https://doi.org/10.48009/2_iis_2013_166-173

Issues in Information Systems

Volume 14, Issue 2, pp.166-173, 2013

HOW ARE NONPROFIT ORGANIZATIONS INFLUENCED TO CREATE AND ADOPT INFORMATION SECURITY POLICIES?

Thomas R. Imboden, Southern Illinois University, timboden@siu.edu
Jeremy N. Phillips, West Chester University, jphillips2@wcupa.edu
J. Drew Seib, Murray State University, jseib@murraystate.edu
Susan R. Fiorentino, West Chester University, susanfiorentino@yahoo.com

ABSTRACT

As news of cyber attacks and data breaches at corporate and government institutions have increased in frequency, the discussion as to whether nonprofit organizations are affected similarly has largely been omitted. While at first glance a typical nonprofit might not seem as valuable of a target to hackers and cyber criminals as business or public sector groups, this study finds that these organizations routinely collect and store data often targeted by digital thieves. But are they storing, transmitting, and processing this data in a safe and secure manner? The creation and adoption of a formal information security policy is often seen as the starting point for a strong information security program at an organization. This study explores the adoption as well as attitudes regarding information security policies at nonprofit organizations in two areas of Illinois.

Keywords: Information Technology (IT), Information Security and Nonprofits

INTRODUCTION

It goes without saying that technology has come to dominate our lives. The increase and prevalence of technology in the workplace has fundamentally changed the way organizations do business. Rarely is important information locked in a file cabinet or on a desktop computer isolated from the rest of the world. Today's organizations store highly sensitive information on remote servers, within databases accessible to the outside world via an internet connection, and on laptop computers that can be taken anywhere. This new way of doing business means organizations are increasingly vulnerable to a breach of sensitive information.

While organizations certainly want to protect against malicious attacks from outside entities, one often overlooked risk of information loss is due to human error [6]. Developing and implementing policies to protect against human error and mismanagement can greatly reduce an organization's risk of information loss or disclosure. To this end, organizations can mitigate their risk by taking deliberate steps to protect sensitive information by 1) budgeting for information security infrastructure and 2) developing and enforcing workplace policies related to information security.

While information security is a topic that has received much attention in the for-profit and governmental sectors, little attention has been focused on how the nonprofit sector handles information security. This oversight is unfortunate given that the nonprofit sector also collects sensitive information such as personal information (e.g. social security numbers, birthdates, household income), credit card information, and health records. Collection of sensitive data will certainly increase in the future. The nonprofit sector has been encouraged to expand its strategic use of information technology via targeted marketing and fundraising [6]. Furthermore, the privatization movement continues to lean on the nonprofit sector to pick up governmental functions [2,6,7]. Both of these trends mean an increasing number of nonprofit organizations will collect sensitive information and store it via electronic technologies.

One of the cheapest and most effective methods an organization can employ to take a step towards protecting sensitive information is through the adoption of a formal information security policy [4]. However, are nonprofit organizations appropriately applying this line of defense? The following paragraphs explore how nonprofit organizations in portions of Illinois approach information security. Special attention is given to information security policies. The study's results find that the size of the organization is the driving factor for adopting an information security policy. This fact is independent of whether the organization had a previous breach of information security.

The authors conclude that nonprofit organizations in the surveyed portions of Illinois need to take more proactive steps to mitigate risk by adopting formal information security policies.

BACKGROUND

Prevalence and Impact of Information Security Breaches

Several recent studies highlight the prevalence of information loss and the need for organizations to take steps to protect client and constituent information. For example, according to the 2008 Computer Crime and Security Survey, 46% of responding organizations reported experiencing some form of a security incident [15,23]. The Privacy Rights Clearinghouse found that a total of 155,048,651 electronic records containing confidential personal information were stolen between January 2005 and June 2007 [14]. Additionally, a 2003 Federal Trade Commission survey found that nearly 10 million consumers in the United States were victims of identity theft in the past year [20] and identity theft was the number one complaint reported to The Consumer Sentinel Network [10].

The cost of information breaches continues to rise for both individuals and organizations. The average annual monetary loss resulting from data breaches reported by US companies doubled in 2007 to an average loss per responding organization of $345,005 [23]. And, it appears that the monetary impact will grow as online behavior of consumers is partially shaped by knowledge of information security breaches [20]. In fact, the concern is so large that the insurance industry has developed products designed to protect organizations from monetary loss due to security breaches [16].

