CLTC
Center for Long-Term Cybersecurity
UC Berkeley

OFFICE OF CYBERSECURITY
SAN FRANCISCO
DEPARTMENT OF TECHNOLOGY

SAN FRANCISCO
DIGITAL EQUITY

CyberCAN: Cybersecurity for Cities and Nonprofits

Strategic Recommendations for the City and County of San Francisco to Improve Nonprofit Cybersecurity

Sarah Powazek
Shannon Pierson

November 2024

Table of Contents

Executive Summary

City governments are committed to serving their residents and meeting the needs of their communities, but they can't do it alone. Cities often depend on local nonprofits to carry out their public service missions and bridge resource gaps in social services. As nonprofits face growing cybersecurity challenges, cities with Digital Equity and Cybersecurity departments are uniquely equipped with the resources, knowledge, and connections required to help nonprofits strengthen their cyber defenses–helping ensure that they can continue their vital work securely and without disruption.

Cybersecurity for Cities and Nonprofits (CyberCAN) is an innovative research partnership between the UC Berkeley Center for Long-Term Cybersecurity (CLTC) and the City and County of San Francisco. This project was designed to help illuminate municipal governments' understanding of nonprofit cybersecurity and identify opportunities to improve the cyber resilience of nonprofit organizations in their local communities

CLTC surveyed 68 San Francisco-based nonprofits to understand their cybersecurity challenges, preferences for support, available resources, and baseline cyber hygiene practices. This survey gathered essential data to understand and address cybersecurity needs within nonprofits.

Key findings include:

1. **Nonprofits are frequent targets of cybercrime,** with 85% of nonprofits surveyed reporting that they have experienced at least one cyber attack. **Nonprofits remain attractive for cyber criminals because they collect and store sensitive information;** 75% of surveyed nonprofits reported that they collect social security numbers.

2. **Nonprofits lack the staff they need to protect themselves against cyber attacks:** 53% of surveyed nonprofits have no full-time IT staff, and those that do have an average of just one full-time IT staff member for every 96 employees.

3. **Nonprofits have moderate adoption rates of basic cybersecurity controls.** While 61% of surveyed nonprofits employ multi-factor authentication (MFA) for email and collaboration tools, 16% do not use MFA at all, and 53% do not offer any type of cybersecurity awareness training for employees.

4. **Nonprofits struggle most with funding and prioritizing cybersecurity:** 46% of surveyed nonprofits ranked funding as their greatest obstacle to improving their organization's cybersecurity, followed closely by a lack of knowledge on what to improve and difficulty prioritizing cybersecurity over competing objectives.

5. **Nonprofits want hands-on, human assistance to improve their cybersecurity.** Nonprofits ranked a city help line and proactive cybersecurity consulting as the highest priority needs for improving their cybersecurity. These items ranked above other cybersecurity resources, such as tools and software, educational websites, and awareness training, emphasizing the necessity of human interaction in cybersecurity resilience.

As trusted leaders and conveners within their local communities, city governments are uniquely positioned to support local nonprofits with cybersecurity. Cities are trusted local leaders, nurture relationships with nonprofits to improve resident services, and provide nonprofit funding. Supporting nonprofits' cybersecurity aligns closely with cities' digital equity objectives, and their specialized knowledge in public-interest cybersecurity positions them to serve as hubs of cybersecurity education and support.

Municipal governments are ideal partners for improving nonprofit cybersecurity. While this report focuses on San Francisco, we expect that many of these findings will hold true for nonprofits around the country. We recommend that city governments consider implementing the following recommendations:

Recommendations:

1. **Provide regular cybersecurity advice** and assistance to local nonprofits.
2. **Host an annual cybersecurity convening** for nonprofits to learn and network with cyber professionals.
3. **Create a nonprofit cybersecurity resource webpage** for the city government website.
4. **Offer cybersecurity funding opportunities for nonprofits** to hire, or contract, cybersecurity talent.
5. **Host student interns to work with nonprofits** on cybersecurity issues.
6. **Provide local nonprofits with low-cost access** to critical cybersecurity tools and software.

Our team looks forward to working with additional municipalities to understand and serve the unique cybersecurity needs of their local nonprofits. By helping nonprofits, cities help protect residents' critical services and sensitive health and financial information from the constant threat of digital harm.

CyberCAN: Cybersecurity for Cities and Nonprofits

The Challenges of Nonprofit Cybersecurity

Nonprofits like food banks, homelessness services, and community development organizations provide critical and time-sensitive services to local residents, and are fixtures of community support for people of all ages. But nonprofits are also the second-most-targeted sector by cyber attacks and are among the least prepared to defend themselves. The Cybersecurity and Infrastructure Security Agency (CISA), the U.S.'s premier cyber defense agency, describes civil society organizations as "high threat level and low defense capability" organizations that are "ill-prepared for and vulnerable to common cyber threats."[1]

Cyber attacks on nonprofits cause immediate and serious damage. In 2020, a hunger relief organization in Philadelphia lost nearly $1 million due to a cyber attack — funding that was intended to go towards building a new community kitchen facility.[2] In 2022, cyber criminals stole records of over 500,000 people from the International Committee of the Red Cross, a tranche of data that included highly sensitive information about refugees, people separated from their families, and missing persons.[3]

While nonprofit cybersecurity is a critical issue and a frequent topic of conversation in cybersecurity circles, most solutions place the majority of the burden upon nonprofits themselves. Developers of cybersecurity standards, toolkits, checklists, and other standalone resources assume that nonprofits have the time and connections to find these materials, the expertise to understand them, and the capacity to make necessary changes.

There is also a notable lack of data available to quantify and describe the cybersecurity challenges nonprofits face. Existing studies largely focus on sentiment analysis, such as studying nonprofits' satisfaction, optimism, budget, and trust in technology, through qualitative surveys and interviews.[4] While such reports can provide helpful context, qualitative information about sentiment alone is not enough to make informed policy and technology interventions to assist nonprofits in improving their cybersecurity.

Several academic studies have assessed the cybersecurity practices of nonprofits in the US and Europe, based on such factors as their use of cybersecurity awareness training and their security-related policies and procedures.[5, 6, 7] However, few studies have focused on a regional set of nonprofits to understand their unique obstacles and relationships with their local government.

CLTC sought to fill this knowledge gap through a focused engagement with San Francisco-based nonprofits. Our survey assessed nonprofits cybersecurity controls and identified the obstacles they face, with the goal of identifying steps that the City and County of San Francisco can take to better support local nonprofits — and to identify steps that may be used by other municipal governments across the country.

[1] Cybersecurity and Infrastructure Security Agency (CISA). (2024, May 14). *Mitigating cyber threats with limited resources: Guidance for civil society*. U.S. Department of Homeland Security (DHS).

[2] Ralph, P. (2020, December 1). *Philabundance falls victim to cyberattack, loses almost $1 million*. PhillyVoice.

[3] (2022, January 19). *Sophisticated cyber attack targets Red Cross Red Crescent data on 500,000 people*. International Committee of the Red Cross.

[4] (2022, December). *Global Nonprofit Trends Report, 5th Edition*. Salesforce.

[5] Hulshof-Schmidt, R. (2018, November). *State of Nonprofit Cybersecurity*. NTEN.

[6] Lazar, A. (2024, March 25). *Cyber-poor, target-rich: The crucial role of cybersecurity in nonprofit organizations*. Cyber Peace Institute.

[7] Lindström, C. (2022). *Cybersecurity experiences and practices in charities A qualitative and quantitative survey of Swedish charities*. DiVA.

CyberCAN: A Roadmap for Municipal Support for Nonprofit Cybersecurity

The Cybersecurity for Cities and Nonprofits (CyberCAN) project was designed to help improve municipal governments' understanding of nonprofit cybersecurity challenges and identify opportunities to improve nonprofits' cyber resiliency.

