are distributed among various client programs on personal computers.

Computer system: All the elements needed for data processing including a core system (comprised of software, data, and hardware and other equipment such as telecommunications devices,) and the support infrastructure (comprised of facilities, staff, and a computer system management plan).

Computer system management program: The policies, practices, and procedures related to the implementation, operation, maintenance, and ongoing control of the computer system. Components of a computer-management program address hardware, software, data, facilities, security, and user support.

Demilitarized zone: Computer security term describing a neutral area between the Internet connection and the rest of a computer network. A computer host or small network is inserted to act as a demilitarized zone (DMZ) that allows outsiders access to an organization's Web pages but inhibits them from gaining access to any of the rest of the organization's computer network. Outsiders that penetrate the DMZ security can access and alter the organization's Web site but the rest of the organization's computerized data is not exposed.

Digital signatures: Analogous to handwritten signatures on paper, digital signatures represent methods of "signing" electronic documents with 0's and 1's in ways that authenticate the sender of the document and reveal any tampering of it. Digital signatures rely on encrypting data that can only be decoded by the intended recipient.

Disaster recovery plans: Plans describing how an organization will deal with unanticipated events, such as power failures or hacker attacks, that disrupt their computer systems. Such plans include elements that focus on preventing disruptions as well as steps needed to resume computer functions and minimize downtime once disasters occur. They may be part of an organization's "business recovery" plan to resume service delivery when events have disrupted services.

Domain name servers: Computers that translate text into computer-readable numbers that map to specific computer addresses. The domain name indicates where to forward a request for a Web page. For instance, a domain-name server would translate a user's entry of http://www.auditor.leg.state.mn.us/ into the site containing the Web page for the Minnesota Office of the Legislative Auditor.

E-mail: The exchange of messages generated, stored, and transmitted by computer, most often using the Internet.

Encryption: A process of converting electronic data into a form that is not understood by unauthorized people. Encryption may involve substituting letters for numbers, rotating letters of the alphabet, or otherwise rearranging data bits in data signals. Decryption is converting the data back to its original form for the intended recipient.

Firewalls: Software and hardware devices to protect computer networks from unwelcome or unauthorized outside access.

Hardware configuration: Combinations of computers and other equipment, often in a network.

Incident response procedures: Steps planned by an organization to prepare itself for computer incidents. Such a plan includes identifying possible incidents (from hackers to internal misuse to natural disasters), listing effective responses to them, and specifying who is to undertake what procedures in the event of any particular incident.

Infrastructure: The people, facilities, and management program needed to support the core components of a computer system, namely its hardware, software, and data.

Internet: A global collection of computer networks connected together to form a single, interconnected network for communications.

Internet service providers: Also referred to as ISPs, Internet service providers offer a "point of presence" or gateway connecting computer users to the Internet and all of its accessible files.

Intranets: Electronic networks that are based on Internet technology but are internal to users within an organization and not accessible by outside users.

Intrusion detection systems: Security software that monitors for intrusions and unusual activities on a computer network.

License: An agreement between a user and a software publisher whereby the user agrees to pay for the privilege of using specific software and promises the software publisher to comply with all restrictions stated in an end-user license agreement. The end-user license agreement typically contains restrictions, such as those that limit the number of computers on which the software may be used.

Life-cycle cost: The full system cost, including all capital, operating, and replacement (including retirement) costs for equipment that arise from owning, operating, maintaining, and disposing of the system.

Listservs: Discussion groups using electronic mailing lists to send e-mail and transmit information about topics of common interest to their members. Computer users subscribe to mailing lists in their areas of interest. All subscribers automatically receive e-mail messages posted by any individual subscribed to that group.

Local area network (LAN): A group of linked computers and equipment sharing a common communications line within an area limited to a few thousand feet. LANs often share the resources of a single computer server.

Mainframe computer: A larger computer with the massive memory and processing power needed for large, complex business applications.

Minicomputer: A mid-range computer that stands between mainframes and personal computers in terms of memory and processing power.

Modem: A device that modulates and demodulates, i.e., converts, computer data into a signal compatible with transmission over cable or telephone lines. Wireless modems convert data into radio signals for wireless transmissions.

