Volume 7, Issue 2
May 2014
ISSN: 1946-1836

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **EDSIG,** the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is currently quarterly. The first date of publication is December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

JISAR Editorial Board

Information Security in Nonprofits: A First Glance at the State of Security in Two Illinois Regions

Thomas R. Imboden
timboden@siu.edu
Southern Illinois University
Carbondale, IL 62901

Jeremy N. Phillips
Jphillips2@wcupa.edu
West Chester University
West Chester, PA 19383

J.Drew Seib
jseib@murraystate.edu
Murray State University
Murray, KY 42071

Susan R. Fiorentino
sfiorentin@wcupa.edu
West Chester University
West Chester, PA 19383

Abstract

Information security is a hot button topic across all industries and new reports of security incidents and data breaches is a near daily occurrence. Much is known about recent trends and shortcomings in information security in the public and private sectors, but relatively little research examines the state of information security in nonprofit organizations. The underlying missions of nonprofit organizations, composition of their workforce, and their reliance on grants and donations for revenue generation streams set nonprofits apart from private business. These facts warrant an examination of information security of nonprofit organizations separate from private or commercial groups. This paper examines the state of information security in nonprofit organizations with results obtained by surveying volunteers or employees at nonprofit groups in two areas of Illinois. A qualitative discussion using observations gained from direct analysis of the security status of three organizations as part of student service learning projects is presented as well.

Keywords: Information Security, Nonprofit, Information Technology

1. INTRODUCTION

Today, organizations thrive on information. Often the success of an organization depends upon the quantity and quality of the data collected and their ability to employ the data as a resource. Collecting information comes with a cost, however. As data collection becomes more prevalent so does the need to protect and secure this data. To date, researchers have focused heavily on how for-profit and governmental organizations use and protect information. To a large extent, research on how the nonprofit sector protects information is lacking. This void is unfortunate considering the size of the nonprofit sector, the increasing reliance on the nonprofit sector to deliver services traditionally provided by governments, and the push within the nonprofit sector to strategically gather information to increase organizational capacity. Nonprofits may be required by law to maintain employee or client information containing medical data, or other personally identifiable information such as social security numbers, credit history, and criminal background check information. Failure to maintain the confidentiality of this information can result in legal liability.

This paper proceeds as follows. First, the authors survey the literature on nonprofit organizations and information security. Next, the authors provide an overview of the research methodology of the study, an electronic survey of employees at nonprofits in Illinois and an in person analysis of technical and operational security protections at three organizations. Then, the authors present the results of this mixed methods study. The results illustrate that there are significant areas where information security can be improved in nonprofit organizations. A set of four nontechnical and operational recommendations are presented to assist nonprofits in improving their security posture. Finally, the future goals of the authors' work in the area will be shared.

2. BACKGROUND

The need for nonprofit organizations to pay attention to information security issues is ever growing. According to Kolb and Abdullah (2009), the FBI and the Privacy Rights Clearinghouse report that nonprofit organizations are highly susceptible to identity theft due to their strong web presence and use of electronic information. The rise of technology and use of digital information can be attributed to the push for nonprofit organizations to increase their use of strategic information technology, which includes making more data driven decisions and using technology to maximize growth (Hackler & Saxton, 2007).

Encouraging nonprofit organizations to employ strategic application of information and information technology will require nonprofit organizations to collect more information on constituents and the public (Kolb & Abdullah, 2009). Additionally, employing technology to maximize growth means that nonprofit organizations must use technology for focused marketing and fundraising, such as donations by credit card purchases and via direct bank withdrawals, often over the Internet. All of this information (personal information, medical records, credit information, etc.), as well as other organizational data are typically kept electronically on network servers and processed online and require organizations to take proactive steps to protect the integrity of the data through strong information security polices (Donohue, 2008).