CLTC was fortunate to have a founding partner in the City and County of San Francisco's Department of Technology (DT). DT and CLTC met in 2023 to discuss nonprofit cybersecurity, and aligned on the CyberCAN project, a research initiative to engage, understand, and educate San Francisco-based nonprofits on cybersecurity and propose measures that city government stakeholders can take to support nonprofits' cybersecurity efforts.

Cities, towns, and municipalities are well positioned to serve as hubs of cyber defense and support for local nonprofits. Nonprofits are best served by working with organizations that they already know and trust, and they often have trusted relationships with city agencies through grant programs and other engagement. Cities also have an integrated understanding of the local populations being served, and can tailor support to be most effective for nonprofits in different neighborhoods. Perhaps most importantly, city governments are permanent institutions and so can provide sustainable and long-lasting support to local organizations.

The CyberCAN project is not just a survey; it is a model for engaging directly with nonprofits and city leaders as integral stakeholders, and laying the groundwork for long-term and sustainable cybersecurity communication. CyberCAN takes a beneficiary-centered approach by working directly with nonprofits to develop realistic and accessible solutions that are effective and tailored to their specific needs.

We hope the value of direct engagement with city decision-makers and nonprofit beneficiaries will be a replicable model for future collaborations between cities, nonprofits, and academic institutions.

Methodology

CLTC set out to generate insights and recommendations to help inform local policymakers on how to allocate cybersecurity and IT resources more effectively to nonprofits. CLTC surveyed San Francisco-based nonprofits to understand their cybersecurity challenges, preferences for support, available resources, and baseline cyber hygiene practices. This survey was designed to gather data essential for understanding and addressing cybersecurity needs within nonprofits. We employed a mixed methods approach by conducting quantitative and qualitative analysis of survey responses.

Survey Scoping and Design

To design our survey, CLTC collaborated with the City and County of San Francisco's Office of Cybersecurity and Digital Equity Office, and we engaged local nonprofits for their input and feedback. The survey development process comprised five stages:

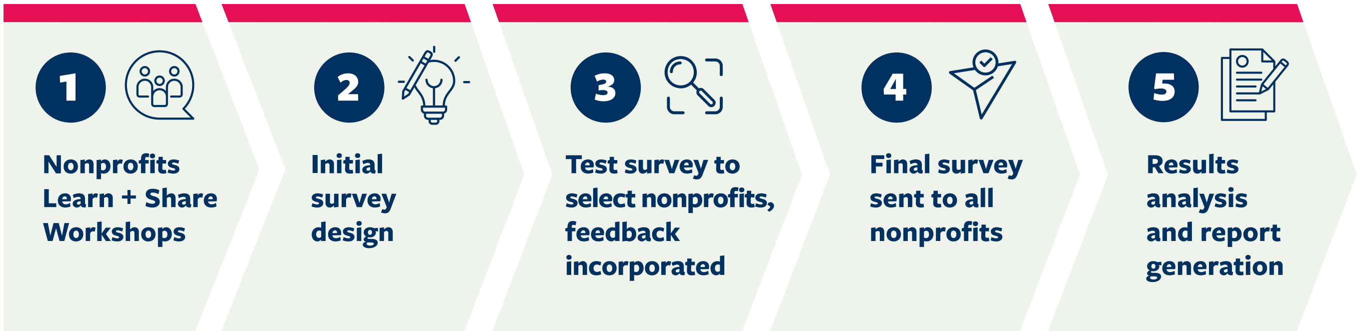
(1) Gathering input from nonprofit workshops on survey design,
(2) collaborating with City of San Francisco cybersecurity staff to create the initial survey design,
(3) conducting a trial survey with nonprofits to gather constructive feedback,
(4) sending out the final survey, and
(5) analyzing the data and publishing results.

CLTC kicked off the CyberCAN partnership in October 2023 by hosting two in-person Cybersecurity Learn + Share Workshops at the San Francisco Department of Technology headquarters. These workshops focused on nonprofit cybersecurity, and our team received input from 16 nonprofits about how their staff and leaders thought about cybersecurity, what they struggled with, and what they thought would help.

Nonprofits also provided feedback on how to make the planned survey more user-friendly and facilitate greater participation. The workshop inspired us to prioritize accessibility by incorporating pop-out definitions of cybersecurity terms, and to use predefined answers for survey questions. The workshop also led to the inclusion of an optional survey section that would provide nonprofits with customized cybersecurity guidance based on their responses.

In developing survey questions, CLTC relied on time-tested cybersecurity standard frameworks that outline the most essential and effective cybersecurity safeguards organizations can implement. These frameworks included the NIST Cybersecurity Framework (NIST CSF) 2.0, ISO 27001 and ISO 27002, and the CIS Critical Security Controls, as well as CISA's Bad Practices and Cross-Sector Cybersecurity Performance Goals (CPGs).

CLTC also consulted with the City and County of San Francisco's Office of Cybersecurity and Digital Equity



1 Nonprofits Learn + Share Workshops

2 Initial survey design

3 Test survey to select nonprofits, feedback incorporated

4 Final survey sent to all nonprofits

5 Results analysis and report generation

Office division throughout the survey development process, meeting bi-weekly with city partners to ensure that the survey captured actionable information about nonprofit cybersecurity obstacles and resource preferences. This collaboration scoped topics covered in the survey and ensured that findings could inform policy recommendations and help city operators substantively address the cyber preparedness of local nonprofits.

Survey Overview

The survey is divided into two sections. Section 1 provides an overview of the cybersecurity resources nonprofits currently have, what they need, and what they find challenging to access. The survey gathered information on respondents' organizations, IT resources, cyber incidents, preferences for resources, and obstacles to improving their cybersecurity. Most of the 15 questions in Section 1 were mandatory for all respondents, with the exception of the question asking about sensitive and potentially unknown security and budgetary information (i.e., "What's your total annual budget?" and "What, if any, cyber incidents has your organization experienced before?").

Section 2 was optional and aimed to establish a baseline understanding of nonprofits' cyber hygiene practices. These five questions assessed the implementation of fundamental and high-impact cybersecurity controls prioritized by the cybersecurity standard frameworks. This section included questions on the implementation of multi-factor authentication (MFA), availability of cybersecurity awareness training, frequency of software updates (patching), types of sensitive data collected, and nonprofits' confidence in their ability to safeguard data. Because this section contained detailed cybersecurity questions, and extended the length of the survey, it was made optional in order to encourage as many respondents as possible to fill out the survey, regardless of their cybersecurity knowledge.

As an incentive to participate, respondents who completed the optional portion of the survey received customized cybersecurity feedback and guidance based upon their answers. The feedback component conveyed the benefits of basic cybersecurity interventions like MFA and automatic software updates. It also provided links to resources relevant to nonprofits, sourced from reputable cybersecurity organizations like CISA, NIST, Google, Microsoft, CrowdStrike, and Norton, among others. The materials featured accessible educational explainers and step-by-step guides to help the organizations implement the recommended cybersecurity measures.

After finalizing the survey, CLTC conducted a three-week pilot survey with 16 nonprofits to gather additional feedback, which was incorporated into the survey. The final survey comprised 20 questions with a variety of formats, including multiple choice, multi-select, ranking, and free-response questions.

Survey Distribution

CLTC distributed the survey to over 220 San Francisco-based nonprofits using the Qualtrics survey software using publicly available information. Additionally, grant officers from the City of San Francisco shared the survey with some of their grantees. The survey was open between March and April of 2024.

After closing the survey, CLTC undertook data cleaning procedures to ensure accuracy and quality in the results by omitting incomplete surveys from the final results and reconciling duplicate submissions to ensure only one submission per organization. To preserve privacy and encourage candid participation from nonprofits, CLTC anonymized the dataset and chose to keep individual survey results confidential, only sharing aggregated results publicly and with the City of San Francisco.

Results and Analysis

Respondent Snapshot

CLTC received 68 complete responses to the required portion of the survey. Of these respondents, 66% also completed the optional survey addendum on cybersecurity controls. We surveyed nonprofits of various sizes, with staffs ranging from two to 700 full-time employees.

