Addressing the Cybersecurity Issues and Needs of Rural Pennsylvania Nonprofit Organizations

Brian Gardner
Penn State Schuylkill
Penn State University
Schuylkill Haven, U.S.
bkg113@psu.edu
0000-0003-1647-5943

Maryam Roshanaei
Penn State Abington College
Penn State University
Abington, U.S.
mur45@psu.edu
0000-0003-4246-3479

J. Andrew Landmesser
Penn State Brandywine
Penn State University
Media, U.S.
jal620@psu.edu
0000-0002-0006-2768

Jennifer Breese
Penn State Greater Allegheny
Penn State University
McKeesport, U.S.
jzb545@psu.edu
0000-0003-0792-2713

Michael Bartolacci
Penn State Berks College
Penn State University
Reading, U.S.
mrb24@psu.edu
0000-0002-0817-4270

***Abstract*—The need for cybersecurity competence has become a strategic area for all types of organizations, be it large or small, for profit or nonprofit. This is an area of particular concern for smaller nonprofit organizations; and especially for those in rural areas with limited resources to address their cybersecurity risks. Cyber-attacks wreak havoc on the networks and systems for services provided to nonprofit consumers. The problems associated with various types of attacks, from outside nefarious individuals/groups or internal personnel, are particularly difficult for nonprofits in rural communities with limited resources for cybersecurity infrastructure and limited staff proficient in cybersecurity knowledge and skills. We have developed a cybersecurity assessment process to ascertain key needs and weaknesses with respect to cybersecurity for nonprofits in such rural communities in Pennsylvania. Additionally, this grant-sponsored work-in-progress research aims to provide guidance to rural nonprofits with "best practices" and related content that can be easily implemented despite their limitations.**

***Keywords*—nonprofit, survey, Cybersecurity, rural**

I. INTRODUCTION

Nonprofit organizations (NPOs) play a vital role in promoting more equitable and thriving communities. Over 1.3 million NPOs [1] operate in the United States providing food, shelter, and education as well as fostering civic engagement and leadership, and driving economic growth for people of every age, gender, race, and socioeconomic status. The impact of NPOs drives economic growth with 12.3 million [1] employments that consume $1 trillion [2] annually for goods and services such as medical equipment. More than 92% [2] of NPOs are small, community-based, and serve local needs. With a primary focus of avoiding financial loss and reputational damage, cybersecurity readiness is at the forefront of many organizations [3]. Yet, NPOs are largely overlooked despite the fact that they collect and store incredibly sensitive data about their donors and volunteers which may include health records, social security numbers, personal information, confidential emails, resources and billing information. Lincke [4] addressed how smaller organizations with limited IT staff can determine security threats, prioritize risks, conform to required regulations in their industry, and plan appropriate defenses. The recent wave of cyberattacks on NPOs amplifies the need for investment in fraud protection and security to prevent data breaches and access to sensitive demographic and financial information which are a gold mine for cybercriminals. Lack of enforced safeguards and cybersecurity readiness not only results in vulnerabilities and threats for NPOs, but it also creates a loss of faith and a sense of not being valued by donors and volunteers. NPOs have unique challenges in gaining the trust of donors and volunteers including the constant cycle of staff turnover, fraudulent transactions, secure access to the technology ecosystem, and data breach procedures. A recent study shows [5] that 45% of NPO employees intend to leave their positions within the next five years creating a loss of cybersecurity and technology adoption knowledge. Additionally, with organizational global fraud losses of over $21 billion annually [6], NPOs should focus on applying current security standards to online donation forms, securing peer-to-peer donations without NPO connection, and complying with security, authentication, and dispersal compliance. In parallel, the NPOs must address security and access to the technology ecosystem. McAfee (2020) research from their Cloud Adoption and Risk Report (2020) [7], showed an increase of 50% in overall cloud services usage. The report indicates internal threats remained low whereas the number of threats from external actors increased by 630%, with the greatest concentration on collaboration services like Microsoft 365, Zoom and Cisco Webex. Yet, another study [8], showed that 55.6% of NPOs do not require multi-factor authentication. Furthermore, data access and breach procedure is another dangerous internal threat that has increased by 47% in 2020 and needs to be addressed by NPOs.

This project seeks to determine the current cybersecurity readiness of rural Pennsylvania NPOs. According to the Center for Rural PA [9], there are 48 rural and 19 urban counties in which a total of 49,632 NPOs [10] operate across a wide range of objectives and employ 15.7% of the overall population. Research conducted [6] indicated that Pennsylvania's rural NPOs were under financial stress, forcing them to significantly cut back on services and operational improvements. While no more current data exists, the effect of the COVID-19 pandemic is believed to have increased the level of financial stress on PA NPOs.