The push for democratic governance heightens the need for nonprofit organizations to employ technology, gather data, and share data. First, the increase in the privatization movement means that nonprofits are increasingly taking on governmental roles (Alessandrini, 2002). Additionally, there is a push for more networked forms of governance, where organizations in a policy domain work together to tackle a particular issue. This means highly sensitive information will need to be transferred between organizations (Kolb & Abdullah, 2009). Finally, nonprofits are also turning to the idea of e-governance and accountability through accessible mediums such as the Internet. Thus, they are relying on technology as a means of communicating with the public, increasing the likelihood of exposure of sensitive data and communications (Smith & Jamieson, 2006). If the sensitive information that nonprofit organizations collect is ever exposed, there may be disastrous effects for the nonprofit organization including financial loss, loss of reputation, damage to employee morale, donor disenchantment and loss, and litigation (Kolb & Abdullah, 2009).

Carey-Smith et al. (2007) find that many organizations do not maintain an atmosphere that is conducive to information security. Many organizations do not promote strong security awareness or monitor behavior that could increase risk. Burns, Davies, and Beynon-Davies

(2006) find that several organizations note a "lack of time and knowledge" as the greatest obstacle to employing sound security policies. They surmise that such barriers may be easily overcome by providing a strong information security policy template that organizations can adopt. Carey-Smith et al. (2007) echo this sentiment, "[w]here resources are scarce, every dollar invested in information security can be perceived as a dollar not spent in direct support of the organizational mission." These findings are also consistent with Imboden et al. (2013) who find that the size of nonprofit's budget is the primary factor predicting whether an organization has an information security policy. This study builds on Imboden et al. (2013 and seeks to better understand to what extent nonprofit organizations employ effective policies and practices to protect their organization's data.

For many organizations, the creation of an information security policy is a challenge due to management's lack of understanding of security concerns and issues. Often a policy is seen as unnecessary as minimal technical safeguards such as antivirus software and firewalls are erroneously viewed as protecting an organization. One method for approaching security and creating an improved security posture for an organization is to begin with the creation and adoption of a formal information security policy (SANS). The information security policy provides the organization with a set of expectations to be met regarding information security as well as outlining consequences for not meeting these expectations (SANS). The policy requires compliance and functions as an internal "law" for the organization. The System Administration, Networking and Security Institute (SANS), a leader in information security education and research, publishes a guide and many examples of security policy documents that organizations can freely use to create their own information security policy documents. This resource may be useful in guiding an organization through the first and arguably most cost effective step towards improving the security for many organizations.

3. RESEARCH METHODOLOGY

This study uses a mixed methods approach to identify attitudes and practices related to information security and policies for nonprofit organizations in two regions of Illinois. The first part of this study utilizes a survey instrument administered to nonprofit organizations in the two regions. The survey provides an overview of how nonprofits use and handle sensitive information, as well as a general understanding of the steps that nonprofit organizations take to adopt formal polices to deal with sensitive information. The second part of the study conducts an in-depth security analysis of three nonprofit organizations identified from the original survey. The purpose of the security analysis is two-fold. First, the in-depth analysis provides support for the results obtained from the survey. Second, and more importantly, the security analysis provides detailed information regarding the security practices of nonprofit organizations that cannot be obtained through a survey. Additionally, this qualitative approach provides the participant group with tangible and actionable recommendations to improve information security.

For initial data collection, the authors developed a survey consisting of 39 open and closed ended questions hosted on a web site for participants to complete electronically. Prospective respondents were identified from publicly accessible databases of nonprofit organizations; however, their participation was anonymous. Participants for this study were solicited via email. Two specific areas were targeted: the Chicago metropolitan region and southern Illinois. While the Chicago region consisted of a primarily urban and suburban population, the southern Illinois region encompassed rural areas in addition to the predominantly suburban Illinois area of metropolitan St. Louis, Missouri. During the approximately one month survey response period, 154 surveys were started by prospective participants, of which 78 were completed.

