Conducting Privacy-Sensitive Surveys: A Case Study of Civil Society Organizations

Nikita Samarin
UC Berkeley / Center for
Long-Term Cybersecurity
nsamarin@berkeley.edu

Coye Cheshire
UC Berkeley
coye@berkeley.edu

Alisa Frik
International Computer Science
Institute / UC Berkeley
afrik@icsi.berkeley.edu

Serge Egelman
International Computer Science
Institute / UC Berkeley
egelman@icsi.berkeley.edu

Sean Brooks
UC Berkeley / Center for
Long-Term Cybersecurity
swb@berkeley.edu

Abstract

Compared to other organizations, civil society organizations (CSOs) often operate in elevated-risk contexts, and attacks against them carry much greater ramifications, including threats to freedom of expression, liberty, and life. We aim to capture the factors that affect the attitudes and intentions of CSO employees to engage in security and privacy behaviors by using a survey-based study to collect data about employees working at US-based civil society groups. In this paper, we describe the steps that we take to minimize risks to the respondents, such as employing a privacy-centric survey design, anonymity-preserving incentive strategies, and recruitment that does not reveal any identities. We hope that our experiences will inform and assist researchers and practitioners working on protective technologies for vulnerable populations.

Author Keywords

High-risk users; civil society; security and privacy; vulnerable populations

CCS Concepts

•Security and privacy → Social aspects of security and privacy; Privacy protections; Usability in security and privacy;

CHI'20,, April 25–30, 2020, Honolulu, HI, USA

Introduction

Researchers and practitioners have traditionally focused on the security needs and practices of the average users, sidestepping underrepresented and vulnerable communities. In recent years, there has been an increase in research examining the security and privacy behaviors of such groups, revealing nuanced and community-specific concerns and practices that differ from those of the average users [8, 26, 30, 24, 7, 15]. One such vulnerable online population consists of employees working for civil society organizations (CSOs), which include a wide range of groups, such as humanitarian organizations, labor unions, advocacy groups, indigenous peoples movements, faith-based organizations, community groups, professional associations, foundations, think tanks, charitable organizations, and other non-governmental and not-for-profit organizations [4]. Compared to other sectors, civil society operates in elevated-risk contexts [23, 21, 10, 12], where attacks often carry much greater ramifications, including threats to freedom of expression, liberty, and life.

Civil society groups often lack the funds and human resources to defend themselves. For instance, they maintain a poor ratio of IT staff to non-technical staff [17], do not conduct vulnerability assessments [2] and do not adopt solutions aimed at improving their cybersecurity [29]. Findings from the 2018 report by the Public Interest Registry indicate that CSOs rarely have access to purpose-built systems and instead, tend to use commodity tools that are not tailored to their needs and elevated risk profiles [14]. For instance, 58% of surveyed CSOs use Facebook messenger, which is not encrypted by default, to communicate sensitive information [14]. Although recent attempts have been made to design security solutions that offer sufficient protection for CSOs [3, 20], they often fail to capture the needs, practices and mental models of their intended users [25, 22].

One could try to dismiss cyberattacks against civil society and elevated-risk users as “edge cases” that deserve less attention than more sophisticated technical attacks, or threats that affect broader user populations. However, there are several reasons why understanding the context in which CSOs operate is essential. First, employees working for CSOs constitute a sizeable proportion of the population. In the US alone, they account for 11.4 million jobs or 10.3% of the non-public sector employment [1]. Second, as most civil society groups employ standard tools used by millions of users [14], while their online risks are amplified compared to the general population, this particularly vulnerable population could be considered “extreme users” [13]. Therefore, understanding the way in which CSO employees use mainstream tools could reveal more insight on usability and security issues that might be overlooked in the studies with typical user communities. Such insights will help to improve the design of technology for the average use-case as well. For instance, enabling key security choices by default in popular platforms would improve the security outcomes both for the high-risk and the average users. Finally, cyberattacks that target CSOs today are precursors of threats that could affect broader user groups tomorrow [28]. Understanding how to protect against such threats for the high-risk users would, therefore, also confer security for the average users.

