SAIS 2022 Proceedings

Southern (SAIS)

4-1-2022

Cybersecurity In Nonprofits: Factors Affecting Security Readiness During Covid-19

Natalia Ermicioi
Marymount University, nermicio@marymount.edu

Michelle Xiang Liu
Marymount University, xliu@marymount.edu

Recommended Citation

Ermicioi, Natalia and Liu, Michelle Xiang, "Cybersecurity In Nonprofits: Factors Affecting Security Readiness During Covid-19" (2022). *SAIS 2022 Proceedings*. 18.
https://aisel.aisnet.org/sais2022/18

CYBERSECURITY IN NONPROFITS: FACTORS AFFECTING SECURITY READINESS DURING COVID-19

Natalia Ermicioi
Marymount University
nermicio@marymount.edu

Xiang (Michelle) Liu
Marymount University
xliu@marymount.edu

ABSTRACT

While cybersecurity is a widely accepted concept, there is much doubt about its application in the nonprofit sector. Numerous studies demonstrate the prevalence of data loss and the critical need for nonprofit organizations to safeguard information assets. Yet the literature acknowledges the concerns that NPOs are usually understaffed and underfunded, rely on volunteers rather than paid professional staff, and lack the skills and infrastructure necessary to establish and sustain security best practices. COVID-19 Pandemic exacerbates this situation to a great extent. This paper seeks to explore whether the factors such as NPOs annual budget size and number of employees impact NPOs cybersecurity readiness during unprecedented circumstances of COVID-19. Survey data from 65 nonprofit organizations was collected and analyzed to gain better understanding of factors impacting cybersecurity readiness of those organizations. Implications for future research and practice are also discussed.

Keywords

Nonprofits, cybersecurity, COVID-19, budget, employees, policy, process, people

INTRODUCTION

Similar to their for-profit counterparts, nonprofit organizations (NPOs) actively use various data collection practices in their operational activities, considering the need for data sharing between multiple sectors. The nonprofit industry was encouraged to gather data in order to plan ahead and establish focused marketing and fundraising strategies (Imboden et al., 2014). While the collected data is helping the NPOs to align with the current technology use, it also makes them vulnerable and at-risk to malicious cyber activities (Ermicioi & Liu, 2021). Therefore, the likelihood of NPO data leakage increases as a result of digital engagement with donors, beneficiaries, the general public, and partners (Imboden et al., 2013) and engagement in other types of activities such as e-commerce on their websites.

According to prior research, creating security controls for nonprofits is just as vital as building strategies, tools, and policies for major enterprises or small and mid-size enterprises (SMEs) (Ermicioi & Liu, 2022).

The present research was conducted initially as part of the author's dissertation work at Marymount University. The current paper represents an extension of Chapter 4 of the author's D.Sc. Thesis (Ermicioi, 2020). The present paper describes only two out of three Independent Variables (IV) of the author's D.Sc. Thesis.

CONCEPTUAL BACKGROUNDS AND RESEARCH HYPOTHESIS

A study conducted by Imboden et al. (2013), later extended in Imboden et al. (2014), surveyed 78 nonprofit organizations in Chicago, Illinois and Southern Illinois and concluded that a nonprofit's budget size can primarily determine whether that organization has an information security policy or not (Imboden et al., 2014). Additionally, the authors highlighted that a unit of $100,000 increase in an NPO's budget might result in 61% increase of the likelihood that that organization has an information security policy (Imboden et al., 2013).

On the other hand, NPOs are frequently understaffed and rely on volunteer work for essential tasks. Suykens, Verschuere, & Rynck (2017) noted that volunteers are recruited by nonprofit organizations for permanent roles, a method considered unacceptable by SMEs. Their study discovered that because of necessity, NOPs staff members have to take on a variety of roles as well as perform a broad range of tasks, putting the organizations in vulnerable positions. Additionally, NPOs fear overpricing when outsourcing technology-related services, therefore, IT-related needs are often handled in-house in NPOs in spite of understaff or deficiency of required IT skills.