The survey instrument was designed to gather data on the composition of information technology and security hardware and software, resources available to the nonprofit, general group demographic and employee makeup of the organization, employee attitude and experience regarding information security, and the types of potentially sensitive or personally identifiable data their organization stores or processes on their information systems.

A small group of nonprofits located within the local area of one researcher were identified and solicited for participation in the analysis of technical and operational information security policies and protections. Participants were asked to complete the existing information security survey (but not included in the results of the previous portion), provide the researchers copies

of any organizational policies or similar documents that referenced information security or related topics, and allow the researchers to access the organization's technology assets to perform a basic security evaluation of the hardware, software, and operational activities of the organization. Students from a volunteerism-focused, student organization from one author's school with an interest or work experience in information security were identified as research assistants and assisted in the organizational analysis. As motivation for the nonprofits' participation, the student volunteers and the authors agreed to document any security concerns or inadequacies discovered at the nonprofits and, if desired, assist with remediation of potential problems.

In addition to the completion of the original survey by administrators at the local nonprofits, a second list of technical and operational security questions were developed from industry and governmental best practice documents. These questions aimed to determine whether common security best practices were followed at the organizations. As an example, the questions were designed to elicit data regarding, but not limited to, the following:

- Does the organization have a formal information security policy and are members aware of its existence?
- Are common information security protections such as antivirus, firewalls, and operating system and third party software updates implemented and kept current?
- Has the organization experienced incidents that presented potential risks to information security?
- What does the nonprofit view as potential risks from poor information security?

Finally, a follow up survey was sent to the organizations that provided documents that governed organizational procedures or activities related to information security. The survey was designed to discover employee knowledge of and adherence to the provisions of the adopted policy. These surveys were administered to staff and volunteers of the respective organization.

4. RESULTS

When examining the data as a whole, we see the organizations in the sample are very diverse, ranging from operations comprised of no full time employees and no formal information security budget to organizations that devoted a substantial amount of formal resources to information security. Table 1 provides average demographic data on organizations that took part in the electronic survey. As noted in the table, on average, organizations dedicated more than $23,000 dollars to information technology and security and nearly half of the organizations stated they had an employee with formal responsibilities devoted to overseeing information security in the organization.

Characteristic	Mean
Budget	$1,331,352
IT budget	$23,408
Number of employees	19.5
Employees dedicated to IT	46.80%

Table 1 - Size of Nonprofits

Table 2 illustrates the types of personally identifiable information that nonprofit organizations collect. Nearly all organizations collect some type of personal information, with 20-30% of organizations collecting what can be considered sensitive information that could be costly for both the organization and constituents if the information were compromised.

Type of Data	
Names	97.80%
Addresses	94.70%
Phone Numbers	89.50%
Birth Dates	53.70%
Social Security Numbers	31.60%
Health Records	20.80%
Criminal Records	11.50%
Income	27.40%

Table 2 - Types of Data Handled

Given that nonprofit organizations are collecting sensitive information, do they take appropriate steps to protect the information? The authors define "appropriate steps to avoid loss of sensitive information" to mean organizations adopting a formal information security policy that meets the security needs of the organization as well as utilizing programs and procedures, such as antivirus programs and ensuring that such programs are up-to-date, to mitigate information loss. While these are certainly not the only steps required to protect sensitive data and information

systems, the authors believe it a foundation for security to be built upon.

Table 3 details the percentages of organizations in the sample that have a formal policy that governs information security. Additionally, this table provides information on the origin of such policies.

Have formal security policy	**56%**
Developed by employees	39%
Developed by board of directors	33%
Template found online	30%
Created by legal counsel	27%
Provided by parent organization	13%
Provided by another organization	12%
Provided by insurance company	6%
Combination of the above sources	44%

Table 3 - Nonprofit Adoption and Development of Information Security Policies

As noted in Table 3, 56% of organizations in the sample had a formal policy governing the use of information technology and security. Of the organizations identified as having a formal information security policy, the origins of such polices are derived from a variety of places. For example, 30% of organizations with information security polices constructed it from a template found online. Very encouraging is that 44% of organizations with information security policies used two or more sources to develop their information security policy. This suggests that nearly half of nonprofit organizations are thinking broadly when developing their policies. For example, an organization may initially acquire an information security policy from a template, but then consult employees, legal counsel, and/or their board of directors to tailor the policy to fit the needs of the organization.