Security and Privacy Behavior

The main goal of our study is to better understand cybersecurity culture and practices in CSOs to improve their resilience to cybersecurity attacks. Drawing on previous work that collected qualitative data from journalists [26], activists [22], and humanitarian workers [19] and several theories of human behavior [27, 5, 16], we establish key factors that affect the attitudes and intentions of CSO employees to engage in protective behavior. These theories have been used to explain a wide range of behaviors, including behaviors relevant to information security, such as compliance with information security policy [18, 31, 9], backing up personal data [11], and security behaviors aimed at protecting home computers [6]. We adapt the scales used to measure constructs from Protection Motivation Theory and Theory of Planned Behavior from the literature on organizational security policy compliance [18, 9]. Our proposed research model is shown in Figure 1.

Furthermore, we want to understand which security and privacy threats pose the highest perceived risk among the employees of civil society groups. Based on our personal experience of working with CSOs and prior work [26, 22, 19], we identify the following seven threats: phishing, malware, online harassment, online reputation attack, physical device compromise, surveillance, and attacks on online services. We assess the respondents' risk perception of each of these risks, and their self-reported risk mitigation strategies for one of these risks chosen at random. We also present our list of risk mitigation strategies to understand whether the respondent is familiar with each of the strategies and if so, whether they actively make use of them.

Methodology

In this section, we discuss our methodology in more detail, bringing attention to aspects of our research design that allow us to collect data from CSO employees without compromising their safety and privacy. We hope that this discussion will benefit other researchers who use survey-based methods to collect information about vulnerable populations.

Survey Design

We conduct an online survey to collect information about the attitudes, intentions, and existing practices of CSO employees. Apart from the usual questionnaire design considerations (e.g. designing scales to measure the constructs, minimizing survey response time, improving the usability of the online interface, etc.), we need to ensure that individual and organizational privacy is completely preserved. This is essential, as connecting certain demographic information and specific behaviors to individual employees could not only compromise their personal safety but also pose risks to other employees and the entire organization. Furthermore, managers or colleagues at the same organization could also use the revealed questionnaire responses against the employee in question. While guaranteeing complete confidentiality of data transmitted over the internet is impossible, we minimize the possible risks to participants by taking the following steps:

Collecting data anonymously. We do not collect any personally-identifiable information from the respondents, including any device or network identifiers (e.g. IP address). We minimize the number of demographic and organization-specific questions, make them optional, and ensure that any individual response containing such information is visible only to the researchers. Moreover, we analyze and present these responses only in aggregate form to prevent any correlational inferences. This is especially important to us, as we do not want to compromise the anonymity of our survey participants through combinations of their responses to different questions. We inform the respondents about our data collection practices and data retention policies in the consent form, highlighting the most relevant parts on a separate page. Although anonymous surveys have some disadvantages over confidential ones, it is crucial for us to ensure that CSO employees do not face any additional risks as a result of participating in our study.

Using anonymity-preserving incentive strategies. As the completion time of our survey is around 15-20 minutes, we want to provide incentives to increase response rates and the quality of responses. As we are not assigning any identifiers to the survey participants, we cannot follow-up with them to provide any direct compensation. Instead, at the end of the survey respondents can select one of three charities, to which we will proportionally donate our compensation budget at the end of the study. We believe that such an incentive strategy increases the quality of the collected data without compromising the anonymity of the respondents.

Target Population

One of the major difficulties in researching vulnerable communities is the problem of locating and recruiting participants, as the researchers often need existing connections and time to establish trust. We conduct survey-based research focusing on CSOs based in the US but not targeting any specific sector or cause in order to observe inter-group differences and understand which segments of the civil society might perceive themselves to be particularly vulnerable to security and privacy risks.

Recruitment. As part of the Center for Long-Term Cybersecurity at UC Berkeley, we provide cybersecurity support to a number of civil society groups, which allows us to gain first-hand experience of the problems and issues that occur within these organizations. Although useful for initial survey design, the number of employees at these organizations would be insufficient to collect quantitative data. For this reason, we partner with TechSoup, a nonprofit that provides technical support and tools to other nonprofits and that operates an international network of nonprofits. This network includes around 300,000 nonprofits based in the US, and TechSoup sends periodic announcements and updates to members of their network via email newsletters. We used one of these periodic email newsletters to distribute our survey through an anonymous link embedded in a banner shown in Figure 2 (the number of newsletter subscribers also guarantees anonymity for each respondent). We avoid explicitly mentioning cybersecurity in the recruitment text and consent form and, instead, we debrief the respondents about the purpose of our study after the survey is completed. This is done to avoid priming participants about security and privacy, potentially leading them to perceive their risk to cybersecurity threats higher than it actually is. Using an email newsletter for survey distribution also enables us to disseminate key findings among the participants without recording their identities. We believe that this will inform and benefit the respondents, and provide an additional method of compensation for their time and effort.