Many types of organizations providing services were represented. The most commonly provided services provided by our nonprofits included workforce development and employment services, arts and culture, housing support, healthcare & mental health services, and food assistance.

Types of Nonprofits Surveyed

- Arts and Culture
- Housing Support Services
- Healthcare & Mental Health Services
- Food Assistance
- Policy Advocacy and Organzing
- Internet/Computer Access and Training Services
- Financial Aid and Financial Education Services
- College Access and Affordability
- Workforce Development and Employment Service

Major Findings

CLTC's quantitative and qualitative analysis of the survey data revealed several major patterns about nonprofit cybersecurity.

Five key findings emerged:

Finding #1: Nonprofits are frequent targets of cybercrime and remain attractive targets by collecting sensitive information.

Finding #2: Nonprofits lack the staff they need to protect themselves against cyber attacks.

Finding #3: Nonprofits have moderate adoption rates of basic cybersecurity controls, highlighting key areas for improvement.

Finding #4: Nonprofits struggle most with funding and prioritizing cybersecurity.

Finding #5: Nonprofits want hands-on, human assistance to improve their cybersecurity.

Finding #1:

Nonprofits are frequent targets of cybercrime, and remain attractive targets by collecting sensitive information.

Nonprofits and Cybercrime

The nonprofit sector is one of the most frequently targeted in the world. In 2021, Microsoft found that non-governmental organizations (NGOs) and think tanks were the second-most-targeted sector by cybercriminals.[8]

Our results reinforced this status quo; the majority of San Francisco-based nonprofit organizations surveyed have suffered a cyberattack, with 85% reporting at least one type of cyber incident.

Our analysis showed that nonprofits experience a variety of cyber threats. Phishing was the most frequently reported form of cyber intrusion, affecting 71% of respondents. This result is consistent with broader cybersecurity trends that track phishing as the most commonly reported form of cybercrime in general.[9]

Business email compromise (32%) and credit card or bank account fraud (29%) were the next most common forms of attack, indicating that nonprofits are experiencing cyber threats that target their limited financial resources and affect business operations.

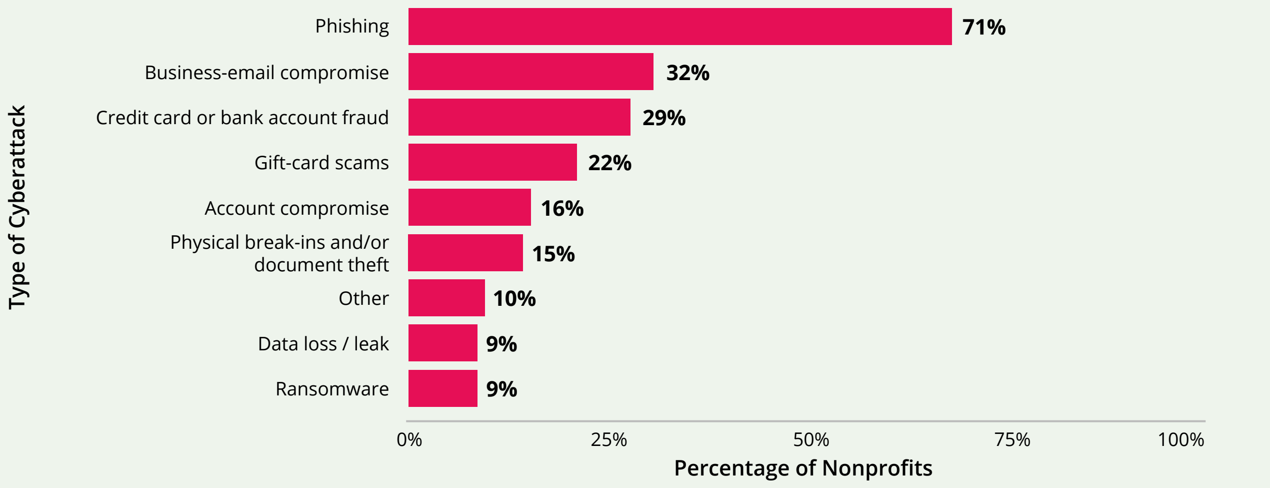
85%

of nonprofits suffered at least one type of cyber attack

These types of attacks can be financially devastating for nonprofits, which often operate on limited budgets and may not be able to afford cyber incident response and recovery costs. Such attacks and their associated costs can divert scarce funding away from core missions and services, disrupting operations and limiting organizations' ability to deliver critical services.

Figure 1: Cyberattacks Experienced be Nonprofits

[68 Responses in Total]



[8] Spelaug, J. (2021, October 21). *Strengthening cyber defenses for nonprofits*. Microsoft.

[9] FBI San Francisco. (2024, April 4). *FBI Releases Internet Crime Report*. FBI.gov.

Nonprofits collect sensitive, valuable information

Organizations collecting personally identifiable information (PII) typically require robust cybersecurity resources to protect this data. Highly sensitive and unchangeable information such as social security numbers and health information is financially valuable to cyber criminals, many of whom are looking for a quick payday. Social security numbers can be used to carry out identity fraud, open bank accounts, sign up for credit cards, and commit tax fraud using a stolen identity. Healthcare information is sensitive and private and can be stolen and used to extort the victim organization, or even individuals, for payment.

As long as they collect and store sensitive information, nonprofits will remain lucrative targets for cyber criminals. Understanding the types of data nonprofits collect can boost understanding of the risks they face — and the urgency of assisting them with cybersecurity protection.

Our results showed that many San Francisco nonprofits collect highly sensitive data from beneficiaries and donors: 75% reported that they collect social security numbers, 61% collect financial information, and 32% collect health information.

75%

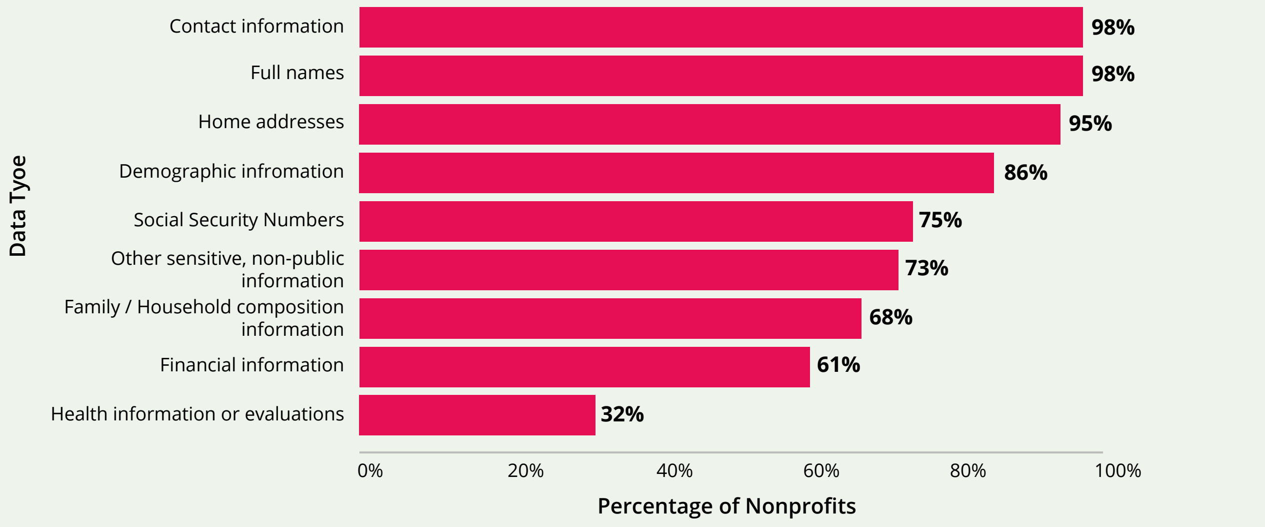
of nonprofits collect social security numbers

This widespread collection of sensitive information is especially concerning when considering the types of populations these nonprofits serve. Some of the most marginalized communities in San Francisco rely on nonprofits for essential services like food assistance, housing support, and healthcare. These residents may not have resources to resolve identity theft or financial fraud resulting from data leaks; such incidents could have significant downstream impacts on their ability to secure credit, housing, and employment.