Also promising is that nonprofit organizations communicate their information security polices to employees and require employees to acknowledge the content of such policies. As detailed in Table 4, 84% of nonprofit organizations with policies formally require their employees to acknowledge policies that govern technology use. What is more, Table 5 illustrates that nonprofit organizations are institutionalizing their technology polices through employee training and inclusion in the organization's employee handbook. A combined 65% of nonprofit organizations hold group or individual trainings, 58% distribute the policy to their employees, and 69% include the policy in their employee handbook.

Required to acknowledged policy	84%
Not required to acknowledge policy	16%

Table 4 - Formal Employee Acknowledgement of Security Policy

Group training sessions	33%
Individual training sessions	32%
Distributed by paper	29%
Distributed electronically	29%
In the employee handbook	69%

Table 5 - How Nonprofits Communicate the Security Policy

In addition to adopting polices to help mitigate threats to security, some nonprofit organizations are also employing appropriate security technologies to help reduce risk. Table 6 provides information on the types of technologies used by nonprofit organizations including antivirus programs, firewalls, and blocking of unauthorized websites and downloads. A large portion of organizations protect all computers in the organization. The data reveal that 80% of organizations have antivirus programs installed on all computers owned by the organization. Additionally, 61% of organizations stated they have firewall programs. There are still a large percent of organizations that are not universally protecting their infrastructure. Less used are web blocking programs that restrict employees from visiting potentially dangerous or prohibited websites.

While nonprofit organizations are using appropriate technologies, our data shows that these organizations are ignoring another risk by not automatically updating software. Recently, malicious attacks have targeted out-of-date versions of operating systems as well as third party applications such as Java, Adobe Reader, and Adobe Flash (Kaspersky Lab, 2012). Table 7 shows that less than half the organizations in the sample use automatic settings to update operating systems and programs.

	Antivirus	Firewall	Web Block
All computers	80%	61%	23%
Some computers	11%	17%	34%
No computers	4%	10%	30%
Unsure	5%	12%	13%

Table 6 - The Use of Antivirus, Firewall, and Web Blocking Programs

Automatic checks	48%
Manual checks	24%
Systems are not checked	17%
Unsure	11%

Table 7 - Maintenance of Operating Systems and Software

Employing information security polices and technologies to reduce organizational risk appear to be born out of real and perceived risk. Table 8 highlights the percentage of organizations in the sample that have experienced specific threats to information security. 43% of the sample notes that they have experienced issues with a virus, spyware, or malware. Roughly a quarter of the sample reports hardware or software malfunctions. And 14% of the sample notes human error leading to an issue with security.

Virus, spyware, and/or malware	43%
Data theft	3%
Hardware theft	10%
Hardware failure	29%
Software failure	24%
Website defacement	3%
Employee error	14%
Employee misuse/vandalism	3%

Table 8: Types of Incidents That Have Occurred

Table 9 suggests that nonprofit organizations are aware of the potential risks of an information breech. In addition to concerns affecting organizational efficiency and effectiveness such as data loss or productivity, organizations are also aware of threats to the organization's reputation and potential legal action that may come for an information breach.

Data loss	80%
Loss of productivity	60%
Hardware damage	32%
Identity theft	33%
General decrease in company security level	31%
Loss of reputation	48%
Legal action	30%

Table 9 - Perceived Consequences of an Information Breach

Security Analysis of Selected Groups

Of the groups solicited for a more in-depth look at their information security policy, employee attitude towards security, and security status, three within one author's locality volunteered for additional focus and participation. Organization 1 (ORG1) is focused on victim advocacy and recovery. Organization 2 (ORG2) serves children in an educational capacity. Finally, Organization 3 (ORG3) serves the community with arts programming. One author has worked with each organization directly and with the support of student volunteers during the course of this project. For each of the three organizations, the administrators responsible for decisions regarding technology or information security were asked to complete the original electronic survey in paper format.