Limitations

So far we have already performed a pilot study, in which we collected 100 responses as part of our scale development process. For the pilot study, however, we recruited participants through Prolific Academic crowdsourcing platform and provided monetary compensation for their participation. After conducting the pilot survey, we also included questions regarding mitigation strategies, as we believe that it is essential to understand existing practices alongside attitudes and intentions. As of now, we collected responses of around 200 employees of civil society groups, but the uptake is slow. We believe reasons might include the difference in populations between the pilot and main study and the lack of direct monetary incentives. We are planning to make adjustments to our survey to decrease response time and search for more ways to reach our target population.

Conclusion

We employ survey-based methods to understand cybersecurity culture and practices at CSOs, their perceived risks of different threats and their self-reported mitigation strategies. We design the survey to balance achieving our research goals with preserving the anonymity of participants. This includes not collecting any information from respondents, employing incentive strategies that do not require any identifiers, recruiting participants and disseminating key findings anonymously using email newsletter lists with a large number of subscribers. We believe that these approaches will preserve the quality of collected data without compromising the safety and anonymity of respondents.

Acknowledgements

We acknowledge the support of the Citizen Clinic at the Center for Longer-Term Cybersecurity who provided expert input and review of our survey instruments. We also thank TechSoup for providing us access to their network of nonprofits and their support during this research project. This research is sponsored by funding from the Center for Long-Term Cybersecurity at UC Berkeley.

REFERENCES

[1] 2014. Nonprofits account for 11.4 million jobs, 10.3 percent of all private sector employment. (2014). Retrieved Febuary 11, 2020 from `https://www.bls.gov/opub/ted/2014/ted_20141021.htm`.

[2] 2017. Not-for-Profit Governance and Financial Management Survey. (2017).

[3] 2019. Advanced Protection Program. (2019). Retrieved Febuary 11, 2020 from `https://landing.google.com/advancedprotection`.

[4] 2020. Civil Society Policy Forum. (2020). Retrieved Febuary 11, 2020 from `https://www.worldbank.org/en/events/2020/04/17/civil-society-policy-forum`.

[5] Icek Ajzen and others. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.

[6] Catherine L Anderson and Ritu Agarwal. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly* 34, 3 (2010), 613–643.

[7] Lindsay Blackwell, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. 2016. LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 610–622.

[8] Danah Boyd. 2014. *It's complicated: The social lives of networked teens*. Yale University Press.

[9] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.

[10] Masashi Crete-Nishihata, Jakub Dalek, and Ronald Deibert. 2014. *Communities@ Risk: Targeted Digital Threats Against Civil Society*. Citizen Lab, Munk Centre for International Studies, University of Toronto.

[11] Robert E Crossler. 2010. Protection motivation theory: Understanding determinants to backing up personal data. In *2010 43rd Hawaii International Conference on System Sciences*. IEEE, 1–10.

[12] Ronald J Deibert, Rafal Rohozinski, A Manchanda, Nart Villeneuve, and GMF Walton. 2009. Tracking GhostNet: Investigating a cyber espionage network. (2009).

[13] John Partomo Djajadiningrat, William W Gaver, and JW Fres. 2000. Interaction relabelling and extreme characters: methods for exploring aesthetic interactions. In *Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques*. 66–71.

[14] Nonprofit Tech for Good. 2018. 2018 Global NGO Technology Report. (2018).

[15] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–15.

[16] James Hedlund. 2000. Risky business: safety regulations, risk compensation, and individual behavior. *Injury prevention* 6, 2 (2000), 82–89.

[17] Robert Hulshof-Schmidt. 2017. Nonprofit Technology Staffing and Investments Report. (2017).

[18] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95.

[19] Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic, Bryan Ford, and Jean-Pierre Hubaux. 2018. On enforcing the digital immunity of a large humanitarian organization. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 424–440.

[20] Ada Lerner, Eric Zeng, and Franziska Roesner. 2017. Confidante: Usable encrypted email: A case study with lawyers and journalists. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 385–400.

[21] Bill Marczak, John Scott-Railton, and Sarah McKune. 2015. Hacking team reloaded? US-based Ethiopian journalists again targeted with spyware. *Citizen Lab* 9 (2015).