Moreover, public exposure or sale of sensitive information could undermine public trust in institutions like nonprofits, pushing resource-strapped residents away from the services they rely on. These survey findings suggest that investing in cybersecurity protections for nonprofits is essential for protecting their mission and critical services.

Figure 2: Data Collected by Nonprofits

[44 Responses in Total]



Finding #2:

Nonprofits lack the staff they need to protect themselves against cyber attacks.

53%
Of nonprofits have no full-time IT staff

21%
Of nonprofits have only 1 full-time IT staffer

1:96
Ratio of IT staff to full and part-time staff

At most organizations, the responsibility for implementing cybersecurity primarily rests with the staff, even those that outsource technology by using cloud products and services. The roles of IT staff can include securely configuring new tools, implementing strong identity and access management, continuously monitoring for suspicious activity, and responding to security incidents.

The quality, training, and number of IT staff can be a useful indicator of the level of cybersecurity investments and protections in an organization.

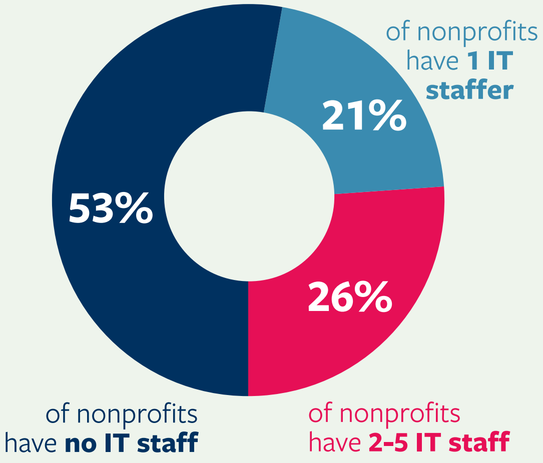
IT and Cybersecurity Staff

In large organizations, IT and cybersecurity responsibilities are often split between several full-time roles, including discrete IT staff, cybersecurity staff, and C-suite leaders, such as a chief information officer (CIO) and chief information security officer (CISO).

Our survey results revealed that most nonprofits are severely understaffed for IT and cybersecurity positions. The majority of nonprofits surveyed **(53%) have no dedicated IT staff at all**. This may reflect that someone within these organizations is carrying out IT tasks as a part-time responsibility, while also being responsible for their main job in fundraising, leadership, or service delivery.

This understaffing represents a severe risk for nonprofits; cybersecurity knowledge remains largely inaccessible for everyday staff, and it is a difficult task to shoulder the burden of an entire organization's IT and cybersecurity needs as a part-time job, potentially without any formal training.

Figure 3: Nonprofit Dedicated IT Staff
[68 Responses]



Distribution of IT and Cybersecurity Staff

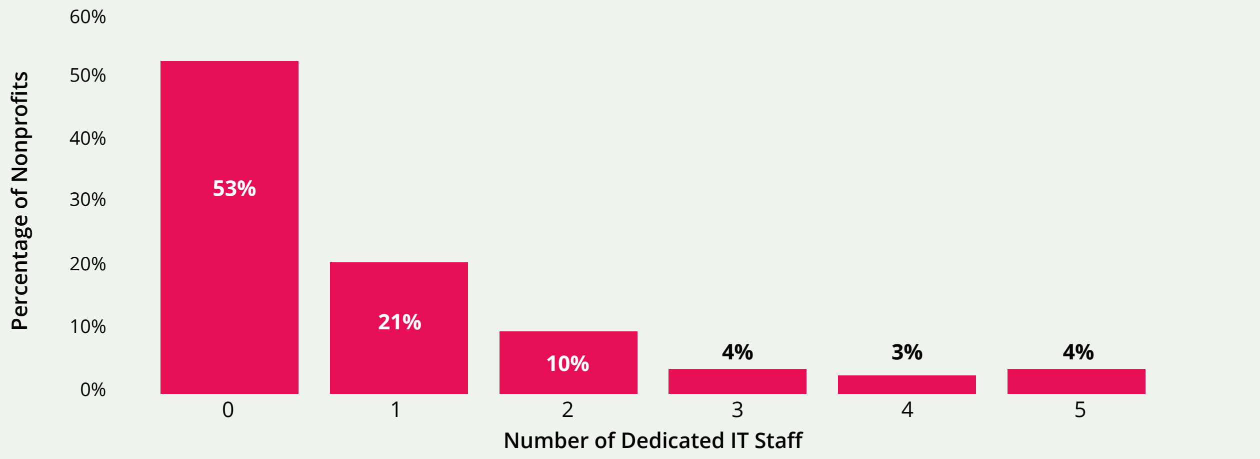
It is important to note that even though 47% of nonprofits surveyed have at least one full-time IT staff member, many had only one staff member. In fact, 21% of nonprofits reported having a single full-time IT staff member for the whole organization, and all respondents reported having fewer than five full-time IT staff.

For nonprofits with any full-time staff dedicated to IT or cybersecurity, the average ratio of full-time IT staff to full- or part-time employees was 1:96. That means on average, an IT staffer at one of these organizations is responsible for protecting 96 staff members.

To put this ratio into perspective, the NTEN Nonprofit Technology Staffing Report found that at small

Figure 4: Distribution of Nonprofits IT Staff

[68 Responses]



organizations, the average off ratio is 4.8 staff members foreach tech staffer, while at large organizations, an average of 35.9 staff members are supported by each tech staffer.[10] Our findings show that the ratio of 96 staff members per IT staffer is 167% higher than the highest average in the NTEN report.

Nonprofits already experience a high turnover rate among volunteers and staff. In 2024, the average yearly turnover rate for nonprofit staff was 19%, 58% more frequently than the 12% turnover rate for other companies.[11] This constant staff fluctuation may add additional strain on limited nonprofit IT staff, as institutional knowledge may be lost and IT operations frequently disrupted.

Use of Managed Services

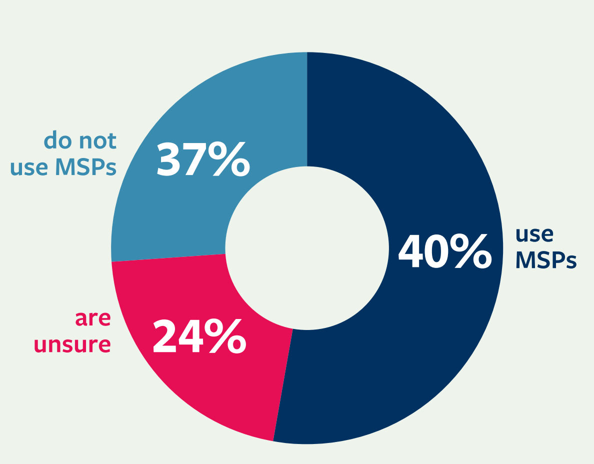
To get a full picture of nonprofits' staffing resources, we also considered the role of third-party supplemental staff, which may be hired as a cheaper alternative or a supplement to in-house IT staff. Third-party providers that manage infrastructure are called managed service providers (MSPs), and those that implement some amount of cybersecurity detection, triage, or response are called managed security service providers (MSSPs).

Our research found that 40% of nonprofits surveyed utilize MSPs or MSSPs for their IT and cybersecurity needs. While we expected that organizations with fewer in-house staff may rely more heavily on MSPs or MSSPs to provide their IT and cybersecurity needs, our survey found the opposite outcome: **nonprofits with one or more full-time IT staff are more likely to use MSPs or MSSPs than nonprofits with no full-time IT staff**.