The Dependent and Independent Variables

The study used two independent variables (IV) directly derived from the literature review: (1) the size of the annual budget and (2) the number of employees. The dependent variables (DV) used in the study (as shown in Table 1) have been sourced from ISO (International Organization for Standardization) 22301:2019 (EN) Security and Resilience — Business Continuity Management Systems (BCMS): (1) Policy; (2) People; and (3) Processes referred in the paper as the 3Ps (ISO, 2019). Each of the DVs is to assess the cybersecurity measures taken by the NPOs from a different perspective. For the purpose of this study, each individual "P" (Policy, People, and Process) is considered a cluster variable (Multiple Dependent Variable) consisting of (4) four adjacent dependent variables. Each adjacent variable corresponds to the survey items (question number) in the study instrument and has been intentionally named as Policy1, Policy2, Policy3, Policy4; People1, People2, People3, People4; and Process1, Process2, Process3, Process4. Table 1 below shows the construction. Appendix A includes an excerpt of the survey instruments.

	Cluster Components	Scale
Policy	Policy1, Policy2, Policy3, Policy4	5-Point Likert Scale
People	People1, People2, People3, People4	5-Point Likert Scale
Process	Process1, Process2, Process3, Process4	5-Point Likert Scale

Table 1. Construction of Dependent Variables

The Research Questions and Hypothesis

In summary, budget and staff limitations are considered the primary concerns developed in the current study by adapting the concepts to the unprecedented circumstance of Covid-19. Therefore, the current research paper seeks to respond the following research questions (RQs):

RQ1: Is there a relationship between the size of the annual budget of an NPO and the cybersecurity measures (3Ps) taken by an NPO during COVID-19?

RQ2: Is there a relationship between the number of employees of an NPO and the cybersecurity measures (3Ps) taken by an NPO during COVID-19?

The research used the following null hypothesis:

Hypothesis 1_{null}: The size of the annual budget has no effect on people aspect of cybersecurity readiness.
Hypothesis 2_{null}: The size of the annual budget has no effect on process aspect of cybersecurity readiness.
Hypothesis 3_{null}: The size of the annual budget has no effect on policy aspect of cybersecurity readiness.
Hypothesis 4_{null}: The number of employees has no effect on people aspect of cybersecurity readiness.
Hypothesis 5_{null}: The number of employees has no effect on process aspect of cybersecurity readiness.
Hypothesis 6_{null}: The number of employees has no effect on policy aspect of cybersecurity readiness.

Figure 1 is a representation of the Research Model that includes the IVs -Size of the Annual Budget and Number of Employees; the Multiple Dependent Variables with their corresponding cluster components, and the Research Hypotheses. Refer to Appendix B for a higher resolution.

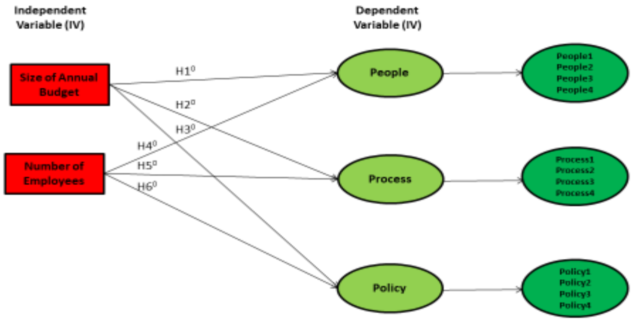


Figure 1. The Research Model with the Corresponding Cluster Components

RESEARCH METHODOLOGY

The Research Design

The study used a quantitative, nonexperimental survey research approach. A snowball strategy was adopted to collect the necessary data. The response rate to the survey was tracked via a chain of custody. The data analysis process used a total of sixty-five (65) valid responses. The respondents self-identified as "members of the NPO's leadership team," and they expressed their perceptions of their organization's cybersecurity preparedness during COVID-19 through the survey.

The study used an existing, previously utilized instrument – the National Cyber Security Alliance (NCSA) survey for assessing SMEs' cybersecurity practices (2020). The instrument was obtained directly from the NCSA's website, and no particular permission was necessary according to their Public License Grant to Use Website Contents. This study's instrument replaced the original instrument's "small business/business" with "nonprofit" and added a time frame statement: "during COVID-19." The current research study counted on the original instrument's internal and external reliability.