The cost of information security extends beyond losing the confidence of the public. Picanso [20] notes that both federal and state governments are reacting to the concerns of citizens by adopting a myriad of regulations that place the responsibility of enacting proper security measures on the organizations. This means organizations must be willing to invest in proper security measures or face legal and monetary consequences of not complying with current law.

The Need for Nonprofit Information Security Measures

The need for nonprofit organizations to develop an awareness of information security issues is ever growing. Kolb and Abdullah [16] note that the FBI and the Privacy Rights Clearinghouse report that nonprofit organizations and colleges and universities are highly susceptible to identity theft due to their strong web presence and use of electronic information. Moreover, Heckler and Saxton [13] articulate the need for nonprofit organizations to increase their use of strategic information technology. This includes making more data driven decisions and using technology to maximize growth. The former will require nonprofit organizations to collect more information on constituents and the public. The latter refers to using technology for focused marketing and fundraising, such as credit card purchases and donations via direct bank withdrawals or credit cards. All of this information (personal information, medical records, credit card information, etc.), as well as other organizational data are typically kept electronically on network data servers and processed online [9,14,16].

Additionally, the push for democratic governance heightens the need for nonprofit organizations to employ technology and gather and share data. First, the increase in the privatization movement means that nonprofits are increasingly taking on governmental roles [2,6,7]. 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 [16]. 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 form of communication with the public, increasing the likelihood of exposure of sensitive data and communications [26]. Exposure of sensitive information can have disastrous effects on a nonprofit organization, including financial loss, loss of reputation, damage to employee morale, donor disenchantment and loss, and litigation [16].

Information Security Preparedness in Nonprofit Organizations

While there is a gap in research toward understanding information security in the nonprofit sector, Carey-Smith et al. [6] posit that we should expect to see similar behavior in the nonprofit sector when compared to similar sized organizations in the for-profit sector. As Carey-Smith et al. [6] note, "nonprofit organizations and small to medium enterprises have many similarities, the major one being the relative lack of resources of much of the nonprofit and [small to medium enterprise] in the sectors when compared with larger corporate and government organizations." Small to medium size organizations simply do not have the expertise or monetary resources to invest in strong information security measures [5].

Exacerbating the problem is the rise in contract-based governance, which is highly outcome-based. Organizations are working with less money and must demonstrate results—meaning there is less money and less motivation to devote scarce resources to items that do not aid in strong outcomes, such as information security [11]. Carey-Smith et al. [6] say it best, "[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."

There are issues beyond monetary resources that influences proper security preparedness. As noted by Carey-Smith et al. [6], "recent research has found significant problems with information security culture, information security awareness and use of information security policies." Some organizations simply do not maintain an atmosphere that is conducive to information security. These organizations do not promote strong security awareness or monitor behavior that could increase risk. When management fosters a culture that promotes security, employees are more likely to exhibit the same behavior [28].

In addition to the issues discussed above, it appears the lack of proper information security infrastructure and policies is due to time constraints and inexperience of management. Burns et al. [5] find that most for-profit organizations note a "lack of time and knowledge" as the biggest barrier to adopting a formal information security policy. They provide the following anecdotal evidence from one company, "[i]f we were sent a standard small business policy document we would probably adopt it but have no time to sit and think something like this through at present." They surmise that such barriers may be easily overcome by providing a strong information security policy template that organizations can adopt.

What Do Strong Information Security Polices Look Like?

For many small to medium sized 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 anti-virus software and firewalls are erroneously viewed as protecting an organization. The preferred 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. Organizations approach this differently; some draft their own internally, others copy policies from other organizations or templates, while some consult legal counsel. Unfortunately, many ignore this step altogether.

The purpose of an information security policy is to provide the organization with a set of expectations to be met in regards to information security as well as outlining consequences for not meeting these expectations [25]. The policy requires compliance and functions as an internal "law" for the organization. Often a security policy is viewed as a highly technical undertaking when in reality most organizations simply need daily tasks associated with computer and system activity and behavior addressed. Supplemental documents such as security standards or guidelines can be added to address specific needs, technical requirements, or recommended practices [25].

Security policies for nonprofits should address issues such as employee or volunteer use of technology assets, use of social media by individuals on behalf of the nonprofit, and the safe storage or destruction of sensitive information on both electronic and physical media. The policy should outline procedures and required approvals for various activities that may present a risk to the organization's data or security, and it will explain actions that may be taken by management if these procedures were ignored.