This result may indicate that cybersecurity inequity can perpetuate itself. Organizations making limited to no investment in their IT and cybersecurity infrastructure may lack relevant in-house expertise to understand where investments are needed and make use of services like MSPs and MSSPs.

Figure 5: Nonprofits Use of MSPs/MSSPs

[68 Responses]



[10] Hulshof-Schmidt, Robert. (2019, November) *The 10th Annual Nonprofit Technology Staffing and Investments Report*. NTEN.

[11] Cerini, Kenneth. (2024, March 18) *2024 Nonprofit Trends*. Cerini & Associates, LLP

Finding #3:

Nonprofits have moderate adoption rates of basic cybersecurity controls, highlighting key areas of improvement.

CLTC surveyed San Francisco-based nonprofits about their adoption of the most highly recommended and effective cybersecurity controls: multi-factor authentication (MFA), routine software updates, and cybersecurity awareness training. Overall, CLTC found moderate rates of adoption across these measures, indicating that while many nonprofits possess a moderate level of cybersecurity literacy and allocate some time and resources to cybersecurity, there remain some gaps that nonprofits need to address.

Multi-Factor Authentication

Enabling MFA is widely recognized as one of the simplest and most effective ways to reduce the impact of cyber intrusions for an organization. MFA adds an extra check to confirm a user's identify as they are logging into an account with a username and password, for example by requiring them to enter a code from an SMS text or authentication app. According to CISA, requiring MFA for account access can lower the risk of account breach by 99%.[12] All of the cybersecurity frameworks consulted for this study strongly recommend MFA for administrative accounts or all users, and it is a proven method for preventing unauthorized access to an organization's information systems.

Survey results showed that nonprofits have moderate adoption rates of MFA for email and collaboration tools, such as Microsoft 365, Google Suite, and Dropbox, with 61% of respondents implementing this security measure. This indicates that more than three out of five nonprofits surveyed have taken steps to secure their email and collaboration platforms against unauthorized access. This is a good sign, as small nonprofits rely heavily on email and file-sharing tools for their day-to-day operations, and protecting these accounts with MFA is a critical first step.

One factor that may contribute to this moderate adoption rate may be that these types of email and collaboration tools increasingly prompt users to enable MFA upon account setup, making it easier for organizations with limited cybersecurity or IT know-how to integrate the feature.

We were alarmed to discover that 16% of nonprofits do not utilize MFA at all within their organizations, and 25% make MFA optional on one or more platforms. This may increase the risk of account compromise; without MFA, it only takes one weak password to allow unauthorized access to a staff or leadership account. Expanding the use of MFA on all critical services is an important area of improvement for these nonprofits.

16%
of nonprofits do not use MFA

61%
of nonprofits have MFA set up for email and collaboration tools

25%
of nonprofits make MFA optional on one or more platforms

[12] Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Multifactor Authentication*. U.S. Department of Homeland Security (DHS).

Software Updates (Patching)

Regularly updating computer software and operating systems is important for cybersecurity because it ensures that security updates, which can protect against new software vulnerabilities, are implemented quickly. Automatic updates can be especially effective, as software will update itself as soon as new updates are released, eliminating the need for staff to manually track and implement changes. Frequent update cadences are considered by most cybersecurity frameworks to be a best practice for protecting software and systems against new vulnerabilities.

Our findings show that 50% of nonprofits update software on a sufficiently regular basis: 34% enable automatic updates, and 16% manually update their software every month.

However, the other half of nonprofits followed a more infrequent update schedule, with 20% updating whenever there is time, and 9% updating every 3-6 months or longer. Another 20% of nonprofits reported alternate schedules or practices not explicitly listed in the provided options. These respondents often indicated uncertainty about the update schedule, with some noting that they weren't sure or that update frequency varied depending on the software. Infrequent update cadences can leave software vulnerable to newly discovered security threats and mark another area of improvement for many nonprofits.

Cybersecurity Awareness Training

Cybersecurity awareness training is essential for equipping an organization's employees and volunteers with knowledge about how to protect their information and spot common cyber attacks like phishing emails. Cybersecurity education is a tested method for protecting against the risks caused by the "human factor," when cyber attackers deceive and take advantage of employees to compromise their organization's security. Such methods, which include spear phishing and social engineering, are used in up to 74% of data breaches.[13]

Just over half of surveyed nonprofits (52%) do not offer any cybersecurity awareness training to their staff and volunteers. Thirty percent of nonprofits require all staff members and volunteers to complete training, while 18% provide training to only some staff and/or volunteers. That such a sizable portion of nonprofits do not use or require awareness training for all employees highlights another area of improvement for nonprofit cyber defense.

Figure 6: Cadence of Computer Software and Operating System Updates by Nonprofits

[44 Total Responses]

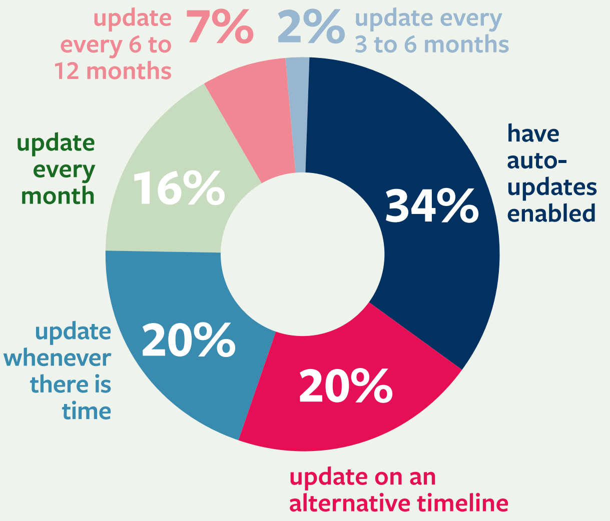
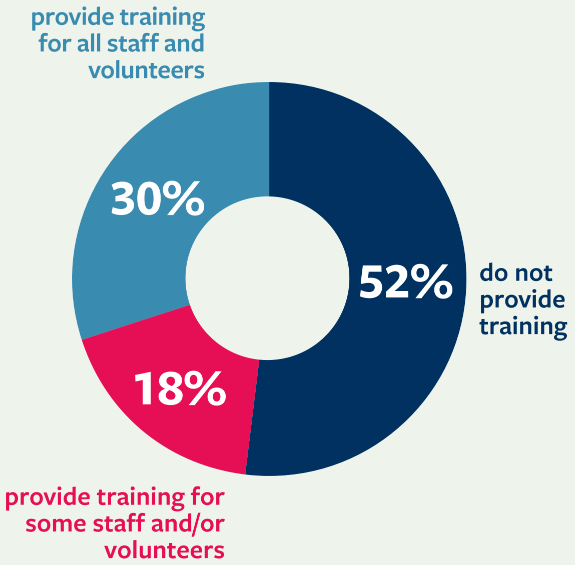


Figure 7: Cybersecurity Awareness Training Offered by Nonprofits

[44 Total Responses]



12 Verizon Business. (2024) *2024 Data Breach Investigations Report*. Verizon.

Finding #4:

Nonprofits struggle most with funding and prioritizing cybersecurity.

Ranking Cybersecurity Obstacles

The survey sought to identify the specific challenges that hinder nonprofits from adopting cybersecurity measures. Survey respondents ranked a variety of obstacles based on how much they impede their progress.

The five obstacles provided were:
(a) not enough funding for cybersecurity and IT,
(b) a lack of knowledge on what to improve,
(c) organizational culture is resistant to cybersecurity changes,
(d) leadership does not care about cybersecurity, and
(e) difficulty prioritizing cybersecurity over competing objectives.

Highly Ranked Cybersecurity Obstacle: Prioritization

Almost all nonprofits (89%) ranked prioritization as one of their top three obstacles; difficulty in prioritizing cybersecurity over competing objectives was the most commonly listed of all five obstacles. Prioritization was also the obstacle most commonly ranked #2 by survey respondents.