Previous work conducted in 2009 and 2020 [10] focused on rural PA local governments and NPOs respectively identifying common needs and vulnerabilities that can be addressed through specific policy recommendations relayed to the PA legislature and PA government agencies. The findings indicated the unfulfilled cybersecurity needs of such agencies are substantial. Even larger non-profit organizations such as the United Way do not have the overall budgets to devote to proper cybersecurity software, hardware, policies, and employee training. Non-profits do not have the funds to hire consultants or add employees to address cybersecurity issues.

In this project data was obtained from i) the Center for Rural Pennsylvania [9] - statewide and county data and analyses related to rural nonprofits, ii) TaxExemptWorld.com [12] - leading commercial nonprofit database widely used in nonprofit research, and iii) the National Council of Nonprofits [6] – provides information regarding current and emerging policy at the state and federal levels.

II. DISCUSSION OF SURVEY TO BE USED

The research team met to review the objectives of the research study to reach concurrence on a common baseline of understanding about the types of data we would need to collect to develop a solid set of recommendations. Each researcher entered their questions into a Word document stored in a Microsoft Teams space that had already been established to collect other deliverables produced from this research effort. The team has met multiple times to refine the wording and organize questions with related themes into multiple logical groupings and eliminate duplicates. The survey questions cover eight key areas:

1. Internal vs. External IT services and resources
2. Website security
3. IT and Security budgeting
4. Current risk environment
5. Business continuity/disaster recovery plan
6. Physical security
7. Logical access control
8. Inventory

One of the main challenges with the survey development is that we expect our survey to be completed by respondents with a wide range of knowledge – some with little or no IT or cybersecurity expertise with others who may be at the other end of the spectrum. As we fine tune each question, we have been careful to choose wording clearly communicating what type of data we are looking for and avoid excessive use of technical jargon. In cases where the use of technical jargon is unavoidable, we plan to include additional verbiage along with the question that offers the responder an explanation of any technical terms or concepts used so that they have enough information to answer the questions to the best of their knowledge. The additional verbiage will appear either as an annotation embedded in line with the question or in a separate hover text overlay that appears when the cursor moves over the question.

We are sensitive to the fact that some of the survey respondents may have limited knowledge about how IT/Cybersecurity policies and procedures are implemented within their organization, if at all. As such, they may encounter a question that they do not have the expertise to provide a concrete answer. For any questions where we ask for a “Yes”/”No” response, we will include an “I don’t know” option. Selecting an “I don’t know” option would seem like it would not be valuable input for our data collection, but in fact it may highlight an area within their operation that requires further investigation to determine whether there is a potential exposure from a cybersecurity perspective that needs to be addressed.

The survey also includes several open-ended questions allowing respondents to enter a free-form response. Our survey instrument provided its own rating of our survey quality from the early drafts of our question bank and generated a warning about how a large number of open-ended questions may depress response rates because it increases the time the respondent spends completing the survey. To address this, some of the open-ended questions were converted into multiple-choice questions. Having more discrete responses to our survey questions will also help us correlate the data and facilitate the formulation of well-founded recommendations. Furthermore, some of the multiple-choice options represent ranges (such as “between *x%* and *y%*”) to help organize the responses creating an ontology for more precise analysis. We will continue to verify that the ranges chosen correlate to widely accepted industry metrics within the context of what is being measured.

The ability to control the sequence and flow of the questions was also an important consideration in designing the survey. We will continue to evaluate each question to determine which questions require a response. Furthermore, some of the multiple-choice questions have been designed with logic to determine which question(s) will be displayed next based on the choice(s) selected. This logic will allow respondents the ability to skip over a single or an entire block of questions that may not be relevant to their organization or within the respondent’s domain of expertise to answer. The ability to offer the capabilities and features mentioned above were key considerations for selecting a survey tool.

Along with refining the survey content, the team discussed survey development and survey dissemination. Several popular survey creation tools were considered such as Google Forms, Microsoft Forms and Qualtrics, to name a few. All have robust features to support the content, logic, and security we plan to implement in our survey instrument. Qualtrics was chosen as the best survey tool for our needs because of the large number of question types that can be added, the ability to implement conditional logic to control the flow of questions based on a respondent's response, optimizing the look and feel of the survey for desktop and mobile use, and of course the extensive data collection and reporting capabilities. All the questions collected in the Word document have now been transferred into a Qualtrics survey and is continually updated in draft mode. Having the questions in Qualtrics has also made review sessions more efficient to edit questions in real-time, modify the question sequence and groupings instantly using the drag-and-drop capability, and preview how the survey will look to the respondents in desktop mode and mobile before distribution.