The Population

The study considers nonprofit organizations located in the D.C., Maryland, and Virginia (DMV) area as its target population and used corresponding ZIP Codes to determine the NPOs located in the designated geographic area. According to the current project's research design, the only organizations that have been considered are those that are registered 501(c)(3) organizations that fulfill the following criteria: (1) an annual income of less than $49,999,999; (2) a primary exempt activity serving human beneficiaries; and (3) a number of employees less than 250 (IRS, 2019). Additionally, only organizations that filed taxes with the IRS in 2019 were considered, as their information is publicly available on the IRS website during the time of this survey study being conducted.

RESULTS

IBM's SPSS Statistics software, version 26.0, was used to perform the data analysis. The study used Descriptive Statistics, Correlation, and Multiple Dependent Variable Linear Regression analysis to examine the research questions and test hypotheses. Appendix C includes a table with the scales of the independent variables. Table 2 below describes the characteristic of the NPOs sample through the Descriptive Statistics:

Variable	Scale	Mean	Standard Deviation	Minimum	Maximum
Size of Annual Budget	Size	5.62	2.993	1	12
Number of Employees	Number	1.83	1.183	1	4

Table 2. Descriptive Statistics

To establish the possible relationship between IV and DV, the study used a common correlation test used in social science research - Pearson’s correlation; its corresponding coefficient (r) is used to establish if two variables are “correlated or related to each other.” Frequently utilized interpretations of the r values are enumerated as follows (Akoglu, 2018): 1- Perfect; 0.7 – 0.9 – Strong; 0.4 – 0.6 – Moderate; 0.1 – 0.3 –Weak; 0-Zero. Table 3 illustrates the results of the Pearson’s correlation analysis:

	Sig. (2-tailed)		
	Correlation		
Size of Annual Budget	Pearson Correlation	1	
	Sig. (2-tailed)		
	Correlation		
Number of Employees	Pearson Correlation	.114	1
	Sig. (2-tailed)	.366	
	Correlation		
People1	Pearson Correlation	.252*	.361**
	Sig. (2-tailed)	.043	.003
	Correlation	Weak	Weak/Moderate
People2	Pearson Correlation	.128*	.378**
	Sig. (2-tailed)	.003	.002
	Correlation	Weak	Weak/Moderate
People3	Pearson Correlation	.277*	.318**
	Sig. (2-tailed)	.025	.010
	Correlation	Weak	Weak/Moderate
People4	Pearson Correlation	.327**	.295*
	Sig. (2-tailed)	.008	.017
	Correlation	Weak/Moderate	Weak
Process1	Pearson Correlation	.395**	.226*
	Sig. (2-tailed)	.001	.043
	Correlation	Weak/Moderate	Weak
Process2	Pearson Correlation	.220*	.338**
	Sig. (2-tailed)	.048	.006
	Correlation	Weak	Weak/Moderate
Process3	Pearson Correlation	.189*	.197*
	Sig. (2-tailed)	.025	.025
	Correlation	Weak	Weak
Process4	Pearson Correlation	.093	.388**
	Sig. (2-tailed)	.045*	.001
	Correlation	Weak	Weak/Moderate
Policy1	Pearson Correlation	.497**	.240*
	Sig. (2-tailed)	.000	.025
	Correlation	Moderate	Weak
Policy2	Pearson Correlation	.095*	.360**
	Sig. (2-tailed)	.045	.003*
	Correlation	Weak	Weak/Moderate
Policy3	Pearson Correlation	.434**	.293*
	Sig. (2-tailed)	.000	.018
	Correlation	Moderate/Strong	Weak
Policy4	Pearson Correlation	.384**	.350**
	Sig. (2-tailed)	.002	.004
	Correlation	Moderate/Strong	Moderate/Strong

Table 3. Correlations IV and DV

And finally, to determine the effect of the IV on the DV, the Wilks' Lambda test was used. Wilks' Lambda is a widely accepted social scientific statistical test utilized in multivariate analysis of variance (Multiple Dependent Variable Linear Regression). Wilks' Lambda test tests the null hypothesis and considers the following two conditions simultaneously (Northern Arizona University (NAU), 2020): (1) Box's Test of Equality of Covariance Matrices, which tests "the assumption of homogeneity of covariance across the groups." In the case of a value lower than 0.05, the significance value, the assumptions are not met (IBM, 2020). (2) Wilks' Lambda has a significance level lower than 0.05 for the assumptions to be met (Northern Arizona University (NAU), 2020).