It is notable that prioritization was more important than knowledge to some nonprofits than knowledge. A common narrative in nonprofit cybersecurity is that nonprofits are not aware of the cybersecurity risks, and have to be educated on what cybersecurity is and why it is important. But both in these survey findings, and during in person workshops, nonprofits displayed clear understanding of the threat of cyber attacks and their potential impact on nonprofit operations and resident information.

As mission-driven organizations, nonprofits may face more friction than most for-profit companies to allocate time and resources away from their core purpose towards a topic like cybersecurity. Even if nonprofits understand cybersecurity risks, it is an extremely difficult tradeoff to make between hiring an IT employee and something with tangible mission impact, like being able to expand a food pantry.

Figure 8: Top Ranked Nonprofit Cybersecurity Barriers
[68 Responses]

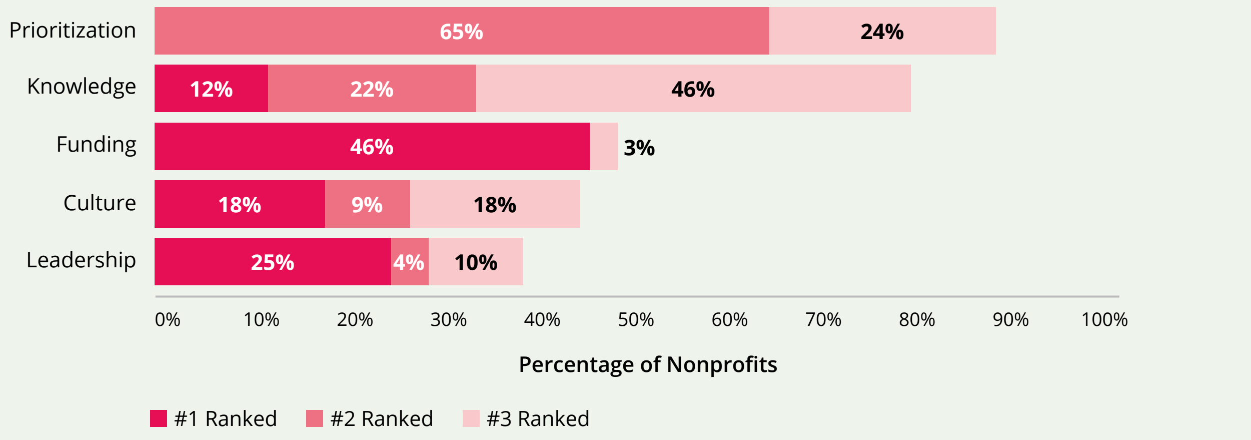
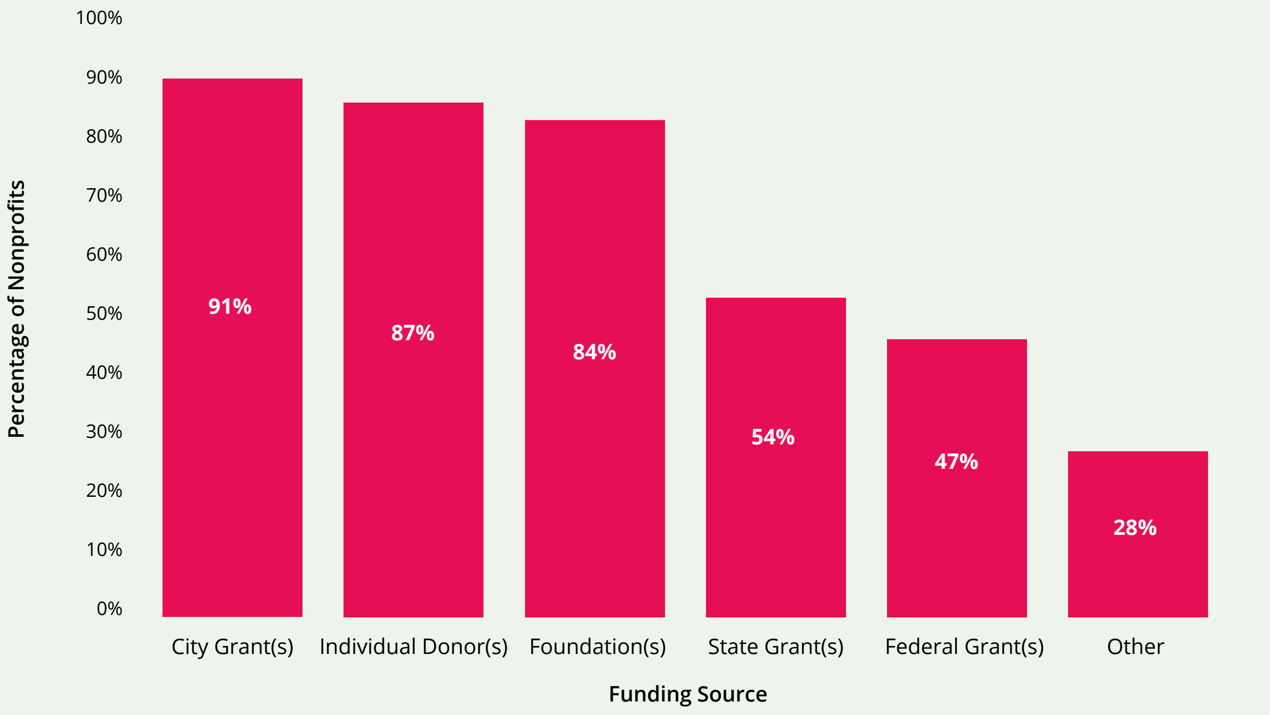


Figure 9: Nonprofit Funding Sources

[68 Responses in Total]



Highly Ranked Cybersecurity Obstacle: Funding

Another highly ranked obstacle is funding; it was the most commonly ranked #1 obstacle preventing nonprofits from adopting cybersecurity measures, with 46% of nonprofits ranking it as the top obstacle. Nonprofits face significant financial constraints just to stay in operation and fulfill their service missions, so it is no surprise to learn that this is an element they most struggle with for cybersecurity.

One reason for this obstacle could be low overall budgets for cybersecurity. Surveyed nonprofits (67) had an average technology budget of $48,000 in the 2023 fiscal year, though **9% of nonprofits reported a technology budget of $0**. This budget could be spent on more than just cybersecurity, but also IT and computer needs, including software, laptops, and internet access.

Nonprofit Funding Sources and Restrictions

Another reason funding is an important obstacle is that nonprofits are constrained from using existing funding for cybersecurity. Nearly all respondents received funding directly from the City and County of San Francisco, with 91% reporting they used city grants as funding sources. Philanthropy was a common funding source as well, as 87% of nonprofits receive funding from individual donors and 84% from foundations.

It is worth noting that in the workshop, several participants noted that they were unable to use certain funding opportunities for cybersecurity because it was considered “overhead,” a designation used to describe any activities not put directly towards the project being funded.

Grants from city, state, federal, and private philanthropy can all have caps on the amount of funding allowed to be used for overhead, typically at around 10%. This means that nonprofits are forced to spread limited overhead funding across human resources, employee salaries, finance, and technology, making it much more difficult to allocate budget towards cybersecurity.

Finding #5:

Nonprofits want hands-on, human assistance to improve their cybersecurity.

Ranked Cybersecurity Needs

Nonprofits' preferences for how they learn about and implement cybersecurity improvements matter; staff and leadership know best what resources could practically and feasibly be deployed within their organizations.

For this reason, CLTC sought to gather input from nonprofits about their preferences for cybersecurity resources.