III. IDENTIFYING RURAL PA NONPROFITS

The research team is currently compiling a list of non-profit organizations using information published on the Center for Rural Pennsylvania [9], TaxExemptWorld.com [11], and the Pennsylvania Department of Community and Economic Development [14] websites. The Center for Rural Pennsylvania website [9] has several resources we used for determining which PA municipalities are classified as rural vs. urban. The county map provides a general classification of whether the county has a rural or urban designation. However, each PA county has dozens of municipalities within its borders with each one having their own specific rural vs. urban designation. Ultimately, we used a list published on this site that details which municipalities within each PA county are designated as rural vs. urban as our starting point for compiling the data we needed for this study. This table was imported into one of the tabs within an Excel spreadsheet that will drive our identification and distribution efforts.

The TaxExemptWorld.com site [11] contains a page that can generate a list of non-profit organizations by state and county. The search results include a list of non-profits operating in the county along with their address, non-profit classification, and financial information if available. A manual process was developed to capture the information from the search results and format it into our spreadsheet using some Excel programming. The search results from the TaxExemptWorld.com website did not include information to link the address to a specific county or municipality. We were able to correlate this information by entering the street address and city of the non-profit organization into a separate webpage on the PA Department of Community and Economic Development site [14] that does a lookup against their records and returns the county, municipality, and school district where the address is located. That information was then correlated with the table of municipalities we imported from the Center for Rural Pennsylvania extract to classify each non-profit organization by their rural/urban status.

The last step in the process will be to identify one or more primary contacts within each rural non-profit organization that we will target with our survey. Since none of the reference sources mentioned previously included contact information with our searches, identifying this information will largely be a manual process by visiting their websites if they exist or other publicly available information. If the survey recipient turns out to be someone not in the best position to provide responses, we will include verbiage to encourage that individual to redirect the survey to someone else in the organization with the expertise to complete the survey. Furthermore, we hope to reduce the number of surveys we distribute by identifying an individual contact at an umbrella organization that shares similar policies and procedures with other affiliated operations wherever they may be located. The contact information will also be recorded with the other profile data we captured into our Excel spreadsheet in the previous steps.

IV. SURVEY DISSEMINATION AND ANALYSIS OF DATA

Survey distribution will be through the identification of the umbrella organizations followed by a snowball method described by Biernacki and Waldorf [15] for recognition and recommendations within the identified rural organizations.

Qualtrics is the tool facilitating the survey instrument as well as the distribution and collection of results. Qualtrics has several features called "automations" to set up the distribution process. The Import Automation feature will allow us to organize our contact list into a format that can be imported into Qualtrics including the destination email address for the survey instrument. Configuration options will include linking the imported contact list to the distribution automation, setting the distribution schedule (options include immediate/delayed distribution as well as establishing criteria in Qualtrics for distribution frequency), linking the survey name in Qualtrics, customizing the email contact info and message body, setting the frequency of email reminders, and configuring the length of time the survey link will be available before it expires. Qualtrics can also be configured to generate reports directed to the research team when one of the scheduled automations runs to summarize which contacts were targeted for a specific automation run.

Qualtrics offers a Data and Analysis page that can be viewed if you are logged in with an account that has administrative privileges; survey responses can be viewed in a tabular format. The number of data rows shown on these pages can be controlled by applying filters to display selected data rows based on criteria programmed into the filter. Survey responses can also be exported from Qualtrics into multiple formats compatible with other analysis tools.

The research team can drill down to each question and display survey responses as visualizations. This will be particularly helpful for multiple choice questions as it will present the responses with additional analytics including a statistical distribution of the responses recorded displayed in a tabular format and the number of responses recorded for each multiple-choice option displayed in a bar chart. These types of data visualizations will resonate with both non and technical respondents when sharing findings with the respondent organizations.

Rural municipalities of Pennsylvania have non-profits operating with limited resources to address challenges with integrating cybersecurity best-practices while cyber threat actors continue to increase attacks. Our research has a deliverable goal of strategies, techniques, and procedures that non-profits can use to strengthen their cyber posture within their limited resource constraints. Since we are still in the data collection phase of our research from rural non-profits, our preliminary best practices focus on best practices for small businesses that we will further tailor for non-profits after completing our data analysis phase. We plan on disseminating such best practices to participating non-profit organizations as part of the overall research project.

