

Computer Security Practices in Nonprofit Organizations

A NetAction Report



*NetAction is a project of The Tides Center
601 Van Ness Ave., No. 631 * San Francisco, CA 94102
Phone: (415) 775-8674 * Fax: (415) 673-3813 * E-mail: info@netaction.org
Web: <http://www.netaction.org>*

Computer Security Practices in Nonprofit Organizations

Introduction

Information technology is increasingly important to the mission of many nonprofit organizations. As reliance on technology grows, so too does the need for computer security. Security experts were concerned about the vulnerability of computer systems to cyber attacks long before the horrendous events of September 11, 2001; the terrorist attacks on the World Trade Center and the Pentagon have only raised the level of concern.¹ Last year, U.S. corporations spent an estimated \$12.3 billion to repair the damage done by computer viruses, and security experts predict the cost will be even higher this year.² While the focus of computer security concerns has primarily been on the potential threat to corporate and government computer systems, computers are no less critical to the operations of nonprofit organizations devoted to serving the public interest. Moreover, many nonprofit organizations lack sufficient financial resources to recover from a cyber attack.

Some risks are obvious:

- Without daily backups, an organization may lose important data when a hard drive crashes.
- Without regular updates, anti-virus software cannot protect an organization's computers from newly released viruses and worms.
- Without a firewall, malicious hackers can use an organization's server as a spam relay or a launch pad for a distributed denial-of-service (DDOS) attack against a corporation or government agency.

Other risks may not be as obvious:

- Without adequate password protection a disgruntled employee could retrieve addresses from an organization's database and send threatening letters to donors.
- Without encryption, a nosy volunteer could access an organization's personnel records or confidential files.
- Without off-site storage of backups and a data recovery plan, electronic records could be permanently lost if an organization's computers were destroyed in a fire or other disaster.

¹ "Cybersecurity Today and Tomorrow: Pay Now or Pay Later," the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) [pre-publication version].

<http://www.cstb.org/web/pub_cybersecurity>

² "U.S. Cyber Security Weakening,," Reuters, Jan. 8, 2002.

<<http://www.wired.com/news/print/0,1294,49570,00.html>>

With experts warning that the vulnerabilities in computer systems are increasing faster than the nation can respond,³ NetAction wondered whether nonprofit organizations were taking steps to ensure the security of their computer systems. We conducted an online survey of security practices in nonprofit organizations to find out what nonprofit organizations are doing to prevent cyber attacks.

Summary of Findings

Our survey found substantial room for improvement in the security practices of nonprofit organizations. Despite the importance of computers to nearly every aspect of nonprofit operations, only slightly more than half of the nonprofit organizations we surveyed back up their data every day, and only about one third have a data recovery plan in the event of catastrophic data loss.

The need to improve the security of confidential and/or sensitive files (such as personnel records or financial documents) was even greater. Only 4% of nonprofit organizations encrypt all sensitive files. Yet nearly two thirds of the organizations surveyed store sensitive files on computers connected to a local network, and nearly half store them on computers connected to the Internet. Moreover, computer users in nearly one fourth of the organizations we surveyed do not routinely lock or shut down their computers when they are away from their desks, and 80% of the nonprofits indicated that volunteers, interns, outside consultants and/or temporary staff have access to office computers.

The organizations did a somewhat better job of protecting their computers from viruses. About two-thirds of the organizations updated their anti-virus software one or more times per month. However, we also found that about two-thirds of the nonprofits use Microsoft's Outlook or Outlook Express to send and receive email despite the higher risk of an attack by viruses or worms than with other email clients.

Many of the respondents acknowledged the need to improve computer security practices. When asked to identify computer security issues their organization needs to address, about two-thirds of the survey respondents listed user work habits and disaster planning, about half listed data backups and encryption, and about one-third listed virus protection and firewalls.

³ "Cybersecurity Today and Tomorrow: Pay Now or Pay Later," the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC) [pre-publication version].
<http://www.cstb.org/web/pub_cybersecurity>

Section I: Nonprofit Organizations Surveyed

A total of 134 respondents completed our survey.⁴ These nonprofits have annual operating budgets ranging from \$2,000 to \$50,000,000; 64% of them have a budget specifically for information technology, ranging from \$250 to \$400,000 per year. The organizations have full- and part-time staff ranging from 1 to 3,000 employees, and 80% also have volunteers, consultants, interns or temporary staff who have access to computers. The table below indicates the primary focus of their work:

Table I: What is the primary focus of your organization's work?