Network: In reference to computers, a network is a collection of compatible hardware and software arranged to allow computer users to share files and printers (and other peripheral devices) or connect to other networks.

Operating system software: Software that manages the computer resources, such as the central processing unit.

Patches: Repairs or enhancements to software programs to keep them usable until new versions of the programs are released.

Personal computer (PC): Desktop or laptop computers commonly used by staff to perform computing functions such as word processing.

Routers: Specialized computers that direct and transmit bits of data from one network to another. Routers control the flow of messages among computer networks.

Second-level authentication control: A procedure that requires two levels of computer-user identification. For instance, a first level of control may be a password and a second mechanism may be another password or, alternatively, a key, token, or biometric device (which recognizes a person based on biological characteristics such as fingerprints).

Security program: Policies and procedures designed to prevent unauthorized access, alteration, theft, or physical damage to computer systems.

Servers: Computers that share their resources, such as files and printers, with other computers on a network. Servers may be powerful personal computers with large hard-disk capacity, minicomputers, mainframe computers, or specialized computers designed specifically as servers.

Software: A program of detailed instructions to control the operation of a computer. Most software may be subdivided into application software, which helps user perform certain tasks, and system software, which manages how programs run on a computer.

Telecommunications infrastructure: As related to managing computers, equipment such as telephone wires, cabling, or wireless systems used for connecting computers to the Internet and interactin g with data provided on the Internet.

Virus: Programming code that causes unexpected and undesirable events, such as erasing data. Viruses often spread to other computers, unbeknownst to the original recipient. They are commonly transmitted in attachments to e-mail messages, from a diskette or compact disc, or from within files users download to their computers.

Vulnerability assessments: Software tools that scan computer systems to detect security flaws and known software or hardware bugs.

Web sites: Collections of related files (commonly with a beginning file called a "home page") available over the World Wide Web.

Wide area network (WAN): A collection of computers connecting multiple sites or computer networks at high speed across a broad geographic area using switched and dedicated lines (wire, cable, or fiber), microwave, or satellite communications.

Workstation: A powerful personal computer used for specialized functions such as statistical analysis.

World Wide Web: The universe of information accessible via the interconnected computer networks known as the Internet. It operates via accepted standards for storing, retrieving, and exchanging electronic information.

Worm: A self-replicating virus that resides in a computer's active memory, usually detected only when its uncontrolled replication consumes system resources and slows or stops other computing tasks.

Further Reading

Reports and Books

Center for Technology in Government. *Tying a Sensible Knot: A Practical Guide to State-Local Information Systems*. Albany, NY: Center for Technology in Government, June 2001. Available on-line at www.ctg.albany.edu/resources/pdfrpwp/iis1.pdf.

CERT® Coordination Center. *CERT® Security Improvement Modules.* Pittsburgh: Carnegie Mellon University, 2002. Available on-line at www.cert.org/security-improvement/.

Laudon, Kenneth C., and Jane P. Laudon. *Management Information Systems: Organization and Technology in the Networked Enterprise 6th ed*. Upper Saddle River, NJ: Prentice Hall, 2000.

Simmel, Derek, Gary Ford, Julia Allen, Christopher Alberts, Barbara Fraser, Eric Hayes, John Kochmar, Suresh Konda. *Securing Desktop Workstations*. Pittsburgh: Carnegie Mellon University Software Engineering Institute, February 1999. Available on-line at www.sei.cmu.edu/pub/documents/sims/pdf/sim004.pdf.

Web Sites

CNET Networks. *TechRepublic*. Louisville: CNET Networks, 2002. Available on-line at www.techrepublic.com.

Computer Security Division, National Institute of Standards and Technology, U.S. Commerce Department. *Computer Security Resource Center*. Gaithersburg, Maryland: National Institute of Technology, 2002. Available on-line at http://csrc.nist.gov/.

Gartner, Inc. *Gartner Research*. Stamford, CT: Gartner, Inc., 2002. Available on-line at www.gartner.com.

Microsoft Corporation. *Microsoft TechNet.* Redmond, Washington: Microsoft Corporation, 2002. Available on-line at www.microsoft.com/technet/default.asp.

Right Track Associates, Inc. *ITToolkit.* Available on-line at www.ittoolkit.com.