V. EXAMPLES OF SURVEY COVERAGE

Our survey questions are organized into eight (8) categories.

1) Internal vs. External IT services and resources – This section will give us insight into whether IT services and resources are managed internally by individuals employed within the organization or subcontracted to a third-party. The resulting data collection will give us quantifiable data to assess the challenges rural non-profit organizations may have in dedicating the level of support needed to properly secure the organization's information technology assets against a cyber-attack.

2) Website security – This section includes questions that will help us determine whether the organization has a public-facing website, what types of interactions the public can perform on the website (e.g., make donations, register for events, sign up for communications, etc.), and the types of security measures implemented to protect the site against breaches. We expect to draw parallels between how well an organization's website is secured and whether the right level of support is involved in hardening the site and related host technology.

3) IT and Security budgeting – This section includes questions that will provide us with a baseline for whether rural non-profits allocate a portion of their operating expenses to information technology assets and how much of that part of the budget goes towards securing them. We hope to compare what rural non-profits spend on IT compared to for-profit entities and determine if there is a correlation between under-funded operations and the threat risk tied to those organizations.

4) Current risk environment – This section will help us determine each rural non-profit's confidence level in any cybersecurity measures in place and gain a deeper understanding of their approach for implementing them. The responses should yield clear trends showing which organizations are more prepared than others for handling disruptions to their business operations resulting from a cyber incident.

5) Business continuity/disaster recovery plan – This section will help us determine how well prepared each rural non-profit is to recover from a major disaster or a cyberattack that could adversely impact and/or destroy critical IT assets. We will ask whether the organization has a plan for sustaining operations outside of their primary work location if the site became temporarily unavailable.

6) Physical security – We will assess what measures have been taken to secure the physical facilities where the rural non-profit's employees work location. We will look for any gaps in any controls that expose vulnerabilities that need to be addressed.

7) Logical access control – We will collect input on how rural non-profits have implemented authentication and authorization within the organization. We will be looking for gaps in controls placed on application systems and data regularly accessed by employees, whether two-factor authentication is used, and determining whether a bring-your-own-device (BYOD) policy is in place that supports personal equipment being connected to the organization's network.

8) Inventory – We will ask our respondents about their IT asset management strategy and whether they keep an up-to-date record of IT resources in use throughout the organization. We are interested in knowing what assets are in use, whether audits of IT assets are being performed on a regular basis, and whether users that have been issued authorized equipment are following established acceptable use policies.

Our goal is to collect as much data from as many of the rural non-profits in the 67 Pennsylvania counties as possible. Since most of the municipalities where the non-profits operate are designated as rural, our target distribution has the potential of reaching thousands of organizations across the Commonwealth.

We will attempt to identify umbrella organizations that share common IT security policies and procedures with smaller affiliate organizations that operate in the same locality or elsewhere throughout the Commonwealth to optimize the number of surveys that are distributed. From there, we will use any public sources to identify an individual or contact email address associated with each organization (for example, the contact page on organization's website if available). We will target someone in a leadership capacity such as a Board of Director and/or an Executive Director. Additional follow-up may be required by phone if we are unable to find a contact email address for an organization. If our original target contact does not have the capability to provide us with the information requested, we will encourage assistance in redirecting the survey instrument to a qualified individual internally or a related entity. This data collection approach is rooted in research performed by Biernacki and Waldorf (1981) [15] where they documented the benefits and challenges tied to snowball or chain referral sampling techniques.

VI. CONTINUING WORK AND CONCLUSION

Rural municipalities of Pennsylvania have non-profits operating with limited resources to address challenges with integrating cybersecurity best-practices while cyber threat actors continue to increase attacks. Our continuing work will deliver specific strategies, techniques, and procedures that non-profits can use to strengthen their cyber posture within their limited resource constraints. Since we are still in the data collection phase of our research from rural non-profits, our preliminary best practices focus on best practices for small businesses including sound cyber hygiene practices, educating employees, and preparing for incident response that we will further tailor for non-profits after completing our data analysis phase. Participating non-profit organizations will be provided a “Best Practices” guide, based on NIST, CISA, FTC, and Small Business Administration (SBA) deemed most applicable, to assist them in implementing cybersecurity practices and standards as part of the overall research project.

