

Organizational Technology Needs: Evaluation and Implementation

Investment of time and resources are required when evaluating and meeting the technology needs of an organization. There are added challenges when the organization is a not for profit meeting the needs of victims of domestic violence. Protecting the personal identifying information of the individuals served, as well as organizational information, is probably given more consideration by those who provide services to domestic violence victims than any other entity.

This document will assist organizations in planning and evaluating resources as they begin to make decisions regarding improvements or upgrades of current technology or prepare to install new systems and protocols.

ASSESSING YOUR RESOURCES

To begin, complete an inventory of existing software. This includes the versions of particular software packages being used. Then, consider what new technologies would be redundant and/or not compatible with existing software. TechSurveyor at www.techsurveyor.org or www.techatlas.org are resources that provide assistance in conducting an equipment and software inventory. Once provided with specifics of an agency's inventory, these programs will generate reports on resources needed, compatibility issues and other questions an organization should factor into their decision about new software purchases or installation.

This technical assistance publication was written by **Cheryl Robb-Welch**, MCADV Operations Director. Technical Assistance was provided by **Jeremi Rowland of Lanit**, **Keith Stafford**, **Tim Raines** and **www.TechSoup.org**.



Despite minimal resources of a not for profit, with proper planning, an organization can still have a system that meets the needs of the organization and its staff.

Conduct an audit or inventory of the organization's existing hardware. The inventory should include:

- ▶ User
- ▶ Brand
- ▶ Model
- ▶ Serial Number
- ▶ Monitor type and serial number
- ▶ Processor type and speed
- ▶ RAM
- ▶ Hard Disk capacity
- ▶ Operating System
- ▶ Modems or network cards
- ▶ Available ports (i.e. USB)
- ▶ Drives (i.e. floppy, CD or DVD - be specific if reader or writer)
- ▶ Additional equipment attached to system (i.e. scanners)

Other equipment (such as printers or firewalls)

- ▶ Description
- ▶ Brand
- ▶ Model
- ▶ Serial Number

When developing a plan to upgrade or improve an organization's technology, these additional questions should be considered:

- ▶ What is the existing technology in my organization?
- ▶ What is working?
- ▶ What technology does the organization rely on?
- ▶ What is the skill level of staff?
- ▶ Who is relied upon for technological support?

BALANCING FINANCIAL RESOURCES AND THE ORGANIZATION'S TECHNOLOGY NEEDS

Below are some things to consider when examining the needs of the organization and presenting a budget to administrators, boards, or possible funders:

- ▶ What are the organization's most pressing needs?
- ▶ How would new technology improve the way the organization operates or communicates with staff, board or victims of domestic violence?
- ▶ Are computers begin donated by community members or businesses?
- ▶ What is the the cost of upgrading or rehabilitating the equipment

donated?

- ▶ Approximately 30 percent of the total cost of owning a computer system is spent on the initial purchase of the equipment and software. Seventy percent is spent on maintaining and upgrading the equipment and training staff. The larger the network, the more systems there are to maintain.

Computer expenses should be in the organizational budget every year. It should be expected that some of the computers will need to be upgraded, replaced or maintained each year. Plan to budget \$1,000 each year, per work station. This should allow the organization to purchase new computers for a third of the office each year.

Consider training a staff member to conduct routine maintenance work, upgrades and system troubleshooting. Generally, this person will devote one hour per week, per work station. Better yet, consider finding a charitable "tech" person or company in the community. Often, they will conduct repairs and upgrades for a reduced fee, if not free of charge.

FIREWALLS AND SECURITY ISSUES

A firewall is a system or group of systems that enforce an "access or deny policy." The access and deny policy is programming within the firewall that allows certain users access while denying access to those it does not recognize. The firewall filters all the packets (the method in which data is moved from one computer to another) that go in and out of the network and either blocks them or allows them to continue to their destination.

Traditionally, a firewall sits between private systems and their Internet connection. There are basically two types of firewalls, a network layer or an application layer.

A network layer firewall can refuse access to an IP address (a unique address that each computer has in order to communicate with another) or can restrict only certain types of packets to pass. A Cisco Pix Firewall is an example of a firewall that can allow or disallow packets based on the information they carry.

Application layer firewalls are mainly used for logging or filtering the Internet connection. This type of firewall allows an organization to use

No computer connected to the Internet, especially those that store identifying information on victims of domestic violence, should be without security features and protocols that are followed by all of the system's users.

Passwords are an integral part of an organization's computer security. Procedures for password maintenance, usage and administration not only need to be written, but also followed.

one real IP address for external communication and hundreds of non-routable IP addresses.