It is important to explain the purpose behind policy directives in a manner that is understood by those bound by them in order to most effectively receive employee compliance. For example, a policy might prohibit the use of personal email accounts such as Gmail or Hotmail on organization owned computers or equipment. While this may be seen as overly restrictive, it should be noted that personal email accounts often do not have the technical

safeguards or the level of traceability an organization might require. Explaining the motivation behind the policy directives helps the employee empathize with management tasked with implementing and enforcing the policy.

RESEARCH METHODOLOGY

The bottom line is that adopting a formal information security policy is an essential foundation for the overall information security infrastructure [5, 21]. Kolb and Abdullah [16, p.107] put it best, "Any organization [can] have an exceptional state-of-the-art hardware network security protection, but it may take only an uneducated user to download a virus that compromises the organization system or actually publishes confidential data…. Regardless of how secure a network may be, it is only as secure as its weakest link. Intentional or unintentional error by an employee that causes security incidents underline the importance of security awareness programs." Thus, a simple tactic to improving information security is to institutionalize proper behavior through a formal information security policy.

To gain a better understanding of measures that nonprofit organizations take to protect information, including security policies, a survey of nonprofit organizations in the Chicago, Illinois and Southern Illinois areas was conducted. Nonprofits were identified from publicly available lists online. Survey respondents were solicited from the organizations via email and asked to complete an online survey. Most of the individuals solicited were in administrative positions at the organizations and not specifically responsible for information technology or security. There were 154 nonprofit respondents who started the survey and 78 who completed it.

Table 1 - Characteristic of Nonprofits

Characteristic	Mean	Standard Deviation
Budget	$1,331,352	$2,158,211
IT Budget	$23,408	$87,491
Number of Employees	19.5	34.8
Employees Dedicated to IST	46.8%	56.2%

Table 1 shows the basic characteristics of the nonprofits that responded. The average yearly budget of the organizations was approximately $1.3 million dollars. On average, the nonprofits that responded reported employing about 20 people. Less than half of the organizations had employees dedicated to information technology or information security.

Table 2 provides an overview of the types of information that the nonprofits handle. Almost all the nonprofits reported handling names, addresses, and phone numbers. Over half (53.7%) reported handling birth dates. Approximately one-third of the organizations handle social security numbers. Income related data was handled by 27.4% of the organizations while 20.8% processed health records and 11.5% processed crime data.

Table 2 - Percentage of Organizations Handling Different Types of Information

	Percent	Standard Deviation
Names	97.8	14.4
Addresses	94.7	22.4
Phone Numbers	89.5	30.9
Birth Dates	53.7	50.1
Social Security Numbers	31.6	46.7
Health Records	20.8	40.9
Criminal Records	11.5	32.2
Income	27.4	44.8

RESULTS

The first objective of the study is to describe how nonprofits view information technology and security. As already indicated above, many organizations do not employ people to support information technology, yet many organizations handle sensitive information as they serve their clients. Table 3 supports the opinion that nonprofits do not understand the importance of putting policies in place to help protect information. When asked if their organization has an information security policy, only half (56.4%) of the organizations surveyed reported having an information security policy. What is even more concerning is that many of these organizations have had incidents affecting their information security. Approximately two-thirds (67.3%) of the organizations surveyed reported having at least one incident (many had multiple) affecting their information security. Such incidents include viruses, spyware, malware, data theft, and hardware or software failure. Just over 90% of the organizations acknowledge there are risks associated with their organization's information and technology assets. However, that indicates roughly 10% of the organizations do not recognize the potential risks.

Table 3 - Organizations That Have Information Security Policy and Identify Security Risks

Variable	Percent	Standard Deviation
Information Security Policy	56.4	49.9
Risk	90.1	30.0
Incident	67.3	47.4

Who Adopts Information Security Policies?

Given that only half of the sample has an information security policy, it is important to consider why some organizations have information security policies and others do not. Since the sample size is small, it is not possible to control for many confounding factors at one time, but nonetheless a reasonable conclusion can be sought to explain the adoption of an information security policy. Chi-square tests are a useful starting point for understanding which organizations adopt an information security policy.

The first item examined is the relationship between budget size and adoption of an information technology security policy. For analysis purposes, budgets are coded at three different levels: small (budgets less than $100,000), medium (budgets between $100,000 and $1,000,000) and large (budgets greater than $1,000,000). A Chi-square test between budget size using these three categories and the adoption of an information technology security policy reveals there is a strong relationship, $X^2(2, N=64)=16.6$, $p<0.001$. This is not truly surprising given that nonprofits

with larger budgets likely have more at stake and more resources to put into developing an information security policy.