Mission Focus	Percent	# Replies
Arts	5%	6
Children	10%	12
Civil Liberties	3%	3
Civil Rights	2%	2
Consumer Rights	2%	2
Digital Divide	2%	2
Education	14%	17
Environment	4%	5
Globalization	1%	1
Government Accountability	2%	2
Healthcare	7%	8
Housing	5%	6
Human Rights	1%	1%
Hunger	1%	1
Labor Union	1%	1
Peace & Social Justice	3%	3
Social Services	9%	11
Violence Prevention	1%	1
Women	3%	4
Multi-issue	13%	16
Other	13%	16
Total	100%	120

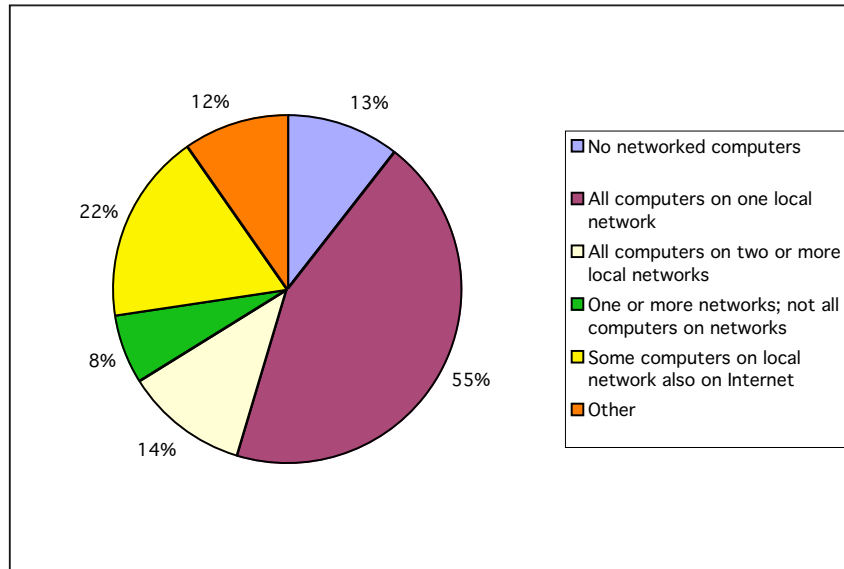
About one third of the respondents indicated they were either information technology managers (26%) or experts in terms of their knowledge (8%). Another 36% described their knowledge of information technology as above average, 25% described themselves as average in knowledge, and 5% indicated they were beginners.

Almost all of the organizations (92%) have web sites; 24% maintain their own site and 68% use a web hosting service. Although 99% of them have computers connected to the Internet, only 38% give staff remote access to office computers when traveling or working from home. In a majority of the organizations (55%) all computers are connected to a single internal network.

⁴ Not all of the respondents answered every question, so the total number of responses is not the same for every question.

Most organizations (89%) have shared data files on their office computers that can be read and/or modified by more than one person. As the following chart indicates, 22% of respondents reported that some networked computers are also connected to the Internet.⁵

Chart A: Are the computers in your office on a local (internal) network? (Check all that apply.)



Not surprisingly given its market dominance, the Windows operating system is used by a majority of the organizations. The table below indicates which operating system is being used:

Table II: Which operating system(s) do you use? (Check all that apply.)

OS	Percent	# Replies
Windows 95/98/Me	73%	88
Windows NT/2000	59%	71
Windows XP	7%	8
Mac OS	18%	21
Unix or Linux	13%	16
Other	6%	7

We also asked who was responsible for setting up, maintaining and troubleshooting office computers and networks. In 57% of the responding organizations an in-house information technology manager was responsible, 39% have an on-call consultant, 20% use a repair service as needed, 11% use volunteers and 8% reported everyone was on their own.

⁵ Some questions allowed participants to check more than one response, so the totals do not necessarily add up to 100%.