Analysis of Organization 1

The first nonprofit organization studied was found to have an information security posture that given the size, mission, and resources dedicated to information technology, impressed the authors. ORG1's information security practices were deemed strongest of the three nonprofits analyzed. ORG1 employed nearly seventy staff and volunteers, had a budget of over $1.25 million, and served over one thousand clients during the past year. They reported a dedicated information technology budget of $8,700 and owned approximately thirty desktop and three laptop computers.

A formal interview with ORG1 administrative respondents illustrated a wealth of useful data regarding the state of information security at their nonprofit. An in-person observation and evaluation of their procedures and information systems proved to be even more illustrative of the link between policy, accountability, and the security posture of the organization.

While ORG1 did not employ any staff with information technology or security background or training, the authors believe that the assignment of technical and security responsibilities to one of the administrative staff served to directly influence the security posture of the organization's information systems and assets. This nonprofit had the highest number of technology assets, staff and volunteers, and annual operating budget. As illustrated below, the authors believe this employee's implementation of several non-technical and basic security protections was the key factor in increasing the security status of the nonprofit. As an example, a "cheat sheet" on safe computing practices is found next to each computer and serves as a reminder to be cautious and vigilant when using the PCs. While room for improvement exists, the organization was found to be performing more of the most common security tasks and best practices, despite the relative size and number of assets, than the other two organizations. More on the steps taken by this employee will be discussed at the end of this section.

ORG1's policy regarding the acceptable use of computing resources was approved six months prior to the authors' examination of the document. As an example, it referenced employee password standards, prohibited the use of personal email for official business, and outlined enforcement and consequences of breaking the policy. Employees were surveyed regarding the policy and its integration into the organization and its culture. These questions sought to determine the following:

1. Are employees aware of the existence of the information security policy?
2. How is the information security policy communicated to employees?
3. Are employees asked to acknowledge their receipt and adherence to the organization's security policy?
4. Have employees received information security training at their current or previous employers?

The results of the employee survey of the above questions are shown in Table 10. Eighteen employees that routinely used computers and technology were solicited for participated in this survey. Nearly 90% of those surveyed were aware of the existence of an information security policy, while only 16% reported being asked to acknowledge the policy either written or verbally.

Have Policy	Yes	No	Unsure
	16	1	1
Communicated	Email	Meeting	Paper Copy
	1	5	12
Acknowledged	Yes	No	Unsure
	3	12	3
Security Training	Yes	No	
	3	15	

Table 10 - ORG1 Employee Security Policy Survey

The nonprofit serves victims of crime, and is mandated by state law to protect the privacy of their clients. As is likely the case with administrators in many nonprofits, one individual "wore many hats", and supporting and administering technology and security was one secondary duty assigned to them. In certain circumstances, inappropriate or unauthorized disclosure could lead to misdemeanor criminal charges. While the administrator possesses no formal background in security or information technology, they took it upon themselves to learn about and take steps to improve the security at the organization by ensuring employees were aware of a few basic activities to protect their computer use and actions.

Student volunteers were also given permission to examine the desktop and laptop computers at ORG1 in order to assess the status of several common applications and operating system settings that affect the system's security and, in-turn, organization security. Specifically, students observed and assessed the following:

- Operating system version
- Status of operating system updates and patches
- Status of antivirus application and associated definitions
- Status and version of Java
- Status and version of Adobe Reader
- Status and version of Adobe Flash
- Screensaver lock and idle delay
- Status of operating system firewall
- Account permissions given to users

The complete results of this analysis will be presented in future work, but an overview found a few common themes.