In short, these two types of firewalls do the same thing -- they just do it at different points of entry. The network layer firewall scans packets at the hardware level before a user ever sees it. This is called a "stateful inspection." The application layer firewall allows packets to pass through a system's hardware, through other layers of the system, then scans the packets prior to the application layer. The application layer is the layer at which a user does their work. For example, Microsoft programs are generally utilized in the application layer.

It can be argued that the network layer firewall provides better protection, but the cost may be prohibitive for most organizations. With advances in technology, the differences between these two type of firewalls are becoming less prominent.

Firewalls are only one method of defense for an organization's computer system. A full system security includes: who is allowed access; how a monitor or screen is positioned in a room for others to be able to view; proper disposal of paper copies; procedures for backing up data and its storage; and protocols regarding passwords.

Password protocols should include how often the passwords are changed, if they will be recorded and how that will be secured. Password policies against sharing of passwords, detailing who has full administrative access, and a set minimal amount of characters to be used in a password should be established. The ideal password is composed of numbers, symbols and letters of the alphabet. Windows servers have the ability to demand users provide only a "strong password." The strong password restricts a user to only use passwords that are comprised of several different key elements, such as having combinations of letters, numbers and symbols.

Most organizations can use the firewalls included in their routers. A router is either provided by the agency's technology partner (a computer company or person that they work with) or by the Internet Service Provider (ISP). The organizations that provide domestic violence services and store battered women's personal information on their systems, should weigh the data security requirements of that information. A breach of information could not only be dangerous to a battered woman, but financially and publicly cost the organization that fails to adequately protect that information.

Work with the organization's system administrator should include defining the organizational network needs. Discussion should include:

- ▶ Who should have access?
- ▶ How much access?
- ▶ What is the purpose of the firewall?
- ▶ Will the firewall supplement the existing security system or will the organization rely solely on the firewall?
- ▶ Should the firewall log activity and generate reports?
- ▶ Is the firewall able to be updated?

Another form of security that most people know about, but do not associate directly with security, is virus protection. Every machine on the network needs to have adequate virus protection with an update service. Viruses are constantly being released onto the Internet, so an update service will keep your machine protected against new viruses. Most services allow a user to schedule the frequency of searching for and installing new updates. The frequency of installing updated virus protection should be a part of the organization's policies and procedures. This will pose an ongoing yearly expense, but is a requirement for all computers connected to the Internet. Keep in mind that a firewall only blocks viruses that come from outside an organization. Some viruses, Trojan Horse viruses for example, can create an opening from inside an organization's system which may compromise the system's integrity.

Patch management is also an important form of security. Patches are released almost every day to fix security issues in software. A policy/procedure to keep up with these patches is a must in today's Internet connected environment.

If an organization is utilizing a dial-up connection, then personal firewalls for the machines dialing-up are a must. Machines can be attacked any time you are connected to the Internet, even on a dial-up line.

Depending on the size of the organization and their policies, additional elements such as Intrusion Detection Systems (IDS) could be implemented to add real-time monitoring and traceability of breaches of the system.

Lastly, an organization should consider having a written policy/procedure on recovering or reinitiating daily operations after a disaster.

Integrity of systems goes beyond physical and electronic security. It includes procedures that outline how daily operations will begin should a disaster occur and the facility is destroyed or if operations must be moved until the event ends.

The method by which an organization connects to the Internet is a matter of financial investment and the needs of the user. Discuss the security features of the equipment being installed with each of the providers before deciding on an Internet service provider.

The policy/procedure should consider:

- ▶ In the event of a fire or the need to relocate operations, how will work begin again?
- ▶ Where will the new equipment come from?
- ▶ Daily backups: Who conducts them and who stores them?
- ▶ Off-site storage of those backups. Consider where the back up tapes be stored while off site.
- ▶ Is a set of software kept off-site or in a secure location? Computer programs and software that are used to conduct daily operations should be kept in a secure location that is easily accessible so that a quick start-up can begin.
- ▶ If the system is off-line, how will bills be paid and intakes conducted?
- ▶ In the event of a breach of security, what plan of action will be taken?
- ▶ In the event of a system user's breach of security, what action will be taken? Is there any way for the agency to trace where the breach occurred and/or a way to prevent it from happening again?
- ▶ If cell phones are to be used until regular phone service can be established, is staff familiar with safety procedures when communicating with battered women?
- ▶ Does the organization have adequate insurance to cover damage to computer systems?