Finally, when we asked respondents to list all the ways in which computers were used in their organization, virtually all of the respondents indicated that their organizations use computers for a wide range of critical operations, as indicated in the following table:

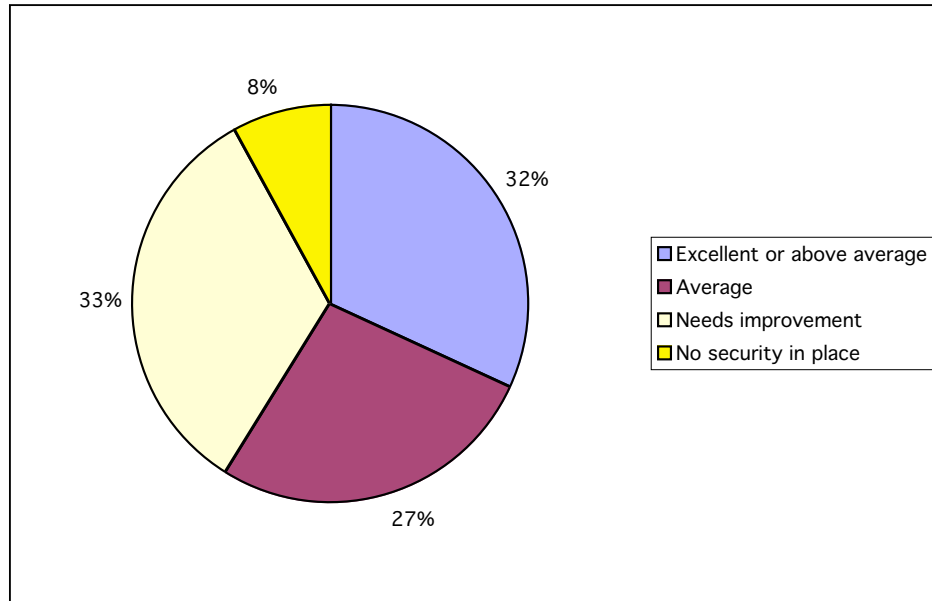
Table III: In the list below, please check all of the ways in which your organization uses computers.

<u>Response</u>	<u>Percent</u>	<u># Replies</u>
<u>Word processing</u>	<u>99%</u>	<u>118</u>
<u>Information management</u>	<u>99%</u>	<u>118</u>
<u>Marketing</u>	<u>88%</u>	<u>105</u>
<u>Fundraising</u>	<u>75%</u>	<u>89</u>
<u>Email lists</u>	<u>79%</u>	<u>94</u>
<u>Web site</u>	<u>87%</u>	<u>104</u>
<u>Staff communications</u>	<u>82%</u>	<u>97</u>
<u>Board communications</u>	<u>73%</u>	<u>87</u>
<u>Other</u>	<u>16%</u>	<u>19</u>

Section II: Computer Security Practices

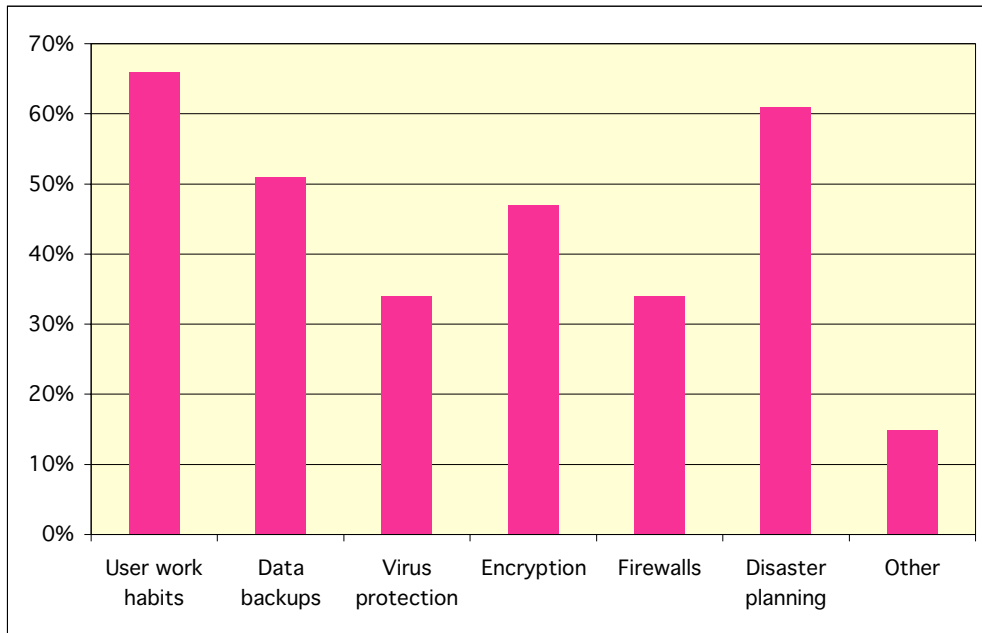
When asked how they would characterize the state of their own organization's computer security practices, nearly a third of the respondents (32%) acknowledged that their computer security practices needed to be improved. The chart below shows how respondents described their own organization's computer security.