- Older systems that were performing slowly were more likely to be missing

operating system updates and running out of date third party applications.
- While the security policy required use of time delayed screensaver locks, a majority of the systems did not implement them.
- Overall, systems were running recent versions of third party applications with few exceptions.
- Surge protectors were supplied and used for most workstations.
- Antivirus software was running, updated, and virus scans ran regularly.
- Most computers contained files in their My Documents folder that their users were responsible for backing up. The type or importance of these files was not examined.
- A majority of the user accounts logged in when students performed their security analysis were operating with full administrative privilege.

Analysis of Organization 2

The second organization (ORG2) was substantially smaller than ORG1 in terms of the number of employees, budget, and clients served. The annual budget was reported at $650,000, of which none was allocated for information technology and security. Approximately twenty-five employees and volunteers worked with the nonprofit over the last year. Of these, three are considered managers with the power to make decisions regarding information technology; however, technology purchases must be approved by board members.

ORG2 reported that an information security policy did not exist. They reported a lack of expertise as well as a lack of an industry or legal requirement as factors contributing to lack of a policy. The managers acknowledged storing or processing potentially personally identifiable information on their systems.

ORG2 owns two desktop computers, which are primarily used by the management staff to keep track of financial information, communicate with clients, and to create operational paperwork. It was originally observed that of the two computer systems, one was completely nonfunctional and had been for months, creating a burden on the organization. During the course of discussion with this group, the second PC suffered a hardware malfunction, rendering the organization unable to perform several regularly required operational duties via their standard procedures. It was found that data, including some which was critical to the groups operation, had not been recently backed up on either of the two failing computers. A volunteer was solicited by the organization to assist and two replacement PCs were purchased, configured, and installed. A data recovery firm was contracted to restore the data lost during the system hardware failures. It was also noted that other instances of virus infection, hardware failure, and software or data corruption had previously affected the nonprofit. No employee was responsible for information technology and security at ORG2. Antivirus software and firewalls were running on the computers, but operating system and third party applications were out of date and not routinely updated. The organization was also unaware that their Internet router created an unneeded and unused wireless network access point.

Analysis of Organization 3

The smallest organization in terms of budget was ORG3. They reported an annual budget of $25,000, of which none was allocated for information technology and security. ORG3 is unique in that while only employing one paid staff member, approximately 120 volunteers supported the organization and made use of the four desktop computers used by ORG3 to help serve the community and fulfill the group's community arts mission. Like ORG2, it was reported that a security policy did not exist and that a lack of perceived need and lack of expertise required to create one was behind this fact. Again, like ORG2, it was reported that a recent incident caused by employee misuse resulted in the loss of mission critical donor related files from a storage device. Recreating the files took over forty hours of volunteer time. Unlike ORG2, it was reported that antivirus software was not used but common third party applications and operating system updates were regularly checked and maintained. Personally identifiable information for volunteers and donors is stored or processed on ORG3's computers.

Common Themes from Direct Organization Observations

There were several common characteristics or shared themes found across the nonprofits. All three organizations reported loss of data due to hardware or software failure, employee misuses or error, or similar circumstances. In two cases, it was reported that the missing data had been backed up at one time, but when attempting to recover the data from backup copies, they were found to be too old to be useful or corrupt. In one

circumstance one group paid a specialized data recovery firm $500 to recover data critical to the organization. In a second case, a volunteer had to recreate customized files crucial to donor and underwriting activities taking over forty hours to do so.

A second common theme was the lack of a dedicated information technology support staff member or even consultant who regularly provided guidance and assisted with maintenance of information systems. All the organizations reported having at times paid for help from local technology businesses as needed, often only when an emergency need arose. Contrasting this with the need to regularly perform software updates and other types of routine maintenance to improve security, it was expected that these tasks were neglected, putting individual and organization wide systems at higher risk. As ORG2 and ORG3 reported no budget funds allocated for information technology, it would stand to reason that paying outside help to fix technology issues would be a last resort. Secondly, given the need for nonprofits to rely on volunteers, it was found that each group relied on the information technology help and skills of volunteers trained in or working in IT positions.