ASSESSING AN ORGANIZATION'S NEED FOR WIRELESS TECHNOLOGY

Properly configured wireless technology provides an expansion of the range of a wired network. For example, a large building could be networked easier by a wireless connection than by hardwiring all the terminals to a main network router.

Things to consider:

- ▶ Wireless networks expose the system to a range of users, not just the ones you have authorized. This may range from your next door neighbor to “spammers.” This is equally true for those in rural and urban environments.
- ▶ The network may be configured to allow only authorized users to the system, but an improperly configured access point may allow other unauthorized users to access any computer on the internal network.
- ▶ Information moving between terminals in the agency could be

intercepted by an unauthorized user. This could include emails, documents, database information, or financial and personnel records.

- ▶ There are safer ways to operate a wireless network, but often this will require a financial investment from the organization. Data encryption, access controls and requiring certificates (which are authorization codes) all come at a price. The price is often beyond what a not-for-profit agency is able to invest.
- ▶ How would a wireless network benefit the organization?
- ▶ What kind of financial resources is the organization prepared to invest? This is generally a much more expensive connection than a traditional cable connection, but if the organization is starting from scratch, compare the costs of both.
- ▶ What security level should the organization consider? (As this is of a much higher security risk, this should be given added weight if the confidential information of battered women and their children are stored on computers to be added to this network.)
- ▶ Is performance a consideration? For most users, the answer is “yes.” Depending on the number of users, a wireless network may not be adequate.

INTERNET CONNECTIONS AND STAFF ACCESS

There are basically four different methods to connect to the Internet. These methods include what are considered broadband technologies: dial-up connections; digital subscriber line (DSL); Cable; and T1 connections.

- ▶ Dial-up connections use a standard phone line and are generally very slow.
- ▶ DSL (Digital Subscriber Line) is a family of digital telecommunications protocols designed to allow high-speed data communication over existing copper telephone lines between end-users and telephone companies. DSL allows a user to have phone service and Internet connection simultaneously. This connection to the Internet is continuous.
- ▶ Cable Internet is generally provided by a cable television provider and provides a fast connection without interrupting phone usage. Cable internet leaves a user constantly connected to the Internet.
- ▶ A T-1 line actually consists of 24 individual channels. Each 64Kbit/second channel can be configured to carry voice or data

When researching the pricing differences in Internet connections, speed should be a factor in the decision making process. If an organization is hosting or developing their own Website, or using a Web-based program such as on-line banking, a slower connection may not be worth what initially appears to be a savings to the organization.

Clear policies on the use of the Internet by staff and program participants should be written. Policies concerning limits on a user's privacy, such as if email correspondences will be monitored, should be outlined as well as policies concerning downloading items from the Internet to the organization's computers.

traffic. Most telephone companies allow the purchase of just some of these individual channels known as a fractional T-1 access. This would be beneficial for organizations that pay a lot of money for more than 10 phone lines in addition to Internet and fax lines. A T-1 could cost an organization approximately \$1,000 a month and, therefore, may not be an option for most.

There is generally mixed reaction to the use of the Internet by staff. Some administrators are concerned about wasted time, while others believe there may be much to be gained by having Internet available to staff. Policies on Internet use should be established prior to installation.

Some things to consider:

- ▶ What can the organization do on the Internet that cannot currently be done?
- ▶ Which staff would benefit from Internet access or email?
- ▶ How important to the organization is the speed of the Internet connection?
- ▶ What type of connections are available in the area? If the organization is hosting and developing its own Website, a faster connection will be a greater benefit to the assigned staff.
- ▶ Consider a budget for Internet connection and any hardware needs that it may require.
- ▶ Are there enough phone lines to accommodate an Internet connection?
- ▶ What services will the organization need from an Internet provider, such as Website hosting or multiple email accounts?
- ▶ Has security of the data on the machines connected to the Internet been considered? If the organization is hosting its own Website, has security and the increased risk for intrusion been considered?
- ▶ Are the systems networked to a computer that is connected to the Internet? If this is a DSL or cable modem, then there is an extra risk to being constantly connected to the Internet. It is critical to have a firewall in this situation.
- ▶ Does your organization have a PC, network and an email policy for employees with access to these resources?
- ▶ Does the organization have a policy that requires filtering content for staff using the Internet? If filtering is a requirement, there may be added expenses for such a service.

DATA COLLECTION AND POLICY CONSIDERATIONS

Data collection has become an often discussed topic among domestic violence advocates. Databases that are inter-connected and share information are an even more controversial topic. Questions such as, "Why is the data collected?" and "How secure is the information we keep?" and "What are the possible consequences if the system/information is breached or viewed by an unauthorized user?" are all questions that must be considered by advocates. Below are some things to be considered by administrators, boards and developers who create or install you data collection software programs.