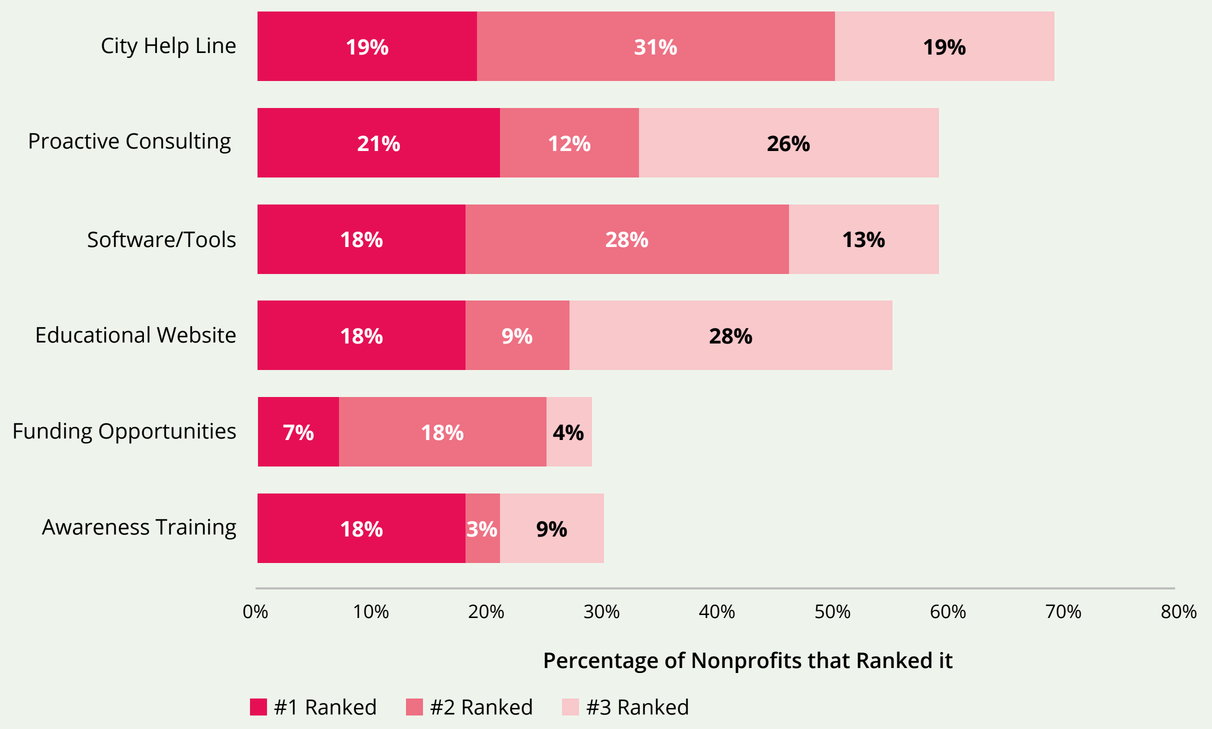
Nonprofits were asked to rank the following solutions based on their cybersecurity needs:

(a) free cybersecurity awareness training,
(b) a website with cybersecurity education materials and toolkits,
(c) consultation services to recommend improvements,
(d) City of SF Cybersecurity Helpline,
(e) access to cybersecurity software/tools, and
(f) cybersecurity funding opportunities.

Top 3 Cybersecurity Needs:

1. City Help Line | 2. Software and Tools | 3. Proactive Consulting

Figure 10: Top Ranked Nonprofit Cybersecurity Wishes



Higher Priority Cybersecurity Solution: City Help Line

The most commonly top-ranked solution was for a city-run help line, with 69% of respondents ranking it in the top half, and 50% of respondents ranking it in the top two solutions. A city-provided helpline would offer nonprofits free and on-demand access to IT and cybersecurity expertise when needed. It is notable that many nonprofits seek someone to provide affordable and reliable cybersecurity assistance, and is consistent with our finding that many nonprofits do not have full-time IT staff.

Higher Priority Cybersecurity Solution: Proactive Consulting

Another solution that ranked high on nonprofits' wish lists is proactive consulting, when professionals meet with organizations to assess their cyber defenses and recommend strategic improvements. Consulting ranked among the top three most valuable solutions by 59% of respondents and was the most common #1 ranked solution.

Similar to a city helpline, proactive cybersecurity consulting provides nonprofits with expert one-to-one guidance by a full-time professional. The strong preference for both proactive consulting and a city helpline underscores nonprofits' need for human assistance, not toolkits or other static, DIY tools, to guide them through cybersecurity improvements.

Access to a website with cybersecurity education materials and toolkits was also highly ranked, with 54% of respondents ranking it in the top three. Such a resource could centralize a wealth of information relevant to nonprofits and consolidate the city's informational resources. A dedicated website could potentially save nonprofits time and effort in searching for up-to-date, non-profit information on cybersecurity guidance and resources for specific topics.

Lower Priority Needs: Funding and Awareness Training

The solutions that were ranked lowest by survey respondents were cybersecurity funding opportunities and free cybersecurity awareness training, both of which were ranked in the top three by just 29% of respondents. Awareness training ranked as the lowest priority (#6) more than any other solution.

While funding was identified as the biggest hurdle to improving nonprofits' cybersecurity, it ranked low as a solution. This discrepancy may suggest that funding alone is not enough to improve nonprofit cybersecurity; when presented with more specific actions, such as hands-on assistance, nonprofits preferred these solutions. These results may also provide a clue about how nonprofits would invest funds if they had them, with an emphasis on 1:1 professional assistance or staffing.

Free Response Solutions

Respondents were given an open-ended prompt to specify additional needs beyond the provided options. Several themes emerged from these findings:

Theme #1 – Dedicated human assistance is needed

Several respondents emphasized how important having dedicated staff time dedicated to cybersecurity would be. Over a dozen specifically noted their desire for either a dedicated IT staffer or an affordable IT contractor, MSP, or MSSP to work only on cybersecurity.

Theme #2 – High-use technologies requested

Some respondents detailed the type of tools they were interested in acquiring, adding more color to the rankings of the "Software/Tools" need. The requested tools included:

- A monitoring or / alertingaltering system (typically called security iInformation event mManagement (SIEM) in the cybersecurity field);
- Cybersecurity awareness training;
- Email fraud detection tools; and
- A password management system.

Theme #3 – First-steps knowledge and training are needed

Several participants noted the need for specific guidance on key areas of cybersecurity, such as what to do in an emergency and how to keep up with changing technology. More broadly, participants expressed confusion on how to protect themselves and where to go to learn about cybersecurity and IT concepts.

Cities Can, and Should, Be Hubs of Cyber Defense

Cybersecurity is a team sport, and everyone has a different role to play in protecting nonprofits from cyber attacks, including state and federal governments, enterprises, vendors, associations, and nonprofit leaders.

City governments, though, are uniquely positioned to support local nonprofits with their cybersecurity defenses:

1 **Cities already have working relationships with nonprofits.** Cities provide grants to many local nonprofit organizations to support their work addressing community needs and enhancing community well-being. City governments nurture strategic relationships with local nonprofits, relying on them to achieve their policy objectives in the areas of public health, housing, education, community and economic development, and arts and culture.

2 **Cities have specialized knowledge about public-interest cybersecurity,** which enables them to effectively support and guide nonprofits on their cybersecurity journeys. Cities employ technologists with expertise in IT and cybersecurity who are committed to ensuring the security and resilience of the local institutions that uphold public life. These public servants are well-versed in facilitating cybersecurity with limited resources, and can recommend practical cybersecurity solutions to nonprofits that will better serve residents.

3 **Cities' digital equity objectives align with cybersecurity.** Offices of digital equity in city governments aim to close the digital divide and improve access to digital resources and literacy for low-resource and marginalized communities. Nonprofit organizations play an important role as key distributors of resources like broadband access and computer training for community members. By providing cybersecurity support to nonprofits, cities can help these organizations better serve their communities while advancing their broader digital equity goals.

All of the following recommendations are aimed at helping the City of San Francisco invest in local nonprofits and improve their cybersecurity protections — not because the City is the only entity who should be involved, but because it is well positioned to make a significant impact on nonprofit's digital security.

Policy Recommendations

Recommendations at a Glance

Education

#1 **Provide regular cybersecurity advice** and assistance to local nonprofits.