Another common theme that is evident, given the examples of data loss and hardware failure, is the lack of redundancy in business critical hardware and applications, and the absence of regular and reliable backup technologies and processes.

Lessons Learned

Several key actions or themes that were believed to contribute significantly to the positive security stance of an organization were identified.

1. **Have an Information Security Champion –** Identify a single employee who can be charged with leading the effort for improved security. Understanding and implementing even the most basic security practices such as maintaining operating system and third party application updates will help decrease incidents.
2. **Create a Policy -** A basic policy addressing information security will help employees understand that information security is important to the organization and will provide a level of expectation regarding their use of technology.
3. **Train and Talk –** While it is unreasonable to expect volunteers and employees to become security experts, several basic tasks and activities can contribute to improving security. A regular discussion, whether in the form of formal meetings or as an informal email reminder of security tips, serves to open dialogue on the subject and keep it fresh in their minds.
4. **Develop Organization Specific Materials –** Create posters reminding users to think before they click and provide security checklists such as a "Do's and Don'ts" for safe computing to keep next to computers. This can serve as yet another illustration that the organization is concerned with security.

5. FUTURE WORK

The information presented in this paper is simply a first glance at the state of information security in nonprofit organizations. The authors intend to increase data collection efforts to expand to diverse regions across the United States. Results from a larger population will help to determine even further where deficiencies in information security practices and policies exist and provide researchers with a foundation for the development of resources that may help nonprofits. Those with minimal resources and expertise in information technology and security certainly could use help to improve their security posture and use their technology safely and efficiently.

6. REFERENCES

Alessandrini, M. (2002, October) A fourth sector: The impact of neoliberalism on non-profit organizations. Paper presented to Australasian Political Science Association Jubilee Conference, Canberra, Australia.

Burns, A., Davies, A., & Beynon-Davies, P. (2006, November) A study of the uptake of information security policies in small and medium sized businesses in Wales. Paper presented at Global Conference on Emergent Business Phenomena in the Digital Economy, Tampere, Finland.

Carey-Smith, M., Nelson, K., & May, L. (2007). Improving information security management in nonprofit organizations with action. Proceedings of 5th Australian Information Security Management Conference (pp. 38-

46), Perth, Australia: School of Computer and Information Science Edith Cowan University

Denhardt, J. V., & Denhardt, R. B. (2011). The new public service: Serving, not steering. New York: ME Sharpe.

Donohue, M. (2008) States push to encrypt personal data. The Nonprofit Times. Retrieved from http://www.thenonprofittimes.com/news-articles/states-push-to-encrypt-personal-data/.

Hackler, D., & Saxton, G. D. (2007). The strategic use of information technology by nonprofit organizations: Increasing capacity and untapped potential. Public Administration Review, 67(3):474–487.

Hrywna, M. (2007). Nonprofits and data breaches. The Nonprofit Times. Retrieved from http://www.thenonprofittimes.com/news-articles/nonprofits-and-data-breaches/.

Imboden, T. R., Phillips, J. N., Seib, J. D., & Fiorentino, S. R. (2013). How are nonprofit organizations influences to create and adopt information security policies? Issues in Information Systems, 14(2): 166-173.

Kaspersky Lab. (2012). Oracle Java surpasses Adobe Reader as the most frequently exploited software. Kaspersky Lab Corporate News. Retrieved from http://www.kaspersky.com/about/news/virus/2012/Oracle_Java_surpasses_Adobe_Reader_as_the_most_frequently_exploited_software.

Kolb, N., & Abdullah, F. (2009). Developing an information security awareness program for a non-profit organization. International Management Review, 5(2):103–108.

SANS. SANS Security policy project. Retrieved from http://www.sans.org/security-resources/policies/.

Smith, S. and Jamieson, R. (2006). Determining key factors in e-government information system security. Information Systems Management, 23(2):23–32.