Chart B: Which of the following statements best describes your organization's computer security?



We also wanted to know whether the respondents had identified specific computer security issues that needed to be addressed within their own organizations. When we asked what specific computer security issues their organization needed to address, nearly two-thirds of the survey respondents listed user work habits and disaster planning, and about half listed data backups and encryption. Responses to the survey questions that specifically addressed these security practices underscore the need for improvement. The table below indicates the security issues that respondents identified as needing to be addressed by their organization:

Table IV: In your opinion, what are the computer security issues that your organization needs to address? (Check all that apply.)



User Work Habits

In a majority of the organizations, computer users logon with a personal user name (54%) and/or a personal password (68%). While only 3% allow a user to logon without a user name, 10% allow a user to logon without a password, 9% allow all users to logon with the same password, and 4% allow all users to logon with the same user name.

The most basic – and low-tech – security practice is to lock or shut down a computer when it’s not in use. Yet only about a third of the respondents (30%) indicated that computer users *do* lock or shut down their computers most of the time when they are away from their desk. Nearly one fourth (24%) indicated that computer users *do not*. The table below indicates responses to our question about security practices in the area of user work habits:

Table V: Do computer users lock or shut down their computers when they are away from their desks during working hours, and when they leave work? (Select the statement that best describes your office.)

<u>Response</u>	<u>Percent</u>	<u># Replies</u>
Most do all the time	30%	36
Most do some of the time	15%	18
Some do, some don’t	29%	35
No	24%	29
Don’t know	2%	2
Total	100%	120

Responses to some of our other questions underscore the importance of this simple security measure. For example, 89% of the survey respondents indicated that there are shared files on office computers or office network servers that can be read and/or modified by more than one person, and in 80% of the organizations there are volunteers, interns, outside consultants and/or temporary employees who have access to the computers. Requiring users to logon with a user name and/or a password is not an effective security measure if the user does not logoff before leaving his or her desk.

Data Backups

Our survey included two questions about data backups. First, we asked about the frequency of backups. Only about half of the respondents (56%) indicated that their organization backed up data every day. The following table includes responses to our question about the frequency of data backups:

Table VI: How often is the data on your office computers backed up?

<u>Response</u>	<u>Percent</u>	<u># Replies</u>
<u>Every day</u>	<u>56%</u>	<u>67</u>
<u>One time or more per week</u>	<u>14%</u>	<u>17</u>
<u>One time or more per month</u>	<u>15%</u>	<u>18</u>
<u>Never</u>	<u>1%</u>	<u>1</u>
<u>Don't know how often</u>	<u>9%</u>	<u>11</u>
<u>Don't know if backed up</u>	<u>3%</u>	<u>4</u>
<u>Data not backed up</u>	<u>2%</u>	<u>2</u>
<u>Total</u>	<u>100%</u>	<u>120</u>

The location where backups are stored is also an important security consideration. For example, if the building in which a nonprofit organization is located is destroyed in a fire, a backup stored on site is likely to be destroyed along with the computers. Our survey found that 39% of nonprofits stored backups both on and off site, and 15% stored them only off site. The table below shows responses to our question about the location of backed up data:

Table VII: Where is your organization's backed up data stored?

<u>Response</u>	<u>Percent</u>	<u># Replies</u>
<u>In the office</u>	<u>32%</u>	<u>37</u>
<u>In a separate location</u>	<u>15%</u>	<u>18</u>
<u>In office & off site</u>	<u>39%</u>	<u>46</u>
<u>Don't know</u>	<u>10%</u>	<u>12</u>
<u>Data not backed up</u>	<u>3%</u>	<u>4</u>
<u>Total</u>	<u>100%</u>	<u>117</u>

Virus Protection

Our survey found that nearly two-thirds of nonprofits (63%) update their anti-virus software one or more times per month, only 1% never update the software, and only 3% don't have anti-virus software installed. The frequency with which nonprofits update their anti-virus software is detailed in the following table:

Table VIII: How often is the anti-virus software on your office computers updated for new virus definitions?