The results of the Multiple Dependent Variable Linear Regression test are presented in Table 4.

Independent Variable/Fixed Factor		Box's Test of Equality of Covariance Matrices (Sig.>0.05)	Wilks' Lambda value	(Sig. <0.05)	Null Hypothesis
Number of Employees	People	.470 (pass)	.537	0.002 (pass)	(rejected)
Number of Employees	Policy	.360 (pass)	.532	0.002 (pass)	(rejected)
Number of Employees	Process	.505 (pass)	.552	0.045 (pass)	(rejected)
Size of Annual Budget	People	.809 (pass)	.333	.042 (pass)	(rejected)
Size of Annual Budget	Policy	.141 (pass)	.257	.002 (pass)	(rejected)
Size of Annual Budget	Process	.280 (pass)	.328	.050 (pass at limit)	(rejected)

Table 4. The Multiple Dependent Variable Linear Regression Test

Box's Test of Equality of Covariance Matrices (Sig.>0.05) proved that the test was appropriate for the design.
The Wilks' Lambda for the study's variables is calculated to be ranging from 0.257-0.557 with an associated level of statistical significance, or p-value, ranging from 0.002 to .050 - all constructs passed the cutoff (Sig.>0.05) (SagePub, 2019). This low p-value (under 1.00 (PennSate, 2021) would lead us to reject the null hypothesis and conclude that Number of Employees and Size of Annual Budget has an effect on the 3Ps during Covid-19. The six null hypotheses have been rejected, as shown in Table 4.

DISCUSSION

As the literature predicted, budget limitations indeed are among the biggest challenges that NPOs face when considering the investment in cybersecurity programs. On the other hand, the literature acknowledges the concern that NPOs have limited staff and resources (Ermicioi, 2020). According to Haight (2020), NPOs are frequently "understaffed," engage volunteers instead of paid professional staff, and face the challenges of expertise shortages and little infrastructure support to sustain cybersecurity best practices.

As Correlation analysis and the Multiple Dependent Variable Linear Regression test show, there is a relationship between the number of employees of an NPO and the cybersecurity measures (3Ps) taken by an NPO during COVID-19, and there is a relationship between the size of the annual budget of an NPO and the cybersecurity measures (3Ps) taken by an NPO during COVID-19. Given that fact that small NPOs (small annual budget, lower number of employees) have lower readiness and awareness level regarding cybersecurity during crises, more attentions need to be directed to those organizations because they are more vulnerable to cyber-attacks in compared to other entities. Therefore, more emphasis and cyber awareness activities or actions should target them, as well as resources that can help increase the readiness and awareness level.

CONCLUSIONS

The authors acknowledged the limitations of this study as summarized below. First, the current project's sampling procedure, nonprobability sampling, does not control for selection bias and does not permit sampling error calculation (Singleton & Straits, 2018). Therefore, the current research project is considered an exploratory study aiming to enlarge the limited body of knowledge on the topic rather than an in-depth explanatory study. However, a variety of bias reduction methods have been used. Second, the current study used a small sample size to accomplish the research goal. Therefore, caution must be used when discussing the generalizability of results, especially when extrapolating results onto a larger population. Third, the research study targeted NPOs located in the Washington, DC-Maryland-Virginia (DMV) area with less than 250 employees and an annual budget of less than $50 million. Therefore, precaution must be taken when discussing the applicability of the findings to organizations outside the boundaries mentioned above. Lastly, the research project targeted organizations that have primarily human beneficiaries. Therefore, organizations labeled with letter code C: Environmental Quality, Protection and Beautification and D: Animal-Related according to the National Taxonomy of Exempt Entities (NTEE) code (IRS, 2020) have been excluded, as well as other organizations that do not describe themselves as having "human beneficiaries." Considering the above limitations of the study, a suggestion for future work would be to collect additional data through a different methodology such as collecting qualitative data through interviews and triangulate the findings.