[22] William R Marczak and Vern Paxson. 2017. Social Engineering Attacks on Government Opponents: Target Perspectives. *Proceedings on Privacy Enhancing Technologies* 2017, 2 (2017), 172–185.

[23] William R Marczak, John Scott-Railton, Morgan Marquis-Boire, and Vern Paxson. 2014. When governments hack opponents: A look at actors and technology. In *23rd USENIX Security Symposium (USENIX Security 14)*. 511–525.

[24] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2189–2201.

[25] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. 2015. Investigating the computer security practices and needs of journalists. In *24th USENIX Security Symposium (USENIX Security 15)*. 399–414.

[26] Susan E McGregor, Franziska Roesner, and Kelly Caine. 2016. Individual versus organizational computer security and privacy concerns in journalism. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 418–435.

[27] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.

[28] John Scott-Railton. 2016. Security for the high-risk user: separate and unequal. *IEEE Security & Privacy* 14, 2 (2016), 79–87.

[29] Jorge Luis Sierra. 2013. *Digital and mobile security for Mexican journalists and bloggers*. Freedom House.

[30] Svetlana Yarosh. 2013. Shifting dynamics or breaking sacred traditions? The role of technology in twelve-step fellowships. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3413–3422.

[31] Jie Zhang, Brian J Reithel, and Han Li. 2009. Impact of perceived technical protection on security behaviors. *Information Management & Computer Security* (2009).

Appendix A: Research Model

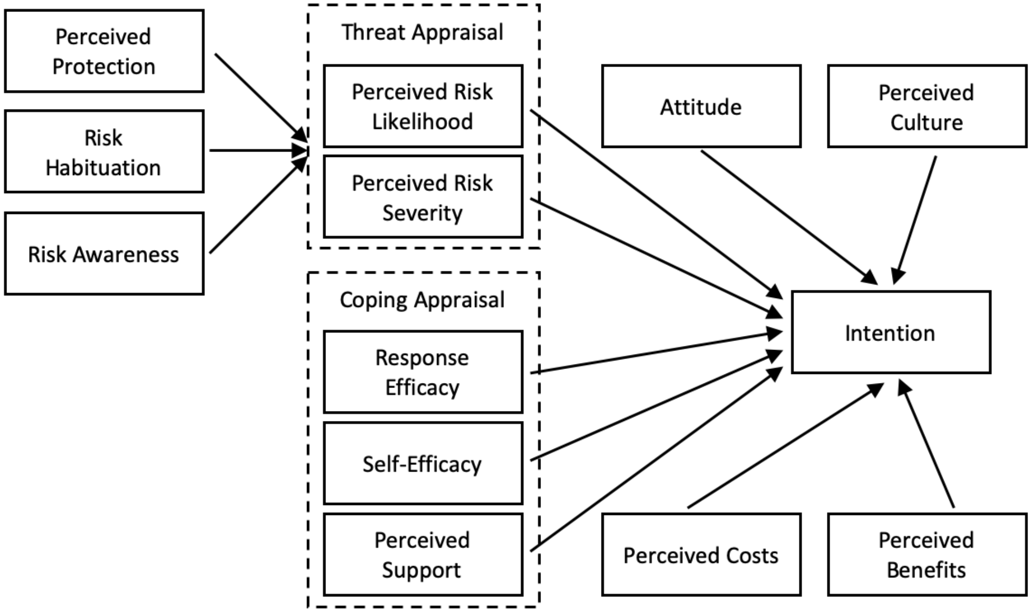

Figure 1: Research model showing variables affecting intention to engage in security and privacy behavior.

Appendix B: Recruitment Banner

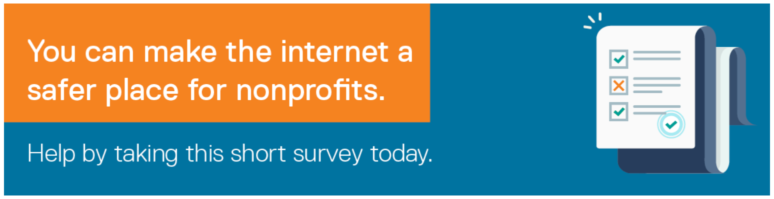
You can make the internet a safer place for nonprofits.
Help by taking this short survey today.

Figure 2: Recruitment banner used as an invitation to participate in the survey.