#2 **Host an annual cybersecurity convening** for nonprofits to learn and network with cyber professionals.

Resource Coordination

#3 **Create a nonprofit cybersecurity resource webpage** for sf.gov.

#4 **Offer cybersecurity funding opportunities for nonprofits** to apply to hire, or contract, cybersecurity talent and/or acquire software and tools.

Implementation

#5 **Host student summer interns** to work with nonprofits on cybersecurity issues.

#6 Provide local nonprofits with **low-cost access to critical cybersecurity tools and software**.

Recommendations

Education

#1 Provide regular cybersecurity advice and assistance to local nonprofits.

Timeline: 12-14 Months | **Difficulty:** ★★★ | **Resources:** High

The City should consider providing regular strategic advice and assistance to local nonprofits to help them take the most important steps to improve their defenses. The Office of Cybersecurity and the Office of Digital Equity could make available one or more staff provide 1:1 virtual meetings with nonprofits to answer questions and offer personalized cybersecurity advice.

Prior to scheduling a meeting, we recommend that nonprofits complete a short cybersecurity assessment such as the CISA Cross-Sector Performance Goals checklist. The assessment will provide city staff with a snapshot of the organization's current cybersecurity practices, and review the answers with the nonprofits to show them where they can improve. City staff can also serve as an educational resource to nonprofits by hosting monthly office hours and providing cybersecurity training workshops.

#2 Host an annual cybersecurity convening for nonprofits to learn and network with cyber professionals.

Timeline: 12 Months | **Difficulty:** ★★ | **Resources:** Medium

The City should consider hosting an annual convening on nonprofit cybersecurity to connect nonprofits with resources, guidance, and training and cultivate a local nonprofit cybersecurity community. This convening could involve interactive cybersecurity workshops on threats and common cybersecurity controls relevant to nonprofits. The convening also presents an opportunity to introduce nonprofit leaders to local cyber defense organizations such as the CISA Region 9 office and its Cyber Security Advisors (CSAs), the Bay Area Urban Areas Security Initiative (UASI), the SF FBI field office, and NGO-ISAC.

Additionally, the City could leverage its unique relationship to major tech companies to invite local cybersecurity experts from industry. This could take the form of event speaking engagements, sponsorship, or even hands-on, and may provide opportunities for the City to secure free or low-cost software for nonprofits.

Recommendations

Resource Coordination

#3 Create a nonprofit cybersecurity resource webpage for sf.gov.

Timeline: 3 Months | **Difficulty:** ★ | **Resources:** Low

The Office of Digital Equity should consider building a centralized nonprofit cybersecurity resource hub on the sf.gov website. This webpage could host all cybersecurity resources for nonprofits offered by the city, such as a scheduling portal for 1:1 meetings with city cybersecurity staff and a calendar of relevant cybersecurity seminars and webinars hosted by the City and its state, federal, and industry partners. It may also highlight cybersecurity resources for nonprofits such as cybersecurity self-assessment tools, toolkits, and other best practices.

Additionally, the webpage could host information on City grants and state and federal funding opportunities available for spending on cybersecurity resources.

#4 Offer cybersecurity funding opportunities for nonprofits to hire, or contract, cybersecurity talent.

Timeline: 12-24 Months | **Difficulty:** ★★★★ | **Resources:** High

The City should consider offering financial support to nonprofits to hire cybersecurity talent, or contract cybersecurity managed services to improve their cybersecurity maturity provide network detection and monitoring services. While the City may provide high-level, strategic cybersecurity advice, nonprofits may need hands-on assistance to implement these recommendations and embark on a cycle of continuous evaluation and improvement.

Some managed service providers (MSPs) primarily work with smaller organizations and nonprofit, such as Sightline Security and Alternative Technology: and some nonprofits may prefer to use MSPs to get hands-on expertise, while others may prefer to hire full-time positions and relieve overburdened IT and cybersecurity teams.

The City should determine whether funding could be scoped into existing grant programs (ex: 5% of all grant funding shall be used on technology, IT, and cybersecurity) or if a new or standalone grant program is needed to provide this funding to nonprofits.

Recommendations

Implementation

#5 Host student interns to work with nonprofits on cybersecurity issues.

Timeline: 12-24 Months | **Difficulty:** ★★★★ | **Resources:** High

The City should consider hosting student internships to assist San Francisco-based nonprofits with cybersecurity topics, creating opportunities for cybersecurity students from local universities and community colleges to get work experience while serving their communities. These internships could involve implementing cybersecurity controls such as multi-factor authentication (MFA), writing policies for IT teams to onboard and offboard accounts, and other items to supplement the strategic cybersecurity recommendations provided by the city staff (See Recommendation #1). As part of this program, interns could be supervised by city employees while being deployed at the nonprofits themselves, allowing for mentorship by the Office of Cybersecurity and the Office of Digital Equity and career paths into public service.

The City can partner with a wealth of higher education in the Bay Area to host interns, including local community colleges and universities. For example, UC Berkeley's School of Information offers a grant for its Master of Information Management and Systems students, providing up to $5,000 in financial support per student for students to pursue summer internships at nonprofit or public interest organizations. This program would enable the City of San Francisco to host paid interns at no cost, and enables nonprofits to receive cybersecurity assistance they may not otherwise be able to afford.

#6 Provide local nonprofits with low-cost access to critical cybersecurity tools and software for SF-based nonprofits.

Timeline: 12-14 Months | **Difficulty:** ★★★★ | **Resources:** Low

The City should consider leveraging its unique relationships with San Francisco-based major technology companies to secure cybersecurity tools and software for San Francisco-based nonprofits. We recommend that the City explore philanthropic initiatives where these companies can support the local community by offering free or discounted access to critical tools such as SIEMs, password management tools, firewalls, updated operating systems, and updated physical equipment.

Conclusion

Conclusion

Cities and nonprofits share a common mission to serve their local communities, but nonprofits in the Bay Area often face cybersecurity challenges that impede their services, and they lack the resources needed to address them. This gap in nonprofit cybersecurity defenses is an opportunity for the City and County of San Francisco to serve as a local hub of cyber defense and support these critical community organizations while advancing their broader digital equity and public service agendas.

Our findings show that nonprofits have limited cybersecurity resources and are common victims of cyber attacks, and this report highlighted areas of improvement that nonprofits themselves surfaced and prioritized. The collaborative process of the CyberCAN initiative has paved the way for strong collaboration between the City, nonprofits, and academic institutions like UC Berkeley, and presents an innovative model of beneficiary-led solution-making to improve nonprofit cybersecurity.

Looking ahead, CLTC hopes to expand CyberCAN to other U.S. cities, investigate the cybersecurity challenges and resource gaps experienced by nonprofits in greater granularity, and develop community-tailored recommendations that improve the cybersecurity posture of these essential nonprofits.

Acknowledgements

On behalf of CLTC, we would like to thank our partners at the City and County of San Francisco for their generous time, leadership, and support of this project. Thank you especially to Rey LaChaux from the Office of Digital Equity, and Nathan Sinclair, Kamroonbanu Mohideenbasha, and Tuan Phan from the Office of Cybersecurity. A special thanks to Michael Makstman, City Chief Information Officer and Executive Director of the Department of Technology, for his commitment to bridging cybersecurity gaps for the whole San Francisco community and his long-term allyship with CLTC. Thank you for trusting us with this important work.

We would also like thank our reviewers Chuck Kapelke, Izzie Deixel, and Chelsea Conard, who graciously lent us their time and gave expert and crucial report feedback.

Finally, this work would not have been possible without the generous financial support of Craig Newmark Philanthropies and Okta for Good, whose broad support of the Public Interest Cybersecurity portfolio at CLTC enables us to pursue new and needed research projects like this one.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

OFFICE OF CYBERSECURITY

SAN FRANCISCO

DEPARTMENT OF TECHNOLOGY

SAN FRANCISCO

DIGITAL EQUITY