Recent Program Evaluations

Game and Fish Fund Special Stamps and Surcharges, Update, January 1994 94-01
Performance Budgeting, February 1994 94-02
Psychopathic Personality Commitment Law, February 1994 94-03
Higher Education Tuition and State Grants, February 1994 94-04
Motor Vehicle Deputy Registrars, March 1994 94-05
Minnesota Supercomputer Center, June 1994 94-06
Sex Offender Treatment Programs, July 1994 94-07
Residential Facilities for Juvenile Offenders, February 1995 95-01
Health Care Administrative Costs, February 1995 95-02
Guardians Ad Litem, February 1995 95-03
Early Retirement Incentives, March 1995 95-04
State Employee Training: A Best Practices Review, April 1995 95-05
Snow and Ice Control: A Best Practices Review, May 1995 95-06
Pollution Control Agency's Use of Administrative Penalty Orders, Update July 1995 95-07
Development and Use of the 1994 Agency Performance Reports, July 1995 PR95-22
State Agency Use of Customer Satisfaction Surveys, October 1995 PR95-23
Funding for Probation Services, January 1996 96-01
Department of Human Rights, January 1996 96-02
Trends in State and Local Government Spending, February 1996 96-03
State Grant and Loan Programs for Businesses February 1996 96-04
Post-Secondary Enrollment Options Program, March 1996 96-05
Tax Increment Financing, March 1996 96-06
Property Assessments: Structure and Appeals, A Best Practices Review, May 1996 96-07
Recidivism of Adult Felons, January 1997 97-01
Nursing Home Rates in the Upper Midwest, January 1997 97-02
Special Education, January 1997 97-03
Ethanol Programs, February 1997 97-04
Statewide Systems Project, February 1997 97-05
Highway Spending, March 1997 97-06
Non-Felony Prosecution, A Best Practices Review, April 1997 97-07
Social Service Mandates Reform, July 1997 97-08
Child Protective Services, January 1998 98-01
Remedial Education, January 1998 98-02
Transit Services, February 1998 98-03
State Building Maintenance, February 1998 98-04
School Trust Land, March 1998 98-05
9-1-1 Dispatching: A Best Practices Review, March 1998 98-06
Minnesota State High School League, June 1998 98-07
State Building Code, January 1999 99-01
Juvenile Out-of-Home Placement, January 1999 99-02
Metropolitan Mosquito Control District, January 1999 99-03
Animal Feedlot Regulation, January 1999 99-04
Occupational Regulation, February 1999 99-05
Directory of Regulated Occupations in Minnesota, February 1999 99-05b
Counties' Use of Administrative Penalties for Violations of Solid and Hazardous Waste Ordinances, February 1999 99-06
Fire Services: A Best Practices Review, April 1999 99-07
State Mandates on Local Governments, January 2000 00-01
State Park Management, January 2000 00-02
Welfare Reform, January 2000 00-03
School District Finances, February 2000 00-04
State Employee Compensation, February 2000 00-05
Preventive Maintenance for Local Government Buildings: A Best Practices Review, April 2000 00-06
The MnSCU Merger, August 2000 00-07
Early Childhood Education Programs, January 2001 01-01
District Courts, January 2001 01-02
Affordable Housing, January 2001 01-03
Insurance for Behavioral Health Care, February 2001 01-04
Chronic Offenders, February 2001 01-05
State Archaeologist, April 2001 01-06
Recycling and Waste Reduction, January 2002 02-01
Minnesota Pollution Control Agency Funding, January 2002 02-02
Water Quality: Permitting and Compliance Monitoring, January 2002 02-03
Financing Unemployment Insurance, January 2002 02-04
Economic Status of Welfare Recipients, January 2002 02-05
State Employee Health Insurance, February 2002 02-06
Teacher Recruitment and Retention, Research Summary, March 2002 02-07
Local E-Government: A Best Practices Review, April 2002 02-08
Managing Local Government Computer Systems: A Best Practices Review, April 2002 02-09

Evaluation reports can be obtained free of charge from the Legislative Auditor's Office, Program Evaluation Division, Room 140, 658 Cedar Street, Saint Paul, Minnesota 55155, 651/296-4708. Full text versions of recent reports are also available at the OLA web site: http://www.auditor.leg.state.mn.us