In summary, small NPOs should have higher cybersecurity awareness and establish information security practices to ensure the safeguard of their informational assets. Furthermore, these entities should be supported through free or affordable cybersecurity programs since they face budget limitations and restrictions as their income is social mission-oriented.

REFERENCES

1. Akoglu, H. (2018). User's guide to correlation coefficients. *Turkish Journal of Emergency Medicine*, *18*(3), 91-93. https://doi.org/10.1016/j.tjem.2018.08.001
2. Ermicioi, N. (2020). *Factors affecting nonprofits' information security readiness during crises: A study of COVID-19's impact on small and medium nonprofit organizations (NPOS) in the DMV area* (Publication Number Order No. 28414637). Marymount University]. Available from ProQuest Dissertations & Theses Global. (2524374134). https://www.proquest.com/docview/2524374134?pq-origsite=gscholar&fromopenview=true
3. Ermicioi, N., & Liu, X. (2021). An Interdisciplinary Study of Cybersecurity Investment in the Nonprofit Sector. *American Journal of Management*, *21*(5), 39-50. https://doi.org/10.33423/ajm.v21i5.4728
4. Ermicioi, N., Liu, X., (2022). *Level of Cybersecurity Readiness of Small and Medium Nonprofit Organizations (NPOs) During COVID-19*. Proceedings of 51st SEDSI (Southeast Decision Science Institute).
5. Haight, L. (2020). NonProfit Hacks: Too small to be hacked? Not! https://digitalthinkingsc.com/blog/2015/7/2/nonprofit-hacks-most-at-risk-least-prepared
6. IBM. (2020). KMO and Bartlett's test. https://www.ibm.com/support/knowledgecenter/en/SSLVMB_subs/statistics_casestudies_project_ddita/spss/tutorials/fac_telco_kmo_01.html
7. Imboden, T., Phillips, J., Seib, J., & Fiorentino, S. (2014). Information Security in Nonprofits: A First Glance at the State of Security in Two Illinois Regions. *Journal of Information Systems Applied Research*, *7*(2), 29-38. http://jisar.org/2014-7/N2/JISARv7n2p29.html
8. 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. https://doi.org/10.48009/2_iis_2013_166-173
9. IRS. (2019). Exempt Purposes - Internal Revenue Code Section 501(c)(3). https://www.irs.gov/charities-non-profits/charitable-organizations/exemptpurposes-internal-revenue-code-section-501c3
10. ISO. (2019). ISO 22301:2019 (EN) Security and Resilience — Business Continuity Management Systems-Requirements. https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en
11. Northern Arizona University (NAU). (2020). Interpreting The One-Way MANOVA. http://oak.ucc.nau.edu/rh232/courses/EPS625/Handouts/Interpreting%20the%20One-way%20MANOVA.pdf
12. PennSate. (2021). 8.3 - Test Statistics for MANOVA. https://online.stat.psu.edu/stat505/lesson/8/8.3
13. SagePub. (2019). 8.3 - Learn About Wilks' Lambda in SPSS With Data From the Global Health Observatory (2016). https://methods.sagepub.com/base/download/DatasetStudentGuide/wilks-in-gho-2016
14. Singleton, B., & Straits, B. (2018). *Approaches to Social Research* (5th ed.). Oxford University Press.

15. Suykens, B., Verschuere, B., & De Rynck, F. (2017). Organizational Hybridity in Flemish Civil Society Organizations: Past Developments, Present Trends and Future Research Possibilities. In *CSI Flanders Working Paper 3*. Ghent: Ghent University

16. The National Cyber Security Alliance. (2020). A new survey released by the National Cyber Security Alliance (NCSA). https://staysafeonline.org/small-business-target-survey-data/

