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

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.

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

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.

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.

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

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

© Corel Corporation 1997

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]

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]

Computer security policies should address identified risks.

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.

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.

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

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.