If the organization does not have a database, here are some things to consider:

- ▶ Why does the organization want to collect the data?
- ▶ How is current data that is collected stored?
- ▶ What purpose would a database serve?
- ▶ Is the data that is currently collected useful?
- ▶ Would the data storage method currently being used be more useful if it was reorganized?
- ▶ Who will have access to the database?
- ▶ Will it be on a network? If so, how will its security be monitored and who is using the system?
- ▶ What is the budget for a new database?
- ▶ Where will the information be stored? Is that location physically secure? How? If the data is stored off-site, who "owns" the data and to what lengths will all parties involved be prepared to protect that data?
- ▶ What equipment or software is required? This includes the equipment to protect the integrity of the system, as well as how many of the current computers will be able to run the new program.
- ▶ Will an existing program be used or will one be created?
- ▶ How will the system be maintained?
- ▶ How will the system be backed up and how often?
- ▶ What does the organization want the database to do?
- ▶ What kind of reports should the database generate?
- ▶ Who else uses the database program that the organization may be installing? Talk with them and ask them how useful or problematic they find the program.

Databases can provide a number of benefits to organizations. However, planning and development of the organization's philosophy concerning the collection of information on those served by the organization must be one of the first considerations of the organization's staff, board and administrators.

Websites that provide information to victims of domestic violence should provide adequate warnings about the dangers involved in communications over the Internet.

If the organization already has a database, consider:

- ▶ Is the current system adequate?
- ▶ Would it still be adequate with a 25 percent increase of information?
- ▶ Is there more than one database and would the organization be better served by combining them?

Policy work

- ▶ Does the organization have a written policy concerning data sharing?
- ▶ Does the organization have a written policy concerning breaches of both internal and external security?
- ▶ Administrators should consider developing a checklist of things staff must do when connected to the Internet.

ASSESSING YOUR ACCOUNTING SOFTWARE

Consider the following questions:

- ▶ Is your accounting managed by an in-house staff person?
- ▶ Is the system computerized?
- ▶ Will it be adequate with a 25 percent increase in volume?
- ▶ Do the current computers run the software adequately?
- ▶ Are there additional features the organization would like to have?
 - ▶ Fundraising management?
 - ▶ On-line banking?
- ▶ If on-line banking is an option, is the Internet connection adequate?
- ▶ Are there specific reporting requirements from grantors?
- ▶ Will someone need to install a new program?
- ▶ Will there be restricted access to the program?
- ▶ Do the machines need to be linked or networked?
- ▶ How many accounting transactions are conducted each month?
- ▶ What is the budget for this project?

WEBSITE DEVELOPMENT AND POLICY CONSIDERATIONS

Websites, though popular and seemingly necessary, should have planning and consideration given to their message, content and style.

Things to consider:

- ▶ What is the message and who is the target audience? Will the site give information about the organization and education about domestic violence? Will it be a resource to battered women or be a “lure” for funders?
 - ▶ If it is a lure for funders, can they make a donation on-line?

- ▶ Will the site be created by staff, volunteers or contracted to an outside source?
- ▶ If it is contracted out, what is the budget?
- ▶ Does the organization own software to produce the kind of site desired?
- ▶ What image of the organization will the site invoke?
- ▶ Will the site provide a means for someone to contact the organization? If so, will that be electronically?
- ▶ If electronically, how will that be done safely and answered timely?
 - ▶ If a battered woman seeks advice from the organization electronically, are there procedures on how to work with her?
 - ▶ Has a client/provider relationship been established by answering her request?
 - ▶ What issues arise if the one seeking services is a minor?
 - ▶ What issues arise if the one seeking services is from another state?
 - ▶ Is there adequate notice to users concerning possible risk to safety?
 - ▶ Does the site give adequate notice of which state in which the site originates?
 - ▶ Is there an established policy/procedure on the following:
 - ▶ Email correspondence with battered women?
 - ▶ Who will respond to emails from battered women?
 - ▶ How much information will the site contain about domestic violence or safety planning?
 - ▶ How will emails from batterers be handled?

Security should always be given careful consideration, especially by agencies that maintain information about victims of domestic violence. Though the list of questions in this publication is certainly not exhaustive, it will provide staff with a place to start when planning for upgrading an organization's technology.

Security should always be given careful consideration, especially by organizations that maintain information about victims of domestic violence.