However, there is no relationship between whether the organization perceives there is a potential risk to information security and adopting an information technology security policy, $X^2(1, N=81)= 0.04$, p=0.84. Likewise, having a past incident that affected the organization's information security does not seem to be related to whether an organization has an information technology security policy, $X^2(1, N=49)= 0.25$, p=0.61.

One would expect that organizations that deal with sensitive information would be more careful with how information is handled and thus have an information security policy outlining proper information security procedures in place. The organizations were asked about the different kinds of information they handled (see Table 2). Of these, we classify social security numbers and health records as sensitive information. Organizations that handle sensitive information are coded as 1 and 0 otherwise. A Chi-square test shows that handling sensitive information and having an information technology security policy are not related, $X^2(1, N=94)=1.79$, p=0.18. This is concerning as we should expect that organizations handling sensitive information would take steps to ensure its security.

Table 4 assesses the factors that influence an organization to adopt an information security policy. The dependent variable is dichotomous, taking the value of 1 if the organization has adopted an information technology security policy and 0 otherwise. Since the dependent variable is a binary measure, a logit model is appropriate. A logit model will predict the probability that an organization adopts an information technology security policy. The explanatory variables are total budget of the organization, amount of budget dedicated to information technology, perceived risk, and the handling of sensitive data. The budget variable is the size of the organization's budget in $100,000. The amount of budget dedicated to information technology is measured in $10,000. Perceived risk is coded as 1 if the organization reported there was a risk of data loss, a loss of productivity, hardware damage, identity theft, a general decrease in security level, a loss of reputation, or legal action. The variable is coded 0 otherwise. The variable for sensitive data is coded as 1 if the organization reported handling social security numbers or health records and 0 otherwise.

Table 4 - Predicting the Adoption of an Information Security Policy

	β	Standard Error	Odds Ratio
Intercept	-3.83	1.97	0.02
Budget of Organization	0.48*	0.20	1.61
IT Budget	1.78	1.08	5.92
Perceived Risk	2.23	1.80	9.27
Sensitive Data	-1.17	0.92	0.31
Pseudo R2	.66		
*p < .05 (two-tailed)			

In Table 4 it is quickly apparent that the size of an organization's budget is important in predicting if it has an information technology security policy. As the size of an organization's budget increases, as denoted by the positive logit coefficient (B), so does the probability the organization has an information security policy. One alarming conclusion drawn from the data is that handling sensitive data does not lead an organization to adopt an information security policy. Likewise it does not appear that organizations are driven by risks to information security or prior incidents that have affected information security as denoted by the large standard error associated with the coefficient for risk.

The odds ratio on the last column of Table 4 illustrates just how important the size of the organization's budget is to the adoption of an information security policy. A one-unit increase ($100,000) in an organization's budget leads to a

61% increase in the odds that an organization has an information security policy. Even more telling, a one standard deviation increase in an organization's budget leads to a 3220% increase in the odds that an organization adopts an information security policy.

Budget size is likely a proxy for a variety of factors that increase the likelihood of adopting an information security policy. For example, a larger budget often means organizations offer a more competitive salary, leading to a more professionalized staff that is attuned to issues such as information security. Additionally, a larger budget means an organization has more resources to spend on training and security infrastructure. This discussion relates to the null findings for risk. Organizations may understand that a risk to their information security exists, but since they lack the resources and/or expertise to deal with security issues they do not place information security as a priority.

CONCLUSIONS

While it is true that perceived cost and lack of need are barriers for small and medium size organizations in developing and adopting a formal information security policy, it can be argued this preventative measure is the most cost effective information security protection an organization can implement. Human error is a great risk to information loss and implementing simple policies and procedures reduces such risks. For the vast majority of nonprofits, hiring an expensive security expert or purchasing pricey security technologies is not necessary or cost effective because they do not deal with large amounts of highly sensitive information. In such cases, utilizing available information security templates may be sufficient. There are a host of resources, such as The Information Security Policy Project by SANS [25] that offer policy templates that are more than adequate for many nonprofits. Organizations can routinely monitor and enforce policy compliance to ensure that employees are maintaining security provisions. Routine training and discussion of information security policies and practices is another means of ensuring the topic is on the minds of employees or volunteers as they perform their duties.