In practicing good cyber hygiene, organizations should utilize strong password requirements and require multi-factor authentication (MFA) for users especially those with administrative access. Another best practice is for organizations to enable auto-update for software where possible. If auto-update is unavailable or infeasible, then prioritize updating applications that are accessible via the Internet. Also, organizations with limited resources to apply on dedicated security personnel should consider using a Managed Security Provider (MSP) for security services. However, these remote non-profits still need someone with cybersecurity skills to negotiate the service level agreement (SLA) with the MSP to ensure specific confidentiality, integrity, and availability requirements will be achieved by the MSP.

Employees in every organization must be trained to recognize and avoid phishing schemes by educating them to think before they click. Thus, even resource constrained non-profits must ensure resources are in place to identify and quickly assess any unexpected or unusual network behavior, whether via MSP or using internal network security monitoring.

Organizations must ensure availability of key personnel for response to an incident as documented in a cyber incident response plan. According to Cichonski, Millar, Grance, and Scarfone [16], successful incident response requires substantial planning and resources. Since we are discussing rural non-profits with limited resources, their plan must also specify means to provide surge support when needed for responding to an incident. Cichonski et al. [16] specify key elements of the plan include the organization’s mission, strategies, and goals for incident response which then inform an appropriate incident response program structure. The cyber incident response plan must ensure timely notification for employees who must understand their roles during an incident. One key step to ensure the ability to respond to an incident is backing up critical data then testing backup and recovery procedures.

ACKNOWLEDGEMENTS

This work is sponsored by a grant from the C3N program of Penn State University in conjunction with the Center for Cyber-Security, Information Privacy, and Trust in the College of Information Sciences and Technology, University Park.

REFERENCES

[1] Carter, T., Chandler, J., Cohen, R., Delaney, T., Higgins, A., O’Leary, A., and Thompson, D. (2019). “Nonprofit Impact Matters Report”, Available at https://www.nonprofitimpactmatters.org/site/assets/files/1/nonprofit-impact-matters-sept-2019-1.pdf

[2] Nonprofit HR. (2021). “2021 Nonprofit Talent Retention Practices Survey”, Available at https://www.nonprofithr.com/2021talentretentionsurvey/.

[3] Faulk, L., Kim, M., Derrick-Mills, T., Boris, E., Tomasko, L., Hakizimana, N., Chen, T., Kim, M. and Nath, L., (2021). “Nonprofit trends and impacts 2021”, Available at https://www.urban.org/research/publication/nonprofit-trends-and-impacts-2021

[4] Lincke S.J..(2015). “Security Planning: An Applied Approach”. Springer Publishing Company, Incorporated. Available at https://dl.acm.org/doi/book/10.5555/2807299

[5] Nonprofit HR, 2021 “2021 Nonprofit Talent Retention Practices Survey”, Available at https://www.nonprofithr.com/2021talentretentionsurvey/

[6] Nilson Report Newsletter Archive (2021). “Card and Mobile Payment Industry News”, Issue 1209, Available at https://nilsonreport.com/content_promo.php?id_promo=16

[7] McAfee, (2020) “Cloud adoption and risk report 2020”, Available at: https://www.mcafee.com/enterprise/en-us/forms/gated-form-thanks.html?docID=3804edf6-fe75-427e-a4fd-4eee7d189265.

[8] Bruce, A., (2020). “Cybersecurity for Nonprofits A Guide”, Available at: https://word.nten.org/wp-content/uploads/2020/02/Cybersecurity-for-Nonprofits_-February-2020.pdf.

[9] Center for Rural Pennsylvania, https://www.rural.pa.gov/, accessed on 9/10/2022.

[10] Snow, R., Leach, E., Tomko, M., (2013). “The Status of Rural Pennsylvania Nonprofit”, Available at: https://www.rural.pa.gov/getfile.cfm?file=Resources/PDFs/research-report/status_rural_of_nonprofits_2013.pdf&view=true.

[11] Tax Exempt World, https://www.taxexemptworld.com/, accessed on 9/10/2022.

[12] Council for Nonprofits, https://www.councilofnonprofits.org/what-is-a-nonprofit, accessed on 9/10/2022.

[13] Ryoo, J., Rizvi, S., Aiken, W., Long-Yarrison, B., (2020). “Information Systems Security Readiness Assessment for Municipalities in Pennsylvania”, Available at: https://www.rural.pa.gov/getfile.cfm?file=Resources/PDFs/research-report/Info-Systems-Security-2020.pdf&view=true.

[14] PA Dept of Department of Community and Economic Development, https://munstats.pa.gov/Public/FindMunicipality.aspx, accessed on 9/13/2022

[15] Biernacki, P., & Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2), 141-163.

[16] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *NIST Special Publication 800-61 Computer Security Incident Handling Guide*, rev. 2. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.SP.800-61r2.