<u>Response</u>	<u>Percent</u>	<u># Replies</u>
<u>One or more times per month</u>	<u>63%</u>	<u>75</u>
<u>Less than once per month</u>	<u>8%</u>	<u>10</u>
<u>Whenever someone remembers</u>	<u>14%</u>	<u>17</u>
<u>Never</u>	<u>1%</u>	<u>1</u>
<u>Don't know how often</u>	<u>10%</u>	<u>12</u>
<u>Don't know if software installed</u>	<u>1%</u>	<u>1</u>
<u>Don't have software installed</u>	<u>3%</u>	<u>3</u>
<u>Total</u>	<u>100%</u>	<u>119</u>

We also wanted to know what happened to nonprofits that had experienced virus attacks. Of the nonprofits that had, 22% had minimal data loss, 47% had no data loss, and 19% had random non-sensitive files emailed to addresses in a user's Outlook address book. Only 5% of the nonprofits that responded had catastrophic or significant data loss from a virus, and only 3% had random sensitive or confidential files emailed to addresses in a user's Outlook address book. Another 12% indicated that they had never experienced a virus attack.

The type of email software that an organization uses can also make a difference. Since the vast majority of viruses and worms are created to exploit features in Microsoft's Outlook and Outlook Express email software, Outlook users are more at risk than users of alternative software programs (such as Eudora or Netscape Communicator). Unfortunately, nearly two thirds of the survey respondents indicated that their organization used Outlook and/or Outlook Express to send and receive email. The following table indicates the email software that respondents used in their organization:

Table IX: What software program(s) are you using to send and receive email? (Check all that apply.)

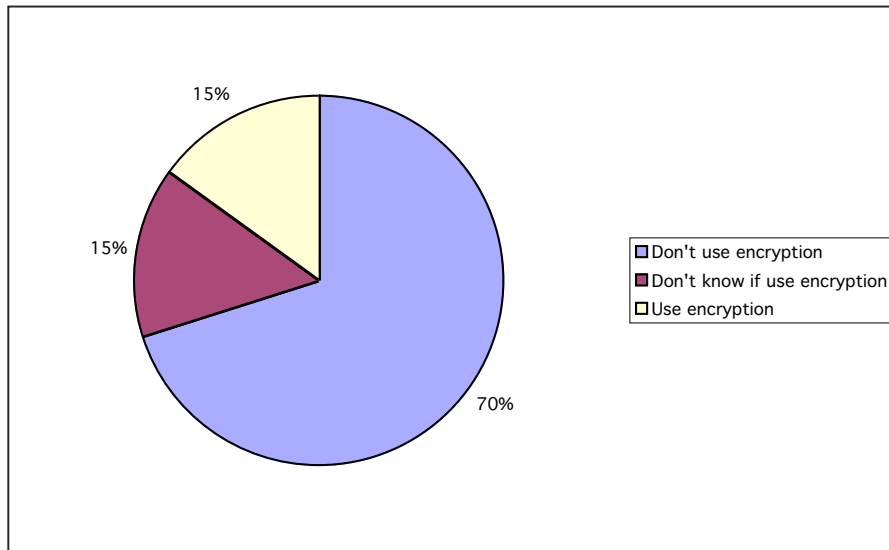
<u>Response</u>	<u>Percent</u>	<u># Replies</u>
Outlook or Outlook Express	64%	76
Entourage	5%	6
Eudora	22%	26
Netscape Communicator	18%	21
America Online	16%	19
Pine/Elm/Mail/Mutt	6%	7
Pegasus Mail	3%	3
Other ⁶	22%	26

Since computers running the Windows operating system are more vulnerable to a variety of cyber attacks, and Microsoft provides patches when security flaws are identified, we also wanted to know if nonprofit organizations update their operating system when patches are available. Our survey found that 29% of nonprofits did update their Windows operating system with patches. However, another 16% did not and 21% didn't know whether or not patches were being run.

Encryption

Encrypting sensitive and/or confidential files is another important security practice. It prevents unauthorized users from gaining access to confidential documents and ensures that any modifications to the data are revealed. Yet 70% of the nonprofits surveyed do not use encryption. The following chart indicates how respondents answered questions about the use of encryption:

Chart C: If your organization uses encryption software to protect sensitive and/or confidential files on your office computers, what software do you use?



⁶ Yahoo and GroupWise were the only others mentioned by more than one respondent.

We also wanted to know more specifically whether nonprofits encrypted sensitive and/or confidential files stored on network computers. Nearly two-thirds of the nonprofits (64%) store sensitive files on computers connected to a local network, and 46% store such files on computers connected to the Internet. But only 4% of the nonprofits encrypt *all* such sensitive files, and 29% indicated that *none* of those files are encrypted.⁷ The following table shows how nonprofits responded when asked about sensitive files on networked computers:

Table X: If there are files on any of your office computers that contain personnel records, financial documents, or other types of confidential or sensitive information, which of the following statements apply? (Check all that apply.)