While it is understandable that nonprofits tend not to focus significant time, efforts, or funds on information security—after all, their social mission is central to their existence—there is good reason to improve information security other than in reducing the potential of exposing individuals to fraud. At the core of the nonprofit sector's existence is public trust. If the public cannot trust nonprofit organizations to properly handle information, the public will put faith elsewhere. The nonprofit sector's future is directly tied to increases in technology and information. The rise of policy networks means nonprofit organizations will need to share sensitive information with other organizations—most likely via electronic technologies and mediums. Additionally, fundraising efforts are increasingly employing digital technology such as internet sales, credit card transactions, and automatic bank withdrawals. This is in addition to the normal rise in technology in the workplace. If an organization has a major breach in information security, their reputation with other organizations and the public could be jeopardized, which in turn can have a substantial impact on their ability to do business.

The implementation of an information security policy, while less technical than other safeguards, is the building block for an organization's complete security picture, helps ensure employees know what is expected, and can serve to reduce liability in the event of a security incident. A future line of research should address the differences in the complexity and stringency of information security policies and what these differences mean in regards to protecting nonprofit organizations.

REFERENCES

1. Anderson, R. (2001). Why information security is hard-an economic perspective. *Proceedings from 17th Annual Computer Security Applications Conference* (pp. 358–365). Washington, DC: IEEE Computer Society.
2. 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.
3. Behn, B., DeVries, D., & Lin, J. (2007). Voluntary disclosure in nonprofit organizations: An exploratory study. *Available at SSRN 727363*.
4. British Columbia Office of the Government Chief Information Officer. (2012). Information Security Policy. Retrieved from http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf
5. 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.

6. 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
7. Denhardt, J. V., & Denhardt, R. B. (2011). The new public service: Serving, not steering. New York: ME Sharpe.
8. Dojkovski, S., Lichtenstein, S., & Warren, M. (2012). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. *Proceedings of the 15th European Conference on Information Systems* (pp. 1560–1571). St. Gallen, Switzerland: University of St Gallen.
9. 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/.
10. Federal Trade Commission. (2010). Consumer sentinel network data book. Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf.
11. Fitzgerald R. (2004, June 27) Not for profit, not for volunteers[Radio broadcast episode]. *Summer Series. Australian Broadcasting Corporation.*
12. Gupta, B., Dasgupta, S., & Gupta, A. (2008). Adoption of ICT in a government organization in a developing country: An empirical study. *The Journal of Strategic Information Systems*, 17(2):140–154.
13. 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.
14. Hrywna, M. (2007). Nonprofits and data breaches. *The Nonprofit Times.* Retrieved from http://www.thenonprofittimes.com/news-articles/nonprofits-and-data-breaches/.
15. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3):549.
16. Kolb, N., & Abdullah, F. (2009). Developing an information security awareness program for a non-profit organization. *International Management Review*, 5(2):103–108.
17. Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with healthcare information technology. *28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (pp.5453– 5458). New York: IEEE.
18. Mirza, A. A. (2010). Failure and success factors of an information system development in a charitable organization. *Global Journal of Management And Business Research*, 10(3):79-83.
19. Nobles, M. (2008). Ensuring Donors Goodwill. *The Nonprofit Times.* Retrieved from http://www.thenonprofittimes.com/news-articles/insuring-donors-goodwill/.
20. Picanso, K. E. (2006). Protecting information security under a uniform data breach notification law. *Fordham Law Review*, 75(1):355-390.
21. Petel, J. (2004) Information security for churches and small non-profit organizations. Retireved from http://www.sans.org/reading_room/whitepapers/basics/information-security-churches-small-non-profit-organizations_1373.
22. Reyes, C. (2005). What makes a good security policy and why is one necessary? Retrieved from http://www.giac.org/paper/gsec/1691/good-security-policy-necessary/103074
23. Richardson, R. (2008) Computer crime and security survey. Retrived from http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf.
24. Saxton, G. D., & Guo, C. (2011). Accountability online: Understanding the web-based accountability practices of nonprofit organizations. *Nonprofit and Voluntary Sector Quarterly*, 40(2):270–295.
25. SANS. SANS Security policy project. Retrieved from http://www.sans.org/security-resources/policies/.
26. Smith, S. and Jamieson, R. (2006). Determining key factors in e-government information system security. *Information Systems Management*, 23(2):23– 32.
27. West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, 64(1):15–27.
28. Willis, L. (2002) Security policies: where to begin. Retrieved from http://www.sans.org/reading_room/whitepapers/policyissues/security-policies_919.