Appendix A – The Survey Instrument: BCMS Components

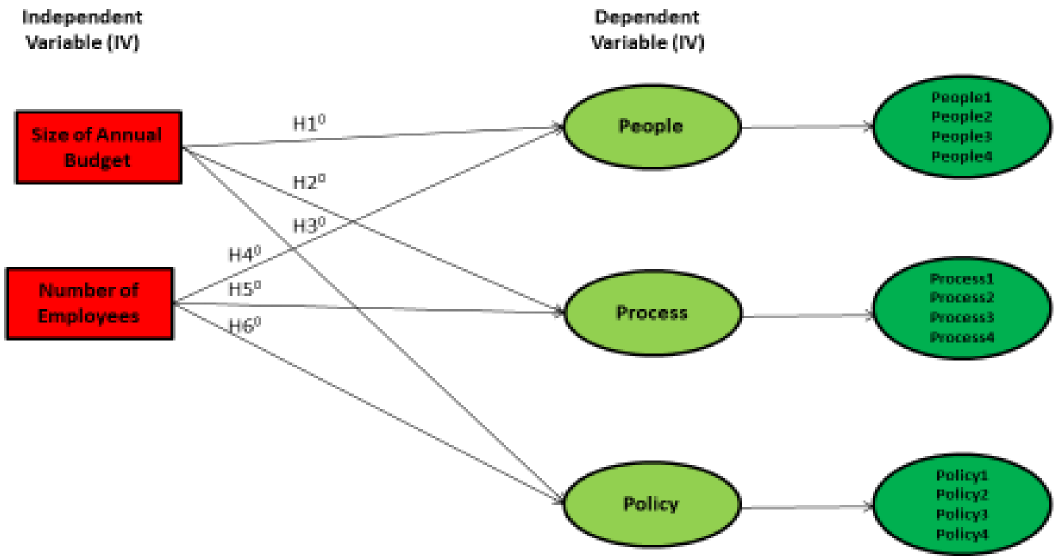
Statement	Component – People	Scale
What level of support do you have for your organization's cybersecurity during COVID-19?	People 1	5-Point Likert Scale
The organization's senior management consistently emphasizes the importance of cybersecurity during COVID-19	People 2	5-Point Likert Scale
Most employees are sophisticated about detecting spear-phishing and other kinds of intrusion attempts during COVID-19	People 3	5-Point Likert Scale
On average, how many hours of cybersecurity training do you require per employee during COVID-19?	People 4	5-Point Likert Scale

Statement	Component – Process	Scale
Does your organization have a clearly articulated process for employees to report potential cyber threats to leadership during COVID-19?	Process 1	5-Point Likert Scale
Does your organization have a clearly articulated business process that outlines how employees should securely dispose of equipment and data during COVID-19?	Process 2	5-Point Likert Scale
If you were to have a data breach or cybersecurity incident during COVID-19, does your organization have a response process you can immediately put into action?	Process 3	5-Point Likert Scale
If you were to have a data breach or cybersecurity incident during COVID-19 and lose access to your computers and network, do you have a process to initiate manual or backup procedures to continue operating your organization?	Process 4	5-Point Likert Scale

Statement	Component – Policy	Scale
Does your organization have a clearly defined and documented cybersecurity policy during COVID-19?	Policy 1	5-Point Likert Scale

If the organization had a computer system business continuity or disaster recovery policy before, was it updated in 2020?	Policy 2	5-Point Likert Scale
Which best describes the knowledge management of cyber security policy in during COVID-19?	Policy 3	5-Point Likert Scale
The organization has a clear, well-established policy for escalating suspicious events during COVID-19.	Policy 4	5-Point Likert Scale

Appendix B - Figure 1. The Research Model with the Corresponding Cluster Components



Appendix C – Independent Variables Scales - Size of Annual Budget and - Number of Employees

Scale	IV1 - Number of Employees
1	1-10 employees
2	11-50 employees
3	51-100 employees
4	101-250 employees
	IV2 - Size of Annual Budget
1	Below $100,00
2	$100, 000 - $250, 000
3	$250, 001 - $500, 000
4	$500, 001 - $1 million

5	$1 - $2 million
6	$2 - $5 million
7	$5 - $10 million
8	$10 - $15 million
9	$15 - $20 million
10	$25 - $30 million
11	$30 - $35 million
12	$35 million - under $50 million
13	Over $50 million (not considered in the data analysis)