<u>Response</u>	<u>Percent</u>	<u># Replies</u>
We have sensitive files on computers connected to a local network	64%	75
We have sensitive files on computers connected to the Internet	46%	54
We have no sensitive files on computers connected to a local networks	9%	11
We have no sensitive files on computers connected to the Internet	9%	11
All sensitive files are encrypted	4%	5
Some sensitive files are encrypted	8%	10
No sensitive files are encrypted	29%	34
Don't know	6%	7
Other ⁸	13%	15

Firewalls

When we asked about firewalls, nearly two-thirds of respondents (64%) indicated that there was a firewall between their office computers and the Internet. But 23% do not have a firewall, and 14% didn't know.

We also asked organizations that had experienced a security breach to briefly describe the experience, and received 42 responses. Some of their comments are included below:

- “We have hackers all the time trying to break in to use us as a spam server.”
- “In the past six years we’ve had three web sites destroyed by hackers. We presume it is because we support women’s equality, but can’t prove it.”
- In 1999, an ex-contractor launched a DDOS (distributed denial of service) attack against our mail server.”
- “When we hosted our email in-house, someone was able to compromise the security and configured the server as a spam relay. Reason: it was set outside the office firewall and connected directly into the DSL router we had at the time.”

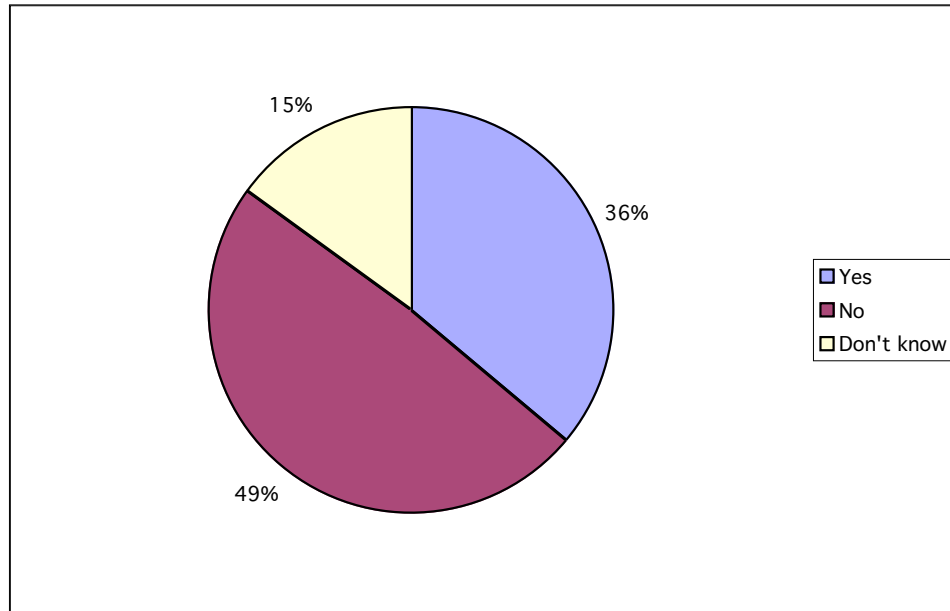
⁷ See “NetAction’s Guide to Using Encryption Software” for detailed information on its use. <http://netaction.org/encrypt/>

⁸ In most cases the “other” comments included more details about security practices related to sensitive files.

Disaster Planning

Nonprofits use computers for virtually all of their critical operations, so preparing for a disaster is no less important for nonprofit organizations than for businesses and government agencies. Yet nearly half of the nonprofits in our survey (49%) do not have a data recovery plan in place to implement in the event of catastrophic data loss, as indicated in the chart below:

Chart D: Does your organization have a data recovery plan to implement in the event of catastrophic data loss?



About the Survey

This report is based on a survey conducted online for a period of 31 days between December 19, 2001, and January 20, 2002. Participation in the survey was solicited via announcements to relevant email discussion lists and NetAction Notes subscribers, and through a notice on the NetAction Notes web site. Since random sampling techniques were not used in the survey, we cannot generalize the results to the larger nonprofit community. Despite this limitation, nonprofit organizations should find the report useful in assessing their own computer security practices and identifying practices that need improvement.

About the Author

Audrie Krause is the founder and executive director of NetAction, a San Francisco-based nonprofit organization dedicated to promoting use of the Internet for grassroots citizen action, and educating the public and policy makers about technology policy. Andrea Jepson and Theresa Chen